Hack Everything...

A Detailed Timeline of the DNC Hack

David Spring M. Ed.

Turning Point News.org

January 10, 2017

The NSA Motto is
Collect Everything...

But in order to
Collect Everything,
Your have to
Hack Everything.

David Spring M. Ed.
Turning Point News.org

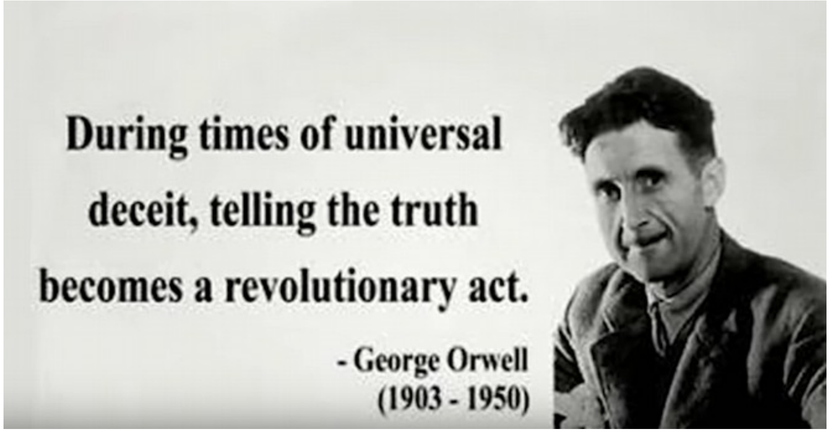
A free PDF download of this report
is available at **TurningPointNews.org.**
As our site may be taken down at any moment,
please help us get the word out by sharing this report.
Permission is granted to download, distribute, repost
& republish all or any part of this report on any website.

Hack Everything…
A Detailed Timeline of the DNC Hack

David Spring M. Ed.

Dedication

This report is dedicated to Edward Snowden,
a true patriot who understood that his duty was
not to defend and protect dishonest leaders,
but to defend and protect
the Constitution of the United States.
Many suspected we were all being watch from “behind the curtain.”
Snowden risked his life to give us the proof.


During times of universal
deceit, telling the truth
becomes a revolutionary act.
- George Orwell
(1903 - 1950)

Acknowledgements

This report provides links to more than 100 other reports.
Each of these reports provided the pieces
in putting together this complex puzzle.
I want to thank all of these researchers for their work.
Together, we can and will overcome deception and deceit.
Those pushing for cyber warfare may have massive amounts of money.
But we have a more powerful weapon… The Truth.

Hack Everything….
A Detailed Timeline of the DNC Hack
--- Table of Contents ---

"The NSA is
Worse than
Your Worst
Nightmare."
Jacob Applebaum

Executive Summary… A Primer on the Power of the NSA

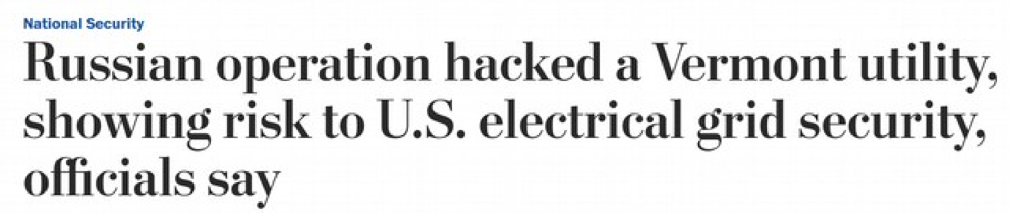
Misleading and blatantly false claims about the attack on the Democratic National Committee (DNC) are being used to create fear in the minds of the American people in order to launch cyber warfare and other sanctions against Russia. These scare tactics are also being used to pass draconian legislation limiting free speech and increase funding for the American Police State. This wave of propaganda is also a convenient excuse to explain away the Democratic Party loss of the 2016 Presidential Election. If we are interested in determining why the DNC hack happened, and how it happened, we first need to separate the lies from the truth so we can understand what happened and when it happened.

There were many significant and inter-related events both before the leak and after the leak. Many false claims have been made about several of these events in what appears to be a propaganda war of distortions, disinformation and outright lies by the main stream media. Numerous articles have been written on both sides of this debate. Yet thus far, there has not been a detailed timeline to review the events as they happened. The purpose of this report is to fill this void. Although a complete timeline of the DNC hack would go all the way back to the 1990s and the beginning of the modern Internet (a subject I have written extensively about in past articles), we will start with the 2007 formation of the NSA Prism Partners Program as the precursor to the 2009 US cyber warfare attack on Iran and carry it to the present day DNC cyber warfare attack. This is therefore an outline of the past 10 years of international cyber warfare – something the American people know next to nothing about.

After the timeline, we will go into detail over who was most likely to have done the hacking and why they hacked the DNC. Our conclusion based on an overwhelming amount of evidence is that the Russian government did not hack the DNC. The only question remaining is who did hack the DNC and why they did it. This is a lengthy report for the simple reason that strong allegations require strong evidence. Just as US Intelligence agencies had a duty to provide irrefutable evidence to the American people to justify launching an attack against Russia, so do we have a duty to provide irrefutable evidence to support the claim that Russia was not responsible for the DNC hack. We believe this report provides that evidence. This report includes numerous well documented facts that have never been released before. Those who spend too much time reading only the main stream media may be shocked by these facts. Others who have spent more time reading independent news sources may not be surprised at all. The truth is a powerful weapon. It is time to shed some light on this darkness. If you have any questions or comments, feel free to email me: david@turningpointnews.org.

Why We Can Be Certain the Russian Hacking Stories are False

On December 30, 2016, we posted an article explaining why the Russian Hacking of the DNC story was false – using actual screen shots from the DHS/FBI Grizzly Steppe report. One day later, there was another false story promoted widely by the main stream media claiming that Russia hacked the Vermont Electric grid. This shocking claim was immediately denied by administrators of the Vermont electric grid. Here is the false headline from the Washington Post:

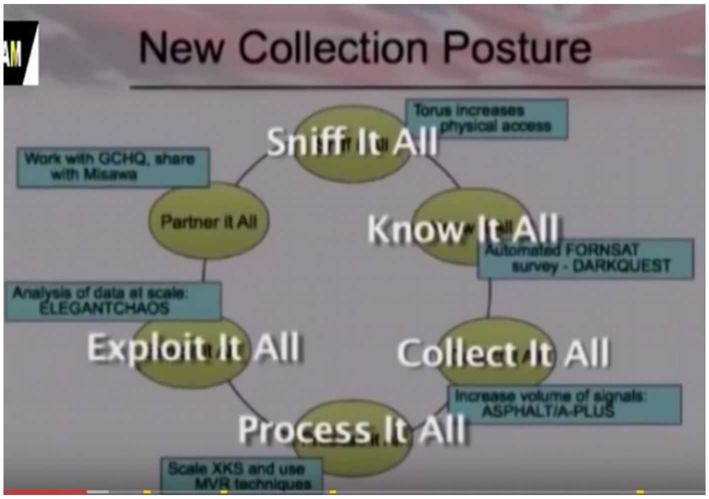


National Security

Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say

We ended our previous article with quotes from two former NSA Systems Administrators, William Binney and Edward Snowden, in which they both noted that if the Russians really did hack the DNC or the Vermont Power System or anything else, **the NSA would certainly have a detailed record of the hack and could provide that evidence to the American people without compromising national security sources or secrets.**

Thanks to the Independent Media, our article was picked up by several prominent websites and read by tens of thousands of people. Unfortunately, the feedback we received (doubting that the NSA has this ability) made it clear that many Americans still have no idea about the true power of the NSA – despite the fact that Edward Snowden provided detailed documents from the NSA more than three years ago describing the NSA's immense power and confirming that the **NSA wants to "collect it all."**



New Collection Posture

Sniff It All

Torus increases physical access

Work with GCHQ, share with Misawa

Partner It All

Know It All

Automated FORNSAT survey - DARKQUEST

Analysis of data at scale: ELEGANTCHAOS

Exploit It All

Collect It All

Increase volume of signals: ASPHALT/A-PLUS

Process It All

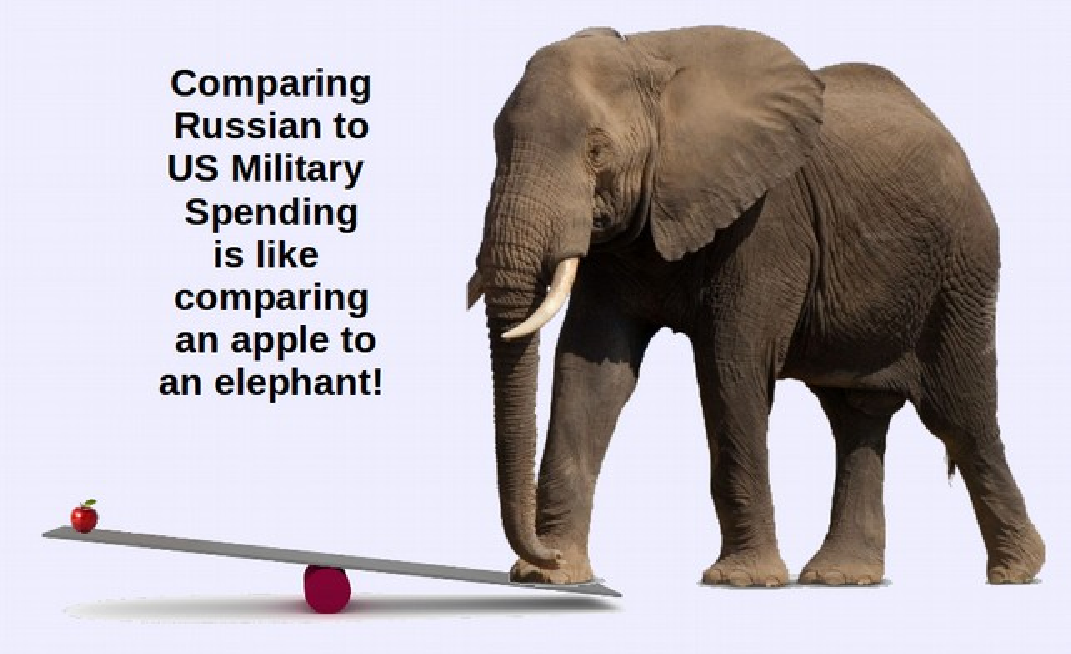
Scale XKS and use MVR techniques

It is dangerous that the NSA possesses such horrific hacking powers. But it is even more dangerous that so many Americans, and perhaps even most Americans, still have no idea what the NSA is capable of and the type of hacking and data recording the NSA does every day – including the mass surveillance of 300 million Americans. We will therefore begin this report with a brief primer on the power of the NSA.

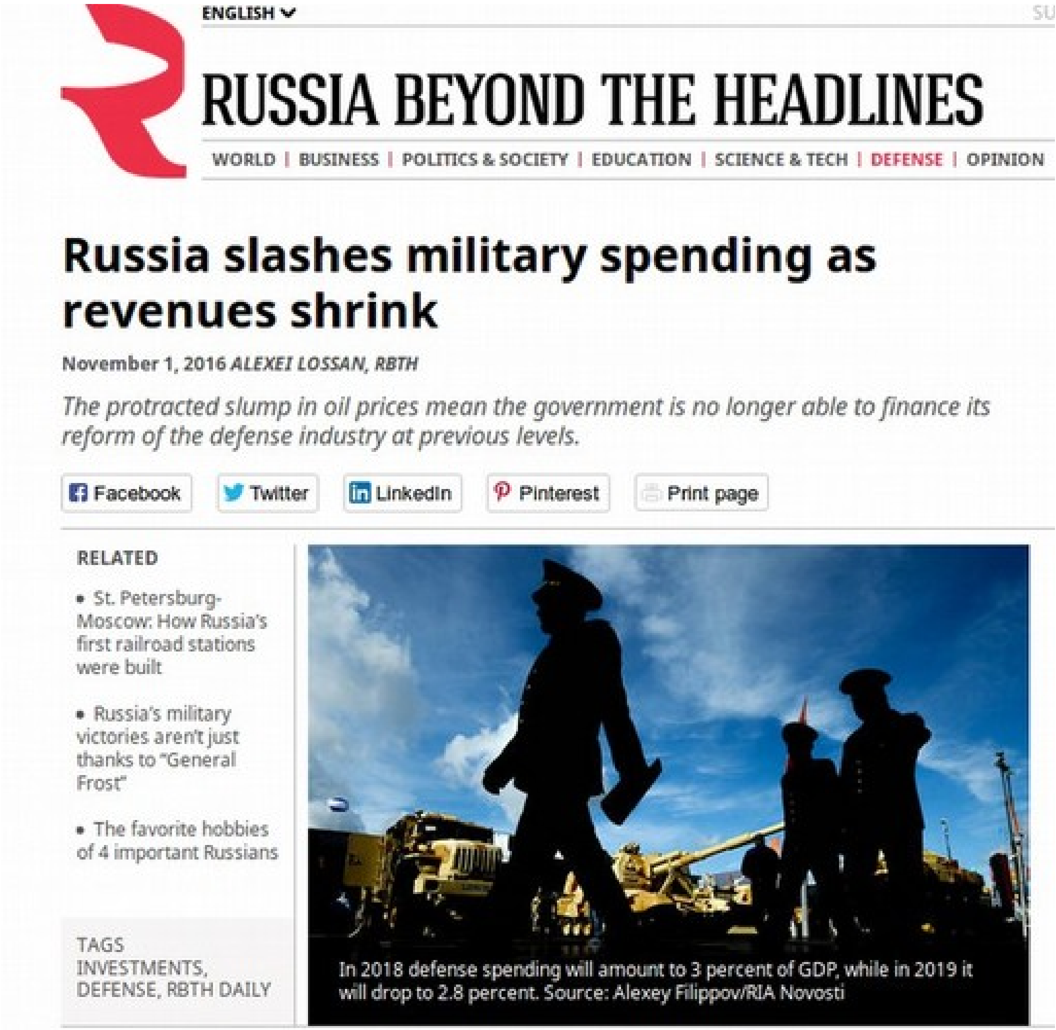
What is the NSA?
The NSA is the National Security Agency. It is the cyber warfare wing of the US military. It is by far the largest and most well funded cyber warfare group in the entire world – much larger than all of the other hackers in the world combined. We know this is true not only from the Edward Snowden documents and William Binney disclosures but also from numerous other sources as we will describe below. Before going into the details of the NSA cyber warfare program, let’s begin with a few important facts:

Fact #1: Follow the Money… Compare US to Russian Military Budgets
The US military budget is currently about $600 billion per year. But this is just the “base” budget and does not include the cost of war in Afghanistan or Iraq or the secret cyber warfare budget or Homeland Security or the FBI. When the entire US Police State budget is added up, it comes to more than one trillion dollars per year.
https://consortiumnews.com/2013/02/02/the-trickery-of-the-military-budget/

By comparison, the Russian military budget is about $50 to $60 billion per year. This means that the US military is 10 to 20 times larger than the Russian military. This also means that the US cyber warfare program is 10 to 20 times larger than the Russian cyber warfare program. In short, the US has 10 to 20 times more hackers and produces 10 to 20 times more cyber warfare programs than Russia.
https://en.wikipedia.org/wiki/List_of_countries_by_military_expenditures


Comparing Russian to US Military Spending is like comparing an apple to an elephant!

US Military Spending Skyrockets while Russian Military Spending Plunges
Due to very low oil prices, Russia is having major financial problems. In addition, Russians population is aging and decreasing and now is only 144 million. Military spending in Russia fell about 5% in the past year. They are expected to decline about 30% more in 2017. Moscow-based newspaper Vedomosti has warned the cuts "brings Russia close to third-world countries.”


ENGLISH
SU
WORLD | BUSINESS | POLITICS & SOCIETY | EDUCATION | SCIENCE & TECH | DEFENSE | OPINION
Facebook
Twitter
LinkedIn
Pinterest
Print page

RUSSIA BEYOND THE HEADLINES

Russia slashes military spending as revenues shrink

November 1, 2016 *ALEXEI LOSSAN, RBTH*

The protracted slump in oil prices mean the government is no longer able to finance its reform of the defense industry at previous levels.

RELATED

- St. Petersburg-Moscow: How Russia's first railroad stations were built
- Russia's military victories aren't just thanks to "General Frost"
- The favorite hobbies of 4 important Russians

TAGS
INVESTMENTS, DEFENSE, RBTH DAILY

In 2018 defense spending will amount to 3 percent of GDP, while in 2019 it will drop to 2.8 percent. Source: Alexey Filippov/RIA Novosti

Here is a recent quote:

"As the economy continues to struggle under the weight of low oil prices and sanctions, Russian authorities have decided to cut defense spending by 1,000 billion rubles ($15.89 billion), or by approximately 30 percent. The figures became clear from the draft federal budget that the government submitted to the State Duma at the end of October, business daily Kommersant reports. Overall, spending on national defense in the federal budget for 2017 is envisaged at 2,840 billion rubles (**$45.15 billion**), or 3.3 percent of GDP." http://rbth.com/defence/2016/11/01/russia-slashes-military-spending-as-revenues-shrink_644019

In addition to the US military being 10 to 20 times bigger than Russia, spending on the US Cyberware program had skyrocketed while spending on cyber warfare in Russia hand plummeted – especially when one accounts for currency exchanges and inflation.

As just one example, the GRU is the Russian Military Intelligence Service. They are similar to our NSA. In 2009, the head of the GRU retired or was fired. His replacement was forced to fire 1,000 staff members and cut the number of agencies almost in half (from 8 to 5).

Then in 2011, the replacement retired or was fired and replaced by Igor Sergun – a person many in Russia said lacked the experience to be the head of intelligence. Igor lasted 5 years but he died of a heart attack in January 2016. There was no one leading the agency for over one month as Putin could not decide on a replacement. Then Putin chose a complete unknown called Igor Korobov who is currently the head of the GRU.

Here is a quote from a Moscow Times article about the gutting of the GRU: :
"A former GRU officer, who spoke on condition of anonymity, slammed the reform, saying it had resulted in old professionals stepping down and greenhorns coming in."
https://themoscowtimes.com/news/gru-spymaster-to-lose-job-report-says-9798

Here are a couple more quotes:
"Another veteran of the GRU, who asked not to be named, said that the situation in the GRU is now close to critical. There is a collapse of the military intelligence, which has long been the eyes and ears of the military command. Special Forces Brigade cut, the new technology does not arrive, experienced professionals retire, there is only the young people who really can not do anything."
http://izvestia.ru/news/501899

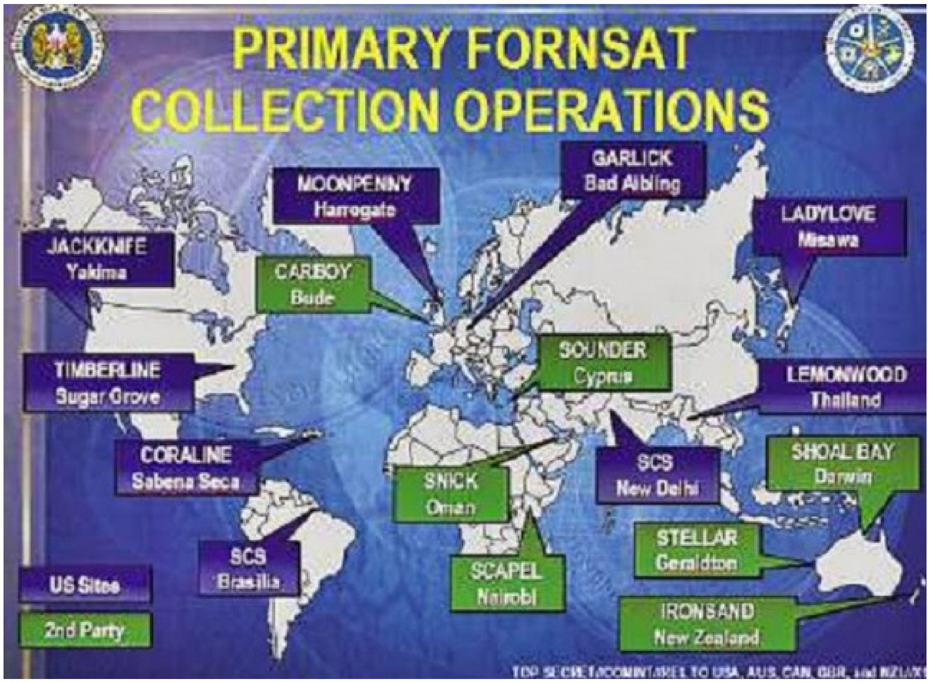
Eighty of its (GRU top one) hundred general-rank officers had been sacked, retired, or transferred.
www.foreignpolicy.com/2014/07/07/putins-secret-weapon/

So we are expected to believe that a Russian spy group that has seen 80% of its top leaders fired, and has had several new leaders in the past several years and is facing a **30% budget cut for 2017** is somehow a threat to the NSA which is already about 10 to 20 times bigger and without a doubt has the most powerful cyber weapons in the world?

In fact, at a televized press conference in the Spring of 2016, Edward Snowden asked the Russian leader Putin if Russia does mass hacking of its citizens the way the NSA does in the US. Putin replied that it would be illegal. Putin later added that he admires the NSA but Russia simply could not afford something like the NSA.

Have we heard anything about this dramatic decline in Russian military spending in the US main stream media? Not one word. Instead, all we hear from the US press is that Russians are attacking the Vermont Power Grid and before we know it, everyone in America will have their heat shut down and their lights turned off. But what is keeping the American people in the dark is not Russian hackers. It is the main stream media that refuses to tell the American people the truth. The insanity of this situation boggles the mind.

Fact #2: Understand the Scale of the NSA Hacking Program
Second, as confirmed in documents provided by Edward Snowden, the NSA has tens of thousands of sub-contractors at hundreds of cyber warfare bases using thousands of servers all over the world.

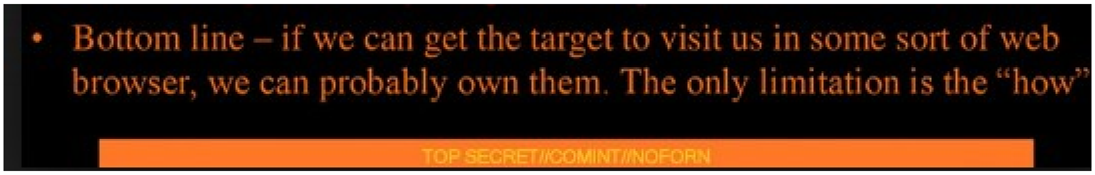


The NSA also has the largest data center in the world. The full scale of the NSA cyber warfare program is almost beyond comprehension. The NSA uses this horrific power to hack and infect millions and even billions of computers around the world. The NSA motto is “Collect Everything.” In reality, this means to “**hack everything.”** The term “everything” does not mean hacking just the systems of criminals – it means hacking the systems of everyone – including you whenever you go on line, or send an email or use a smart phone. “Everything” also includes all information from all networks – whether it is a corporate network or the networks of social groups or political parties. Those of us who have been studying the NSA for years understand that the term “everything” actually means everything. The NSA likes to boast, **“We Collect It All.”** All means all data regardless of the location of the data… “all” means “everything.” I hope this is becoming clearer. Everything would include real evidence in real time if the Russians actually hacked the DNC. There are only two options. Either the NSA has the evidence and is not releasing it. Or the NSA does not have the evidence because it did not happen. https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

Fact #3: Understand the True Power of the Dark Side
Not only does the scale of the NSA hacking program reach nearly every computer in every corner of the globe, but the scope or power of what the NSA is capable of doing to each of those computers is truly frightening. Jacob Applebaum is a security expert and developer of the TOR router. Jacob was originally from the University of Washington in Seattle. But he was forced to move to Germany in order to escape NSA persecution. Sadly, Jacob is still being harassed by government agents even in Germany. Jacob is one of only a few people in the world who was given access to the Snowden documents. After spending months reviewing these documents, Jacob stated that **the power of the NSA is “worse than your worst nightmare.”** I want to encourage anyone who doubts the NSA capabilities to watch this 60 minute talk by Jacob Applebaum. https://www.youtube.com/watch?v=b0w36GAyZIA

The above video may be one of the most important videos every posted on Youtube as Jacob goes into great detail about several NSA hacking programs and includes images from NSA training manuals to confirm that what he is saying is true. Please watch this video before proceeding with this article. It will help you better understand what we are going to cover and reduce the number of folks emailing us and telling us that what we are saying is not possible. What we are about to say is not only possible – but thanks to Edward Snowden, it is well documented. As just one example, the NSA can and does deploy malware by sending out spam emails that trick targets into clicking a malicious link. Once activated, a "back-door implant" infects their computers within eight seconds. https://theintercept.com/document/2014/03/12/nsa-phishing-tactics-man-middle-attacks/

According to one NSA presentation **"If we can get the target to visit us in some sort of web browser, we can probably own them."** Here is a slide from a top secret NSA program called the FOXACID Quantum exploit which according to the NSA has a success rate 80 times greater than a normal email spamming technique. The presentation goes on to say that folks who use either a Windows or Apple computer have a "100% chance" of the hack being successful. The only protection from NSA hacks is to use Linux servers and computers – a topic we will come back to later.



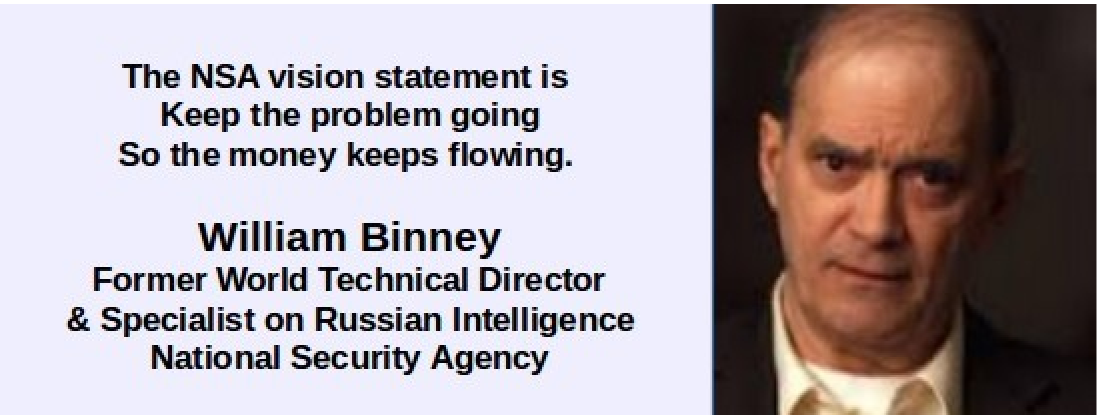
- Bottom line – if we can get the target to visit us in some sort of web browser, we can probably own them. The only limitation is the "how"

TOP SECRET//COMINT//NOFORN

Wikileaks has said that it did not get its information from Russia, Craig Murray, a former Ambassador, said he met with the leaker and it was not a Russian. On the other hand, the NSA has almost unlimited power to hack any group. The purpose of this report is to provide evidence clarifying this point. The NSA has the ability to automatically record the exact time and action of every computer in order to create a complete record of all attacks. So if the Russians did in fact hack the DNC, the NSA would have evidence of the hack. The NSA could release this evidence to the public without compromising a single source or a single secret.

Former NSA lead administrator William Binney concurs. He stated that if the Russians really did hack the Democratic Party server, the NSA would certainly have real evidence. Here is his quote from a December 29 2016 article by Glenn Greenwald:

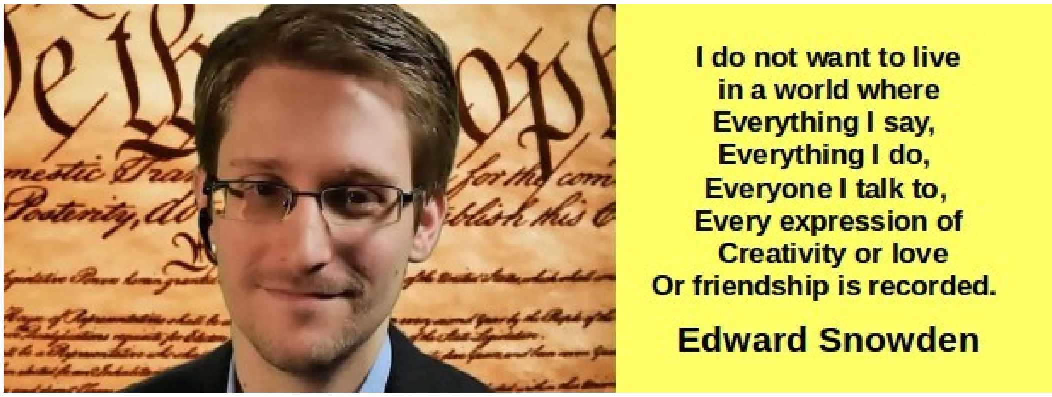
"The bottom line is that the NSA would know where and how any "hacked" emails from the DNC, HRC or any other servers were routed through the network. This process can sometimes require a closer look into the routing to sort out intermediate clients, but in the end sender and recipient can be traced across the network."
https://theintercept.com/2016/12/29/top-secret-snowden-document-reveals-what-the-nsa-knew-about-previous-russian-hacking/



The NSA vision statement is
Keep the problem going
So the money keeps flowing.

William Binney
Former World Technical Director
& Specialist on Russian Intelligence
National Security Agency

Edward Snowden not only confirmed that the NSA has this ability to unravel proxy servers – but that he himself used an NSA program called XKEYSCORE to get access. https://theintercept.com/2016/07/26/russian-intelligence-hack-dnc-nsa-know-snowden-says/



I do not want to live
in a world where
Everything I say,
Everything I do,
Everyone I talk to,
Every expression of
Creativity or love
Or friendship is recorded.

Edward Snowden

Pay close attention to what William Binney said about "routing to sort intermediate clients." What he is talking about is IP or Internet Protocol Addresses. Some who read our previous article claimed that IP addresses do not mean much because they can by bounced through proxies or intermediate IP addresses. These proxies may stop you and I from finding out who is really doing the hacking. But they do not stop the NSA. Both Snowden and Binney have confirmed that the NSA has a way to get past these proxies. This is easy for me to accept because I have spent several years studying the NSA. But the general public seems to have no idea what kind of power the NSA really has. Once you truly understand what the NSA is capable of, then you also understand that **the fact that the NSA has not released this evidence is a strong indication that this evidence of Russian hacking simply does not exist.**

Fact #4: Our Government is not always honest with us

This brings us to the next claim that our government agencies cannot possibly be lying to us. If our government says there is evidence of Russian hacking, we ought to believe our government even though they have failed to provide any evidence to back up this claim. Such a misplaced faith in government overlooks three important facts.

First, these same government agencies lied to us about the Weapons of Mass Deception that caused us to go to war in Iraq in 2003.

YOU WANT PROOF?
THIS TEST TUBE CONTAINS AN ARMY OF RUSSIAN HACKERS. DO YOU REALLY THINK WE'D START A WAR UNDER FALSE PRETENSES?

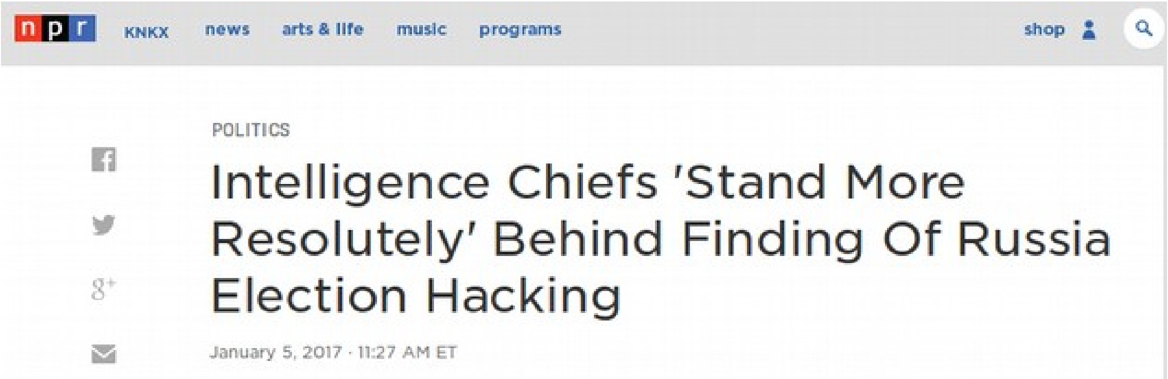
Second, these same government agents also lied to Congress when Congress asked them about their programs of mass surveillance in March 2013. In June 2013, after Snowden provided evidence of mass surveillance, Clapper was forced to admit that he had lied to Congress even though he was under oath to tell them the truth.

MEET JAMES CLAPPER.
HE IS BARACK OBAMA'S
DIRECTOR OF NATIONAL INTELLIGENCE.
IN MARCH, HE WAS ASKED DIRECTLY BY CONGRESS...
DOES THE NSA COLLECT "ANY TYPE OF DATA AT ALL ON MILLIONS OR HUNDREDS OF MILLIONS OF AMERICANS?"
HIS RESPONSE: "NO SIR... IT DOES NOT."

Third, these same government agents repeatedly promised us they would provide us with real evidence of Russian hacking by the end of 2016. They did give us the DHS/FBI “Grizzly Steppe” report. But there was no real evidence of Russian hacking anywhere in the report.

This makes these government agents three time losers. The government now claims that they will release yet another report in January 2017 with evidence that the Russians hacked the DNC. But given all the times we have been lied to in the past, how many times does our government have to lie to the American people before the American people will learn not to trust their government?

Fact #5: The Main Stream Media is not always honest with us.
We will provide two recent examples. First, the current “Sound Bite” that the “Russians Hacked the Election” is Deeply Deceptive. The main stream media has repeated thousands of times that the “Russians hacked the election.” Here is a recent deceptive headline from NPR:

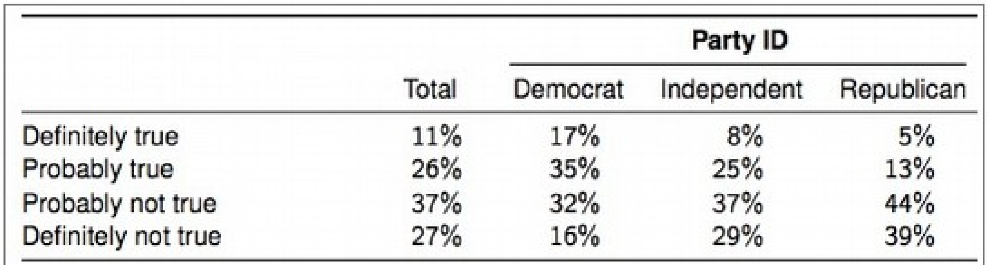


POLITICS

Intelligence Chiefs 'Stand More Resolutely' Behind Finding Of Russia Election Hacking

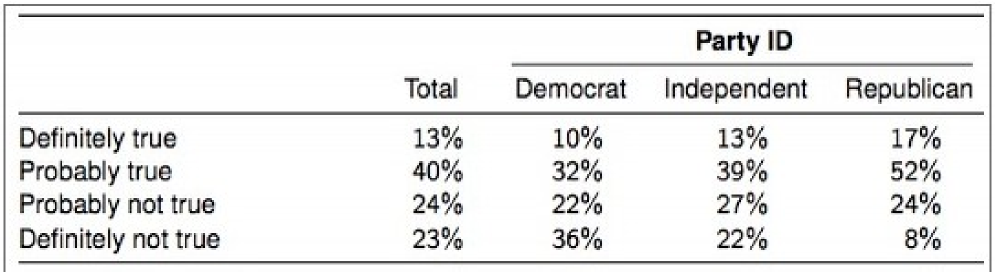
January 5, 2017 · 11:27 AM ET

Hopefully, you are smart enough to know that there has never been a finding that Russia hacked the election. It is not even being alleged that Russia hacked the election. The real allegation is that the **Russians hacked the DNC servers** and then handed the emails to Wikileaks who published them. Because of their embarrassing content, some voters decided to vote for Trump which cost Clinton the election. However, this is not what many Americans think when they are told over and over again that the Russians hacked the election. **What many Americans think is that Russia hacked the American voting machines.** In fact, in a December 2016 poll, half of all Democrats believe that Russians tampered with the voting machines – even though President Obama has repeatedly stated that there is no evidence that Russia hacked any voting machines. Here is the breakdown including Independent voters.



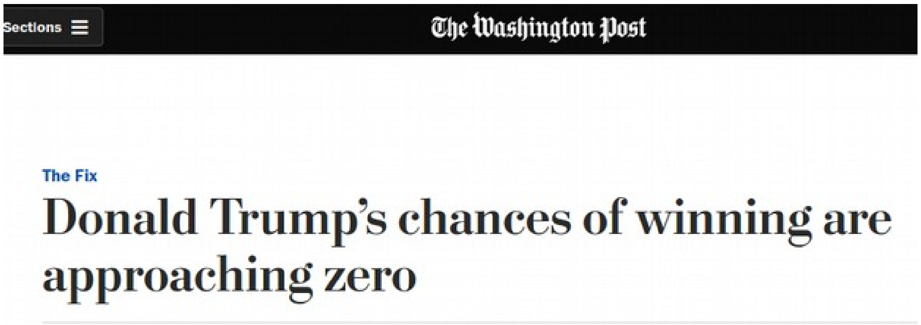
		Party ID		
	Total	Democrat	Independent	Republican
Definitely true	11%	17%	8%	5%
Probably true	26%	35%	25%	13%
Probably not true	37%	32%	37%	44%
Definitely not true	27%	16%	29%	39%

The same poll found that over half of all Americans still think that Iraq had weapons of mass destruction even though none were ever found. https://today.yougov.com/news/2016/12/27/belief-conspiracies-largely-depends-political-iden/



		Party ID		
	Total	Democrat	Independent	Republican
Definitely true	13%	10%	13%	17%
Probably true	40%	32%	39%	52%
Probably not true	24%	22%	27%	24%
Definitely not true	23%	36%	22%	8%

The second example was the reporting right up until the day of the election was that Clinton was going to win in a landslide. Here are just some of the headlines from Election Day, Tuesday November 8, 2016:

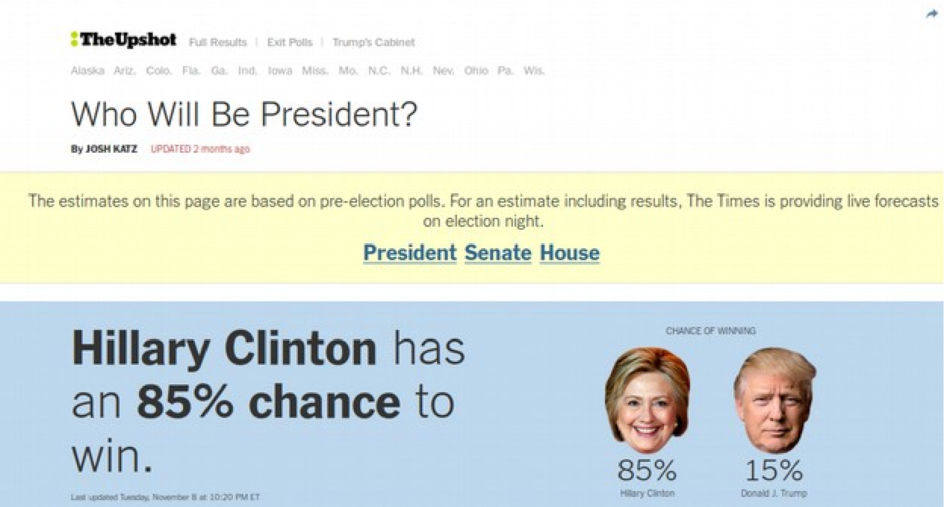


Sections ☰ The Washington Post

The Fix

Donald Trump's chances of winning are approaching zero

https://www.washingtonpost.com/news/the-fix/wp/2016/10/24/donald-trumps-chances-of-winning-are-approaching-zero/?utm_term=.28ad854b10cc



TheUpshot Full Results | Exit Polls | Trump's Cabinet

Alaska Ariz. Colo. Fla. Ga. Ind. Iowa Miss. Mo. N.C. N.H. Nev. Ohio Pa. Wis.

Who Will Be President?

By JOSH KATZ UPDATED 2 months ago

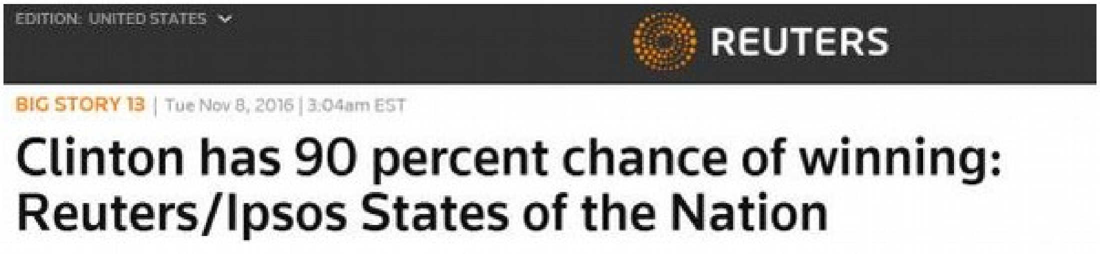
The estimates on this page are based on pre-election polls. For an estimate including results, The Times is providing live forecasts on election night.

President Senate House

Hillary Clinton has an **85% chance** to win.

Last updated Tuesday, November 8 at 10:20 PM ET

http://www.nytimes.com/interactive/2016/upshot/presidential-polls-forecast.html



EDITION: UNITED STATES REUTERS

BIG STORY 13 | Tue Nov 8, 2016 | 3:04am EST

Clinton has 90 percent chance of winning: Reuters/Ipsos States of the Nation

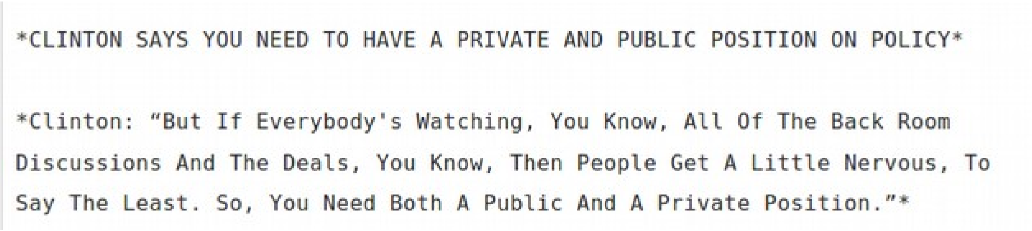
The lesson here is to stop believing everything we are told by the main stream media.

The Real Issue is not the Russians, It is a lack of Honesty

Information released by Wikileaks may have cast Clinton in a negative light. But that was because the majority of independent swing voters already did not trust her as was shown in polls going all the way back to 2015. There were two sets of leaks. One in July 2016 and the other in October 2016.

The July emails confirmed that the former chair of the Democratic Party did in fact collude against Bernie Sanders to prevent a fair primary. When the Chair of the DNC resigned, she was immediately hired by Clinton showing a complete lack of understanding for the perception that the election was “rigged.” This led to the walk out of Sanders supporters at the Democratic Party election. Was this the fault of Wikileaks for revealing the collusion or the fault of Clinton for putting this dishonest person on her campaign team?

The October releases included a Clinton speech to Goldman Sachs explaining why she had a public position opposing cutting Social Security but a private position supporting cutting Social Security.. reassuring them that she had both a public and private position:



CLINTON SAYS YOU NEED TO HAVE A PRIVATE AND PUBLIC POSITION ON POLICY

Clinton: “But If Everybody's Watching, You Know, All Of The Back Room Discussions And The Deals, You Know, Then People Get A Little Nervous, To Say The Least. So, You Need Both A Public And A Private Position.”

Many independent swing voters already did not trust Hillary. This single release may have cost her the election. But should Wikileaks be blamed for revealing the truth or the Democrats be blamed for nominating such a two faced candidate?
https://wikileaks.org/podesta-emails/emailid/927

Then there was what Clinton told a Brazilian bank group in 2013, “We have to resist, protectionism, other kinds of barriers to market access.” The fact that this statement became known after she had publicly opposed the TPP Trade agreement but then had chosen a Vice Presidential Candidate strongly in favor of the TPP Trade agreement likely cost Clinton a lot of swing votes in the Rust Belt states that determined the election. But it was not Wikileaks that chose a Pro TPP VP, it was Clinton.

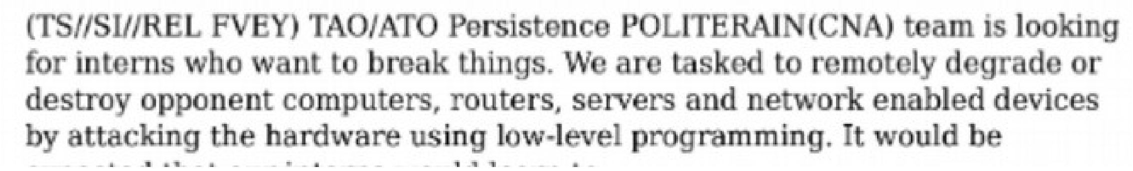
Clinton also said in a June 2013 speech, she believed the United States should intervene in Syria but **as "covertly as is possible**." She also advocated for enforcing a Syrian No Fly Zone that Generals had said would lead to direct conflict with Russia. There was also Bill Clinton getting a million dollar check from an oil baron, while Hillary told bankers that banks got too much blame for their role in the financial crisis. Clinton also said the Dodd-Frank Act had to be passed "for political reasons” and that she thought bankers were best suited to regulate themselves, since "the people that know the industry better than anybody are the people who work in the industry."

Trying to change the focus from what happened in the election by using even more lies to shift the blame to the Russians may be politically easy in the short run. But it will severely harm the American political process in the long run. Nevertheless, it is clear that the main stream media has launched a campaign designed to whip up fear and hysteria in the American people and is trying to turn Russia into some kind of bogey man who is out to get us. The truth is just the opposite. The scary monster is right here in the US and it is called the NSA. Next is our timeline of events leading up to the DNC hack.

Part 1: Evolution of Cyber Warfare Weapons 2007 to 2015

In the late 1990’s, three federal judges ruled that Microsoft was a monopoly that had engaged in price fixing in violation of the Sherman Anti-trust Act. To maintain their lucrative monopoly over computer operating systems, Microsoft made a “deal with the devil” by allowing the NSA to have an open back door into every Microsoft Windows computer. This back door was enabled by placing the Explorer web browser inside of the Windows Operating system. The downside of allowing the NSA access to every Windows computer was that it also allowed hackers access to Windows computers. This back door is still present today – meaning that it is impossible to secure any Windows computer. But in 2007, the NSA launched a new program called **PRISM** that was about to make this dangerous situation much worse.

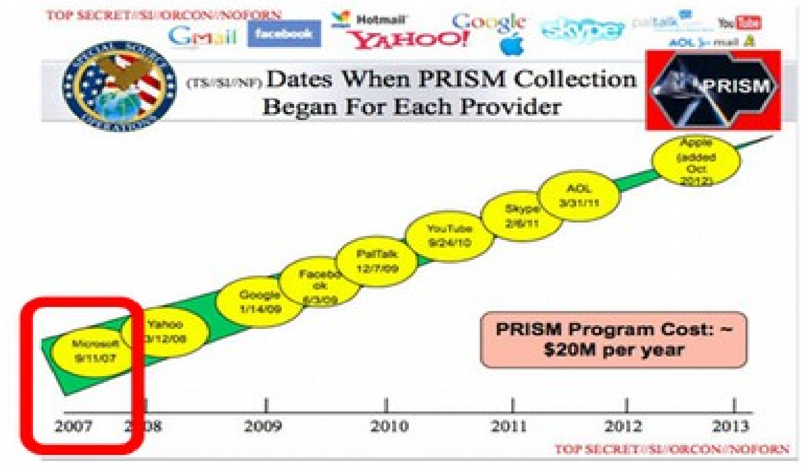
2007: NSA expands its program to actively recruit and train computer hackers.
One of the documents exposed by Snowden in 2013 was a 2007 NSA job posting document in which the NSA actively solicited hackers to go to work for the NSA. The trainees will be taught how to “develop an attackers mindset.” Note that the NSA goal is not merely to monitor computers but to remotely destroy them.
http://www.spiegel.de/media/media-35661.pdf



(TS//SI//REL FVEY) TAO/ATO Persistence POLITERAIN(CNA) team is looking for interns who want to break things. We are tasked to remotely degrade or destroy opponent computers, routers, servers and network enabled devices by attacking the hardware using low-level programming. It would be

September 1, 2007: The NSA begins the Prism Collection Program.

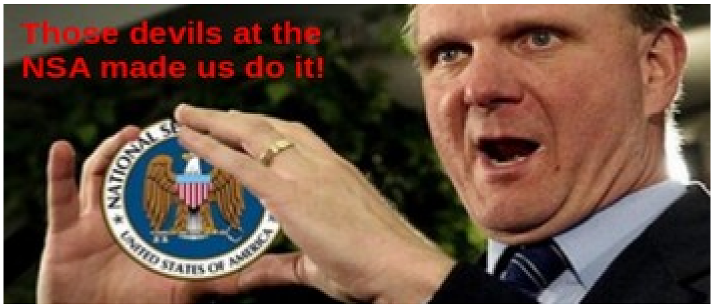
As confirmed in documents provided by Edward Snowden in 2013, the NSA started the Prism Data Collection Program to enlist major US corporations to help with mass surveillance in 2007. Its first recruit was Microsoft in September 2007.



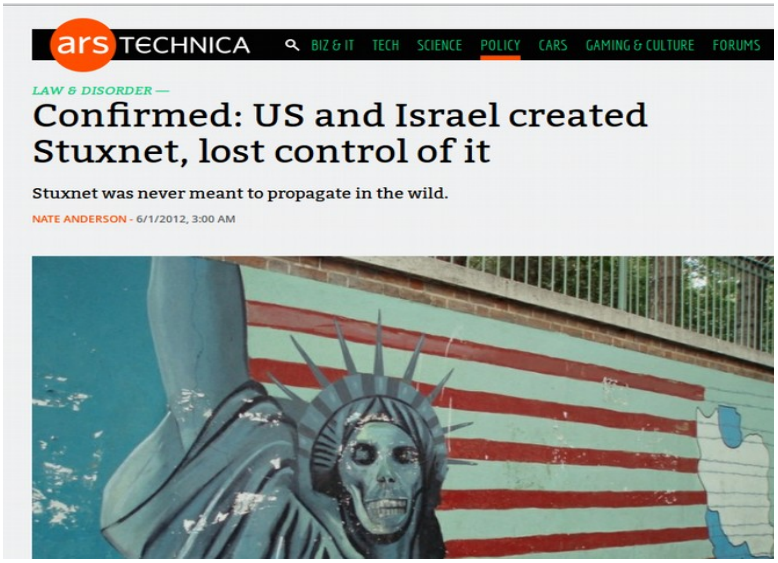
This was also the time that the startup program for all computers except Chromebooks began to change from the simple BIOS program to a complex encrypted program called UEFI. This means that not only is the operating system insecure but so is the startup program as both call back to Microsoft and the NSA using hidden backdoors.

Chromebooks use a much safer startup program called Coreboot that does not have hidden backdoors. I began researching these backdoors in 2010 in order to understand a virus called the Flame virus. I discovered that these backdoors were being used to transmit cyber weapons such as Stuxnet and Flame. I eventually learned that these cyber weapons were created by the NSA.

September 2009: Researching the history of the flame virus led to even more disturbing questions about the relationship between Microsoft and the NSA. Several newspaper reports confirmed that in 2009, Microsoft played a key role in the NSA attack on Iranian Nuclear and Oil Facilities via the development of the Stuxnet and Flame super viruses.



The Stuxnet - Flame viruses soon escaped “into the wild” and began crashing not just Iranian oil facilities but lots of other oil facilities around the world. http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/



LAW & DISORDER —

Confirmed: US and Israel created Stuxnet, lost control of it

Stuxnet was never meant to propagate in the wild.

NATE ANDERSON - 6/1/2012, 3:00 AM

“Flame was designed to masquerade as a routine Microsoft Update.”
http://articles.washingtonpost.com/2012-06-19/world/35460741_1_stuxnet-computer-virus-malware

Here is a 2 minute video about the dangers of the Stuxnet virus. https://www.youtube.com/watch?v=wliTpRLTySU

April 20 2010: The Flame virus caused the BP Oil Disaster
In the summer of 2010, while researching the flame virus, I discovered evidence that the Flame virus led directly to the BP Gulf Oil Spill – the worse environmental disaster in the history of the world. This is something the American people have never been told.

In the weeks before the BP disaster, the Windows computer system froze leading to a lack of control over safety equipment. Symptoms indicate the Flame virus caused the computer crash which led to the explosion.

July 23, 2010: At a government hearing to determine the cause of the gulf oil spill, the oil rig's chief electronic technician, Mike Williams – who miraculously survived the explosion – described the events leading up to the disaster. The full details of his testimony are listed on the following web page.
http://techrights.org/2010/10/12/deepwater-update/

Mike Williams testimony sounded exactly like what happens today whenever a Windows computer is attacked by the Flame Virus. According to Mr. Williams, for months, the computer system on the ill fated BP oil rig had been locking up, producing what the crew called the “blue screen of death.” (Note: The Blue Screen of Death most commonly occurs on Windows computers after a faulty update). When the computers were down, the safety equipment did not work and the well could not be monitored. Five weeks before the explosion, in March 2010, Mike Williams had been sent to the oil rig to fix the computer problem. Mike testified, “The computer screen would just turn blue. You'd have no data coming through."

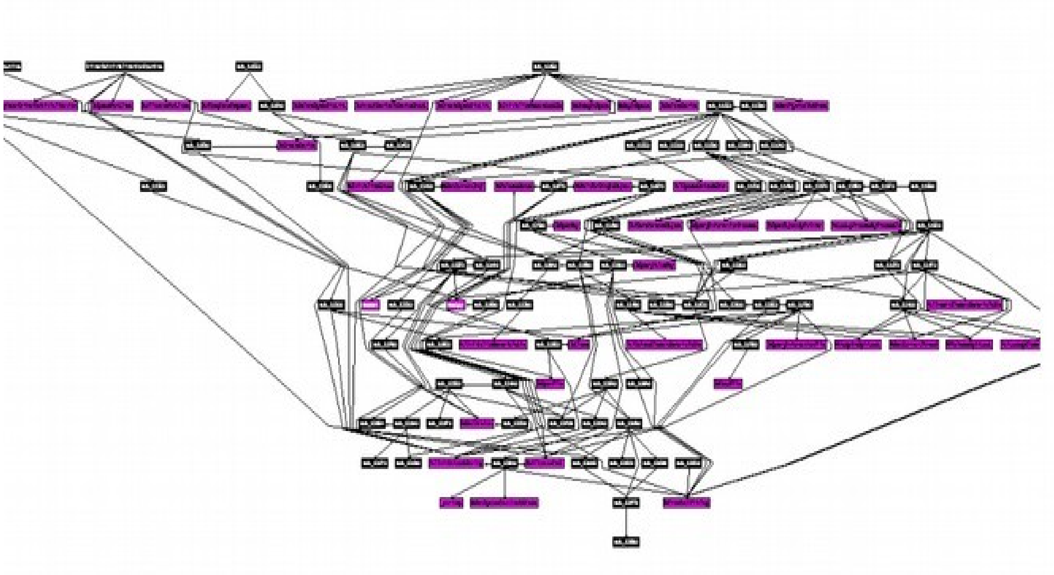
Mike explained that with the computer frozen, the drillers did not have access to crucial data about what was going on in the well. Williams described the Windows computer system as “a very unstable platform” and “bad software” that was the root cause of most of the drilling problems. This buggy Windows based control system left drillers blind when it crashed daily and was responsible for safety system bypasses that eventually destroyed the well seal and led to the explosion. On page 42 of the hearing transcript, Mike Williams stated:

> **“For three to four months we’ve had problems with this computer simply locking up. [sometimes it was a blue screen, sometimes a frozen display] … We had ordered replacement hard drives from the manufacturer. We had actually ordered an entire new system, new computers, new servers, new everything to upgrade it from the very obsolete operating system that it was using.”** http://techrights.org/2010/10/12/deepwater-update/

Thus, according to Mr. Williams, the computer problems began in January 2010. Between the manufacturer and the rig, they could not get the bugs worked out of the new operating system. They couldn't get the old software to run correctly on the new operating system. Microsoft Updates – instead of fixing the problem actually made the problems worse. This was an important clue that their computer system had been infected with the Flame super bug. Who would create such a vicious virus and why? I was not able to connect the Flame virus to the Stuxnet virus and the NSA until a shocking article was published in June 2012.

June 1, 2012: James Risen, a reporter with the NEW York Times, interviewed one of the US generals associated with the Stuxnet project and posted an article where this general described the Stuxnet deployment against Iran in detail. If you are not familiar with the NSA Stuxnet attack on Iran then please read the following article. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all

2010 to 2014: NSA greatly expands their cyber warfare arsenal.
Stuxnet's was not the only cyber weapon created by the NSA. The NSA also created Flame, Gauss and Duqu. Each of these has coding patterns related to previous programs including using many of the same modules, structures and processes. These severely dangerous and harmful programs are very complex. Below is a diagram of code modules in the Duqu Driver. This is only one of more than 100 components that make up the Duqu 2.0 (2015) virus.
https://www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf



Here are a couple of links that describe the evolution of NSA cyber warfare weapons:
https://cdn.securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf
https://www.concise-courses.com/stuxnet-flame-gauss-duqu/

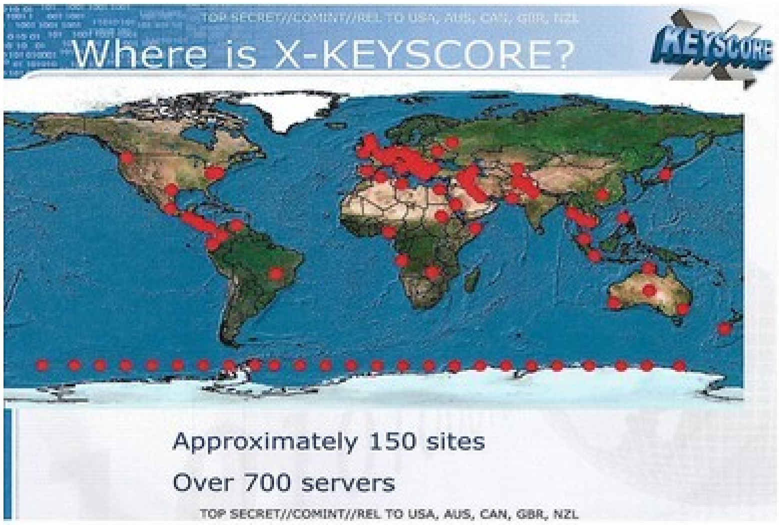
June 6, 2013: Snowden Provides Documents Confirming the Power of the NSA

I was about to publish a book called **"Free Yourself from Microsoft and the NSA"** describing the dangers of the NSA Flame Virus and Stuxnet virus as well as the dangers of open back doors in the Windows operating system in June 2013 – a book I had worked on for more than a year. Here is a link to this book if you would like to read it. https://freeyourselffrommicrosoftandthensa.org/

I realized people would think I was crazy for claiming that the NSA had produced these super weapons. But I was going to publish it anyway. Then, Edward Snowden provides thousands of documents to reporters confirming the hidden power of the NSA. If my prior research had peaked behind the curtain, the Snowden documents blew the lid off the entire NSA operation.
http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data

This is the truth. This is what is happening. This is an architecture of oppression. I don't want to live in a society that does these sorts of things. Edward Snowden June 6 2013

July 13, 2013: Glenn Greenwald explains how the NSA downloads documents from Windows computers. He released documents provided by Edward Snowden on a top secret NSA program called Xkeyscore (aka XKS) which is used to steal and store documents from your Windows computer. Xkeyscore is used through over 700 servers at 150 sites around the world.
http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Where is X-KEYSCORE?

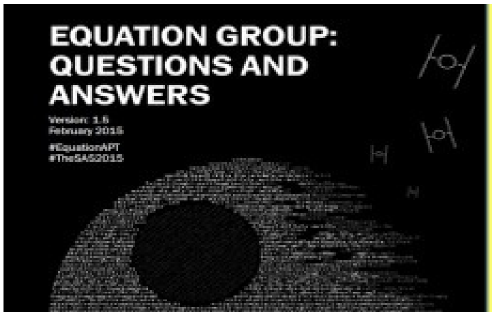
Approximately 150 sites

Over 700 servers

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

February 16, 2015 Kaspersky exposed the Equation Group

Independently from Snowden, a computer security firm called Kaspersky had been analyzing the Flame and Stuxnet cyber weapons. In 2013 and 2014, they published several reports documenting how these super weapons worked. Then in February 2015, they published a report linking them all together. Kaspersky publishes a report on the “Death Star of the Malware Galaxy” which it called the Equation Group (which we know is the NSA). The relationship of Stuxnet to other NSA cyber weapons was confirmed in this detailed analysis.
https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/
https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf



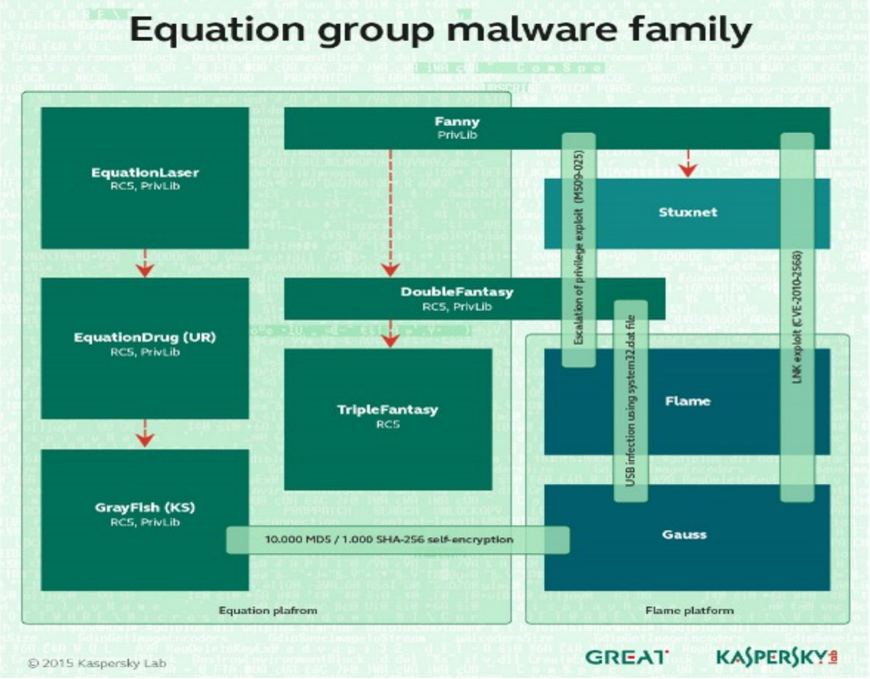
EQUATION GROUP: QUESTIONS AND ANSWERS

Version: 1.5
February 2015

#EquationAPT
#TheSAS2015

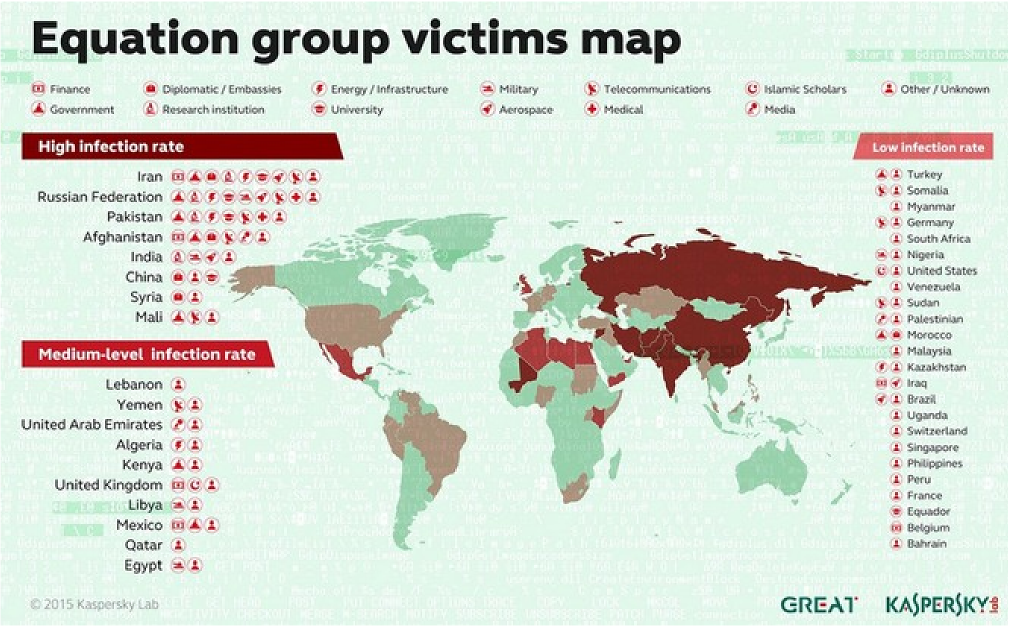
Kaspersky refused to name
Who the Equation Group was
or where they were from.
But because the Equation Group
was responsible for
the cyber attack on Iran
we can be certain that the Equation Group
is in fact the NSA.

The Kaspersky researchers described a group they called the **Equation group** which was infecting computers and websites all over the planet. The report noted that the techniques being used were linked to techniques and malware programs previously developed and used by the NSA including the Flame and Stuxnet viruses which the US used to attack Iranian computers. Here is their diagram of the relationships between the various Equation Group cyber weapons. Note that Stuxnet, Flame and Gauss are all directly related:



Here is a quote from their 44 page report: “All the malware we have collected so far is designed to work on Microsoft’s Windows operating system. The malware callbacks are consistent with the DOUBLEFANTASY schema, which normally injects into the system browser (for instance, Internet Explorer on Windows)… The Equation group uses a vast infrastructure that **includes more than 300 domains and more than 100 servers.”**

Here is a map of all of the victims of the Equation Group according to Kaspersky (Note: this map is not complete as I personally know of victims in countries not on this map). Clearly the primary targets or victims of the Equation group are China and Russia. However, we should note that the Equation Group also targets computers in the US:



April 30, 2013: The NSA/Equation Group Posts a Training Video on Youtube
Having spent years following this evolution of NSA cyber warfare weapons, it is apparent to me that tens of thousands of hackers have been trained by the NSA. Here is a 26 minute Youtube video of the NSA “Red Cell” teaching young military recruits how to hack computers. https://www.youtube.com/watch?v=HnnvVnsDCGw

Most of these hackers eventually leave the US military and then work for thousands of fake cyber security consulting firms funded directly or indirectly by the NSA. Thanks to the revelations of Edward Snowden, we also know the NSA has a network of hundreds of hacking servers in more than one hundred countries around the world.

February 28, 2015: Kaspersky links Cozy Bear to Cozy Duke.

Kaspersky for several years had been the world leader in documenting the hacking activities of the Equation Group, which was responsible for cyber attacks on servers in Iran. These cyber weapons included Stuxnet, Flame, Gauss and Duqu. Kaspersky does not link Cozy Bear or the Equation group to any nation-state because they have a policy of “not getting involved in politics.” But others will later falsely claim that Kaspersky said that Cozy Bear was linked to the Russian government. We will provide quotes from the actual Kaspersky reports which imply that Cozy Bear was not Russian but rather the NSA. Here is a link to their February 28 2013 report on Cozy Duke aka Cozy Bear. https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf

Cozy Bear aka Cozy Duke was used not just to attack the US but many other countries including Russia

Here is a list of the countries that had been targeted by the Duke virus.
“Researchers found 59 unique victims in the following 23 countries: Belgium, Brazil, Bulgaria, Czech Republic, Georgia, Germany, Hungary, Ireland, Israel, Japan, Latvia, Lebanon, Lithuania, Montenegro, Portugal, Romania, Russian Federation, Slovenia, Spain, Turkey, Ukraine, United Kingdom and United States.”

So if Russia really was the source of the Duke virus, then we have to believe that the Russian Federation used this virus to attack itself. Alternately if we want to conclude that the US was the nation that built the Duke virus then we have to believe that the US attacked itself. These are not equal assumptions because, thanks to Edward Snowden, **there is plenty of evidence of the NSA attacking victims in the US.** We know they do this. It is part of their motto to hack everything.

June 10 2015: Kaspersky links Duqu to the Duqu 2 cyber weapon.

In June 2015 Kaspersky admitted that they had been hacked by a new cyber weapon they called Duqu 2.0. Here is a quote from Kaspersky: “Since these have never been made public and considering the main interest appears to have remained the same, we conclude the attackers behind Duqu and Duqu 2.0 are the same.” https://cdn.securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

So Duqu and Duqu 2 were made by the same group. But how do we know these are made by the same group that made Stuxnet, Flame and Gauss? Here we have several sources. First, we have the Kaspersky group who has done detailed analysis of all of these viruses breaking the code and structure of each down line by line. Kaspersky has written hundreds of pages of reports on this topic and they have repeatedly concluded that these viruses were all written by the same nation-state.

Another source is the NSA documents released by Snowden. In these documents are NSA presentations in which they discuss Stuxnet as being one of their “implants.”
https://theintercept.com/2014/11/12/stuxnet/

SON OF STUXNET

The Digital Hunt for Duqu, a Dangerous and Cunning U.S.-Israeli Spy Virus

The June 2015 Kaspersky report confirmed several more Stuxnet like “patterns” of the Cozy Duke hackers:

#1 Cozy Duke uses extremely expensive and rare Zero Day Exploits
Zero day exploits are security holes in software such as Microsoft Windows that not even Microsoft is aware of. The Dukes cyber weapon uses Zero Day attacks just like the Duqu Stuxnet and Flame viruses. In fact, NSA viruses often use a dozen or more zero day exploits.

#2 Cozy Duke was written with Windows Programs by Windows programmers common in the US
Analysis of the Cozy Duke code confirms that it was written using Windows programs. While it is possible that Russian hackers could use Windows computers and programs to write the virus, it is much more likely that they would use Linux computers and programs for security reasons (after all, they know how insecure Windows is and how easy it would be to be hacked by the NSA if they were using Windows programs). By contrast, the NSA often uses Windows programs and programmers because they have a direct relationship with Microsoft. Note that the Equation group cyber weapons were also all written using Windows programs.

#3 Cozy Duke use in the Ukraine declined after US Puppets Took Over Ukraine
Here is a quote from one of the 2015 reports analyzing Cozy Duke:
“Contrary to what might be assumed, we have actually observed a drop instead of an increase in Ukraine-related campaigns from the Dukes following the country’s political crisis. This is in stark contrast to some other suspected Russian threat actors (such as Operation Pawn Storm [10]) who appear to have increased their targeting of Ukraine following the crisis.”

In other words, Pawn Storm saw its use go up after the US CIA backed group took over Ukraine while a much more powerful weapon called Cozy Duke was used less. The Russians would have no reason to use their most powerful cyber weapon less after the CIA backed coup in Ukraine. The only ones with this kind of motive would be the NSA.
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

#4 The Cozy Bear Referral Servers are in Panama, France, Germany, the US and Turkey

After infecting computers and servers, Cozy Bear calls home to the mother ship. According to the Kaspersky analysis, Cozy Bear is programmed to contact specific servers in Panama, France, Germany, the US and Turkey. These five countries all have a strong NSA CIA presence. None of these countries has a close relationship to Russia – especially not in 2014. Understanding that IP addresses can be faked, these are the IP addresses of the mother ship as provided by Kaspersky:

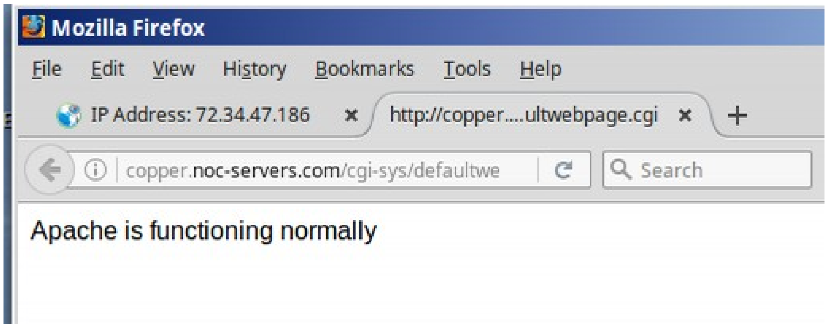
200.63.46.23
95.128.72.24
72.34.47.186
188.40.99.143
85.95.236.114

Here is a review of these IP addresses using http://whatismyipaddress.com

200.63.46.23 is a server owned by **Panamaserver.com**. They are listed as a clean server meaning there have been no reports of them attacking people. This means that people were unaware of who was attacking them and where the attackers were located.

95.128.72.24 is a clean server owned by **cl-turbo.celeo.net** in Paris France. This domain name has no apparent services so how does it make money and stay in business?

72.34.47.186 is a clean server owned by I**HNetworks LLC** in Los Angeles CA. They use the domain name **copper.noc-servers.com**. This domain name has no apparent services. So how does it make money and stay in business? I was able to confirm that this server is using a Linux Apache server program and is also using Cpanel. But that was as far as I could get. Here is a screen shot of this URL:


Mozilla Firefox
File Edit View History Bookmarks Tools Help
IP Address: 72.34.47.186
http://copper....ultwebpage.cgi
copper.noc-servers.com/cgi-sys/defaultwe
Search

Apache is functioning normally

IHNetworks LLC appears to be a web hosting company that purchased a Texas based web hosting company called Eleven2 in 2012 but continued to use the user name of the former company apparently to hide the fact that the company was bought.
http://www.webhostingtalk.com/showthread.php?t=1431081

IHNetwork hosts about 4,000 domain names (most from Eleven2). Most of these domain names have very low traffic. Even at $100 per domain per year, this is only $400,000 annually which would barely pay for the server much less the staff. Here is a link to all of the domain names hosted by IHNetworks and their current traffic levels.
https://w3bin.com/hoster/77

Yet despite this fact, IHNetworks claims on their home page to have servers and data centers located around the world! http://ihnetworks.com/

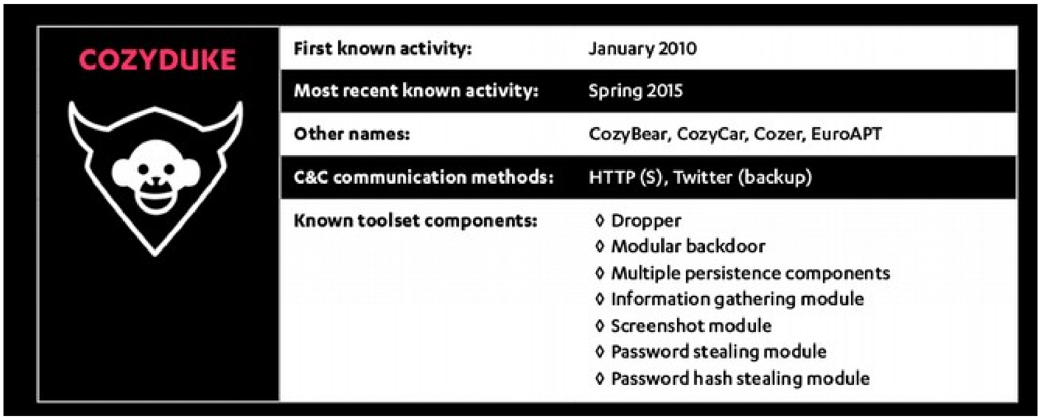
Here is a screen shot of all of the five web hosts that they have bought:

So where is this company getting all of the money to buy these web hosts and pay for servers and data centers all around the world? This company appears to have an unlimited amount of money but its known income is only $400,000 per year! Also, exactly how is it related to Cozy Bear given that it is highly unlikely Cozy Bear would want to use servers located in the US and subject to US laws if Cozy Bear was really from Russia.

188.40.99.143 is a clean corporate server located in Germany. The Internet Service Provider is Hetzner Online AG. This one appears to be a real web hosting company that has been in existence since 1997. Perhaps the NSA just has an account here.

85.95.236.114 is a clean broadband server in Turkey. Just about anyone can use a broadband server so there is no real way to research this connection other than to confirm that the IP address is actually located in Turkey (which I did).

#5 Cozy Bear aka Cozy Duke uses a Twitter account to call the mother ship
The primary method that Twitter uses to communicate with the mother ship is a Twitter handle that uses common phrases about the weather. Should the Twitter account be taken down, Cozy Bear has a backup communication method that uses Google. Given the known relationships between Google, Twitter and the NSA, it is unlikely that Russian hackers would use either of these corporations as their primary means of communicating between their hacking tools and the Home servers. Here is a graphic of Cozy Duke aka Cozy Bear from Kaspersky confirming it uses Twitter to communicate.



COZYDUKE

First known activity:	January 2010
Most recent known activity:	Spring 2015
Other names:	CozyBear, CozyCar, Cozer, EuroAPT
C&C communication methods:	HTTP (S), Twitter (backup)
Known toolset components:	◊ Dropper ◊ Modular backdoor ◊ Multiple persistence components ◊ Information gathering module ◊ Screenshot module ◊ Password stealing module ◊ Password hash stealing module

#6 Fancy Bear also used a US Registrar for one of their hacking domain names.
One of the ways Fancy Bear gains access to computers and servers is by fooling folks to click on a PDF link that activates the cyber weapon. This is linked to a domain name called PDFRegistry.net. Here is the ownership status of this domain name:

Domain Name: PDFREGISTRY.NET
Registrar: 1&1 INTERNET SE
Sponsoring Registrar IANA ID: 83
Whois Server: whois.1and1.com
Referral URL: http://registrar.1and1.info
Name Server: NS-US.1AND1-DNS.COM

1 and 1 is a major US domain name registrar. The domain name was created on April 12 2015, was updated on September 30 2016 and is paid through 2017. Here is the problem with the Russians using a US domain registrar: current US laws allow the FBI nearly instant access to any and all US servers. This should not be allowed. But it is allowed which is why I recommend that website owners host their domain names on servers that are outside of the US. Certainly the Russians are fully aware of the danger of using US web hosts in terms of instant FBI access without even seeking a warrant from a judge. There is no way Russians are going to use US registrars or web hosts for their secret cyber weapon hacking programs. However, the NSA would have nothing to fear from using US servers as the NSA and FBI are best friends.

August, 2015 Fancy Bear used a fake domain name for the Electronic Freedom Foundation to fool folks into downloading their cyber weapons.
Fancy Bear who would later use a DNC related fake domain name to attack folks in March 2016, also used an EFF fake domain name to hack people in August 2015. This is very relevant because one of the world’s biggest opponents of NSA mass hacking is the Electronic Freedom Foundation (EFF). This group has actually filed lawsuits against the NSA and has posted detailed articles explaining to people how they can use tools such as Linux to protect against NSA hacking attacks.

The real domain name for the EFF is **https://www.eff.org/**

EFF
ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD
HOME
ABOUT
OUR WORK
DEEPLINKS BLOG
PRESS ROOM
DEFENDING THE DIGITAL FUTURE:
2017

However the Fancy Bear Cyber weapon used the fake domain name **Electronicfrontierfoundation.org** to fool folks into downloading their cyber weapon. https://www.eff.org/deeplinks/2015/08/new-spear-phishing-campaign-pretends-be-eff

EFF has since purchased this domain name and redirected it to their real domain name in order to try to protect their clients. However, the malicious use of this fake domain name clearly is intended to harm the Electronic Freedom Foundation and those who trust the EFF. No rational person would believe that Russia would want to deliberately undermine one of the NSA's biggest opponents. But there is no doubt that the NSA would want to undermine the EFF and their supporters.

NSA learns how to cover their tracks to hide it is the source of most cyber weapons

To better understand the extreme lengths that the NSA goes to in order to confuse folks about its viruses, let's read a quote from page 43 of one of the most recent Kaspersky Duqu virus manuals: "In the case of Duqu, the attackers use multiple proxies and jumping points to mask their IP connections. This makes tracking an extremely complex problem. Additionally, the attackers have tried to **include several false flags throughout the code**, **designed to send researchers in the wrong direction.** For instance, one of the drivers contains the string "ugly.gorilla", which obviously refers to 9Wang Dong, a Chinese hacker believed to be associated with the APT1/Comment Crew. The usage of the Camellia cypher previously seen in APT1 samples is another false flag planted by the attackers to make researchers believe they are dealing with APT1 related malware. "
https://cdn.securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

In other words, the makers of Duqu (who we know are NSA coders) want us to think they are Chinese hackers when they are not. These NSA hackers even faked time stamps on their activities to make us believe they are operating in a Russian time zone when in fact they are operating in the US Eastern Time Zone.

September 15, 2015 Duqu 2 uses Easily faked time stamps

In June 2016, Crowdstrike issued a report claiming that Cozy Bear and Fancy Bear were Russian hackers. The source document for this claim was a September 15, 2015 report written by a computer security firm called F Secure.
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

This report mistakenly used easily faked time stamps as evidence that the Duke viruses were written by Russians. Here is a quote from the conclusion of the F Secure 2015 Report: "Attribution is always a difficult question, but attempting to answer it is important in understanding these types of threats and how to defend against them... The Dukes have consistently operated large-scale campaigns against high-profile targets...We therefore believe the Dukes to be a single, large, well-coordinated organization with clear separation of responsibilities and targets. This leaves us with the final question: which country? We are unable to conclusively prove responsibility of any specific country for the Dukes.

All of the available evidence however does in our opinion suggest that the group operates on behalf of the Russian Federation. **Kaspersky noted that based on the compilation timestamps,** the authors of the Duke malware appear to primarily work from Monday to Friday between the times of 6am and 4pm UTC+0 [11] . This corresponds to working hours between 9am and 7pm in the UTC+3 time zone, also known as Moscow Standard Time, which covers, among others, much of western Russia, including Moscow and St. Petersburg."

However, since we know the NSA has altered the time stamps on previous programs, it would be a simple matter for them to also alter the time stamps on Cozy Duke. Here is a quote from Kaspersky about why they never attribute any cyber weapon to any nation: "Cyber-spies can stage false-flag operations: the evidence we use to attempt to identify attackers includes timestamps, words in particular languages in the malware code, names or nicknames, and the geographical locations of the command-and-control servers used. But **such evidence is always circumstantial and can easily be forged.**" http://media.kaspersky.com/en/Duqu-2-0-Frequently-Asked-Questions.pdf

It is therefore possible to imagine that the time stamps on the Cozy Duke code are valid and that it was therefore written by Russians. However, such a naive claim ignores all of the other evidence – especially the fact that all the Cozy Duke "call home" server IP addresses are in the US or in countries friendly to the US - which leads to the conclusion that it was the NSA that wrote Cozy Duke. If we conclude that the NSA wrote Cozy Duke, then we must also conclude that it was the NSA and not Russia that hacked the DNC servers. Since the NSA motto is to hack everything, it should not surprise anyone that the NSA was hacking DNC servers – because the NSA hacks all servers.

All of the above was reported and known prior to the DNC hacker attacks. Now that we have a better understanding of how Cozy Bear and Fancy Bear work, and the fact that both are far more likely to be NSA cyber weapons than Russian cyber weapons, let's get back to the DNC hack.

Part 2 Details of the DNC Hack... July 2015 to May 2016

Reminder: APT stands for Advanced Persistent Threat. APT refers to a suspected government sponsored hacker. Fancy Bear is APT 28 and Cozy Bear is APT 29.

September 2015: Cozy Bear also known as Cozy Duke attacks DNC network.

In September 2015, a group called "Cozy Bear" attacked the DNC Server.

The attack was reported to the DNC by the FBI, but strangely, the DNC did nothing about it. Instead, the DNC claims they did not believe the person warning them was an FBI agent!

The timing of the first Cozy Bear attack on the DNC was first reported in the New York Times to be September 2015 with the FBI contacting the DNC almost immediately. http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

However, a report released on January 6, 2017 by the FBI called "Assessing Russian Activities and Intentions in Recent US Elections" states on page 2 that "In **July 2015**, Russian Intelligence gained access to the Democratic National Committee (DNC) networks and maintained that access until at least **June 2016**."
https://www.dni.gov/files/documents/ICA_2017_01.pdf

We will accept the New York Times version of events and dismiss the 2017 FBI report for several reasons:

#1 If the hack of the DNC began in July 2015, this would mean that the FBI sat on this information for more than two months before telling the DNC. Alternately, it would mean that the NSA sat on the hack for two months before telling the FBI. We are certain that the NSA either is Cozy Bear or was monitoring Cozy Bear servers due to past Cozy Bear attacks. We do not believe that either the FBI or NSA would sit on such important information for two months.

#2. The January 6 2017 FBI report contains many other inaccurate and obviously false statements. For example, the 2017 FBI report maintains that the hackers had access until June 2016. This can not possibly be true as Crowdstrike completely cleaned the DNC servers on May 1 2016 and monitored them closely after that. I realize that Guccifer claimed that he had access to the DNC servers until June 2016. But we are certain he was not telling the truth as he also made several other untrue statements and because we are certain that Crowdstrike would have cleaned him out on May 1 2016.

#3: We have discovered several other attempts by the US Intelligence community to change the narrative to make it look like Cozy Bear had access as early as May 2015. We have researched all of these claims and found them to be completely false.

We therefore believe that the original story told by the FBI agent to the NY Times in 2016 has the most validity. According to this FBI agent, he personally warned the DNC that their servers were hacked by a group called the Dukes in September 2015 - but the DNC tech team took no significant action because they did not believe he was actually from the FBI. Nothing was done for months. The incompetent mess was described in detail in a New York Times story a year later. The NY Times article states that the FBI called the DNC repeatedly but was ignored because DNC staffers thought he was an impostor rather than a real FBI agent. The NY Times article claimed that the FBI knew the Dukes were Russians and had a long history opposing them. If this were really the case, then the actions of the FBI and the DNC border on incompetence. The NY Times article links to the **F Secure Report** (we have already quoted about the Dukes which concluded the Dukes were Russian based on the Cozy Duke Time Stamps. As noted before, the F Secure Report ignored a mountain of information such as server call back locations indicating that the Dukes were not Russians but Americans).

Our Comments on the September 15 Cozy Bear DNC Attack
There is a fundamental problem with the first DNC attack. The FBI had evidence that a major crime had been committed with Russians hacking DNC server in Washington DC. Yet all they did was call the DNC? This is not what is supposed to happen when a major crime is committed. The FBI is required to lock down the crime scene and take position of any and all evidence in order to launch an investigation. Warrants are supposed to be entered. The hacked server is supposed to be examined. The server logs would certainly supply important clues that could eventually be traced back to the alleged hackers.

Why didn’t the FBI take control of the crime scene in September 2015???

At the very least, the FBI should should have gotten a copy of the server logs. Instead, we found out on January 5, 2017 that according to the DNC, the FBI has never examined the DNC hacked server and never asked to examine the hacked server.
https://www.buzzfeed.com/alimwatkins/the-fbi-never-asked-for-access-to-hacked-computer-servers?utm_term=.jhKq72BRv#.tgBLXokNE

A day later, the FBI disputed this claim by stating that they had asked to examine the DNC server logs in May 2016 – but the DNC refused their request.
https://www.wired.com/2017/01/fbi-says-democratic-party-wouldnt-let-agents-see-hacked-email-servers/

According to the FBI official, "This left the FBI no choice but to rely upon a third party for information. These actions caused significant delays and inhibited the FBI from addressing the intrusion earlier."

Are you kidding me? Since when does the FBI have to get anyone's permission, other than a judge, to seize evidence after a major crime has been committed? Had the FBI gotten the server and the DNC taken steps to clean the server, we would not today be faced with the difficult task of figuring out who hacked the DNC – and possibly the DNC would not have lost the national election – an election on which they spent over one billion dollars trying to win. The failure of the FBI to take this action is one of many questions that has never been adequately addressed.

March 22, 2016: Fancy Bear Prepares to Attack the DNC

Seven months after Cozy Bear gained access to the DNC server, Fancy Bear decided they wanted in on the action too. So Fancy Bear registered a domain with a typo—misdepatrment.com—to look like the company hired by the DNC to manage its network, MIS Department. Go to Whois.net to find out who owns this fake domain name.
https://www.whois.net/default.aspx

Here is what you will get:
Domain Name: MISDEPATRMENT.COM
Name Server: 1A7EA920.BITCOIN-DNS.HOSTING
Updated Date: 22-apr-2016
Creation Date: 22-mar-2016
Expiration Date: 22-mar-2017

Put in plain English, Fancy Bear used a Bitcoin hosting account to hide their identity. They created the domain name on March 22, 2016 and updated it on April 22, 2016. They need to renew it by March 22, 2017 or someone else will be able to get that domain name.

On June 17, 2016, a pro-government security group called ThreatConnect stated that the person who registered this domain used the name Frank Merdeux. ThreatConnect did not mention and did not seem to be aware of the EFF connection we described above or the Ukrainian connection we describe below. Here is a quote from the June 17 Threat Connect report:

“In reviewing the Domain Whois information reveals that the domain was registered on March 22, 2016 by **frank_merdeux@europe**[.]com. Farsight lists the earliest domain use as **March 24, 2016.** On April 24th, 2016 the domain misdepatrment[.]com moved from the parking IP Address 5.135.183[.]154 to the FANCY BEAR Command and Control IP Address 45.32.129[.]185 where it remains resolved at the time of this writing. The domain misdepatrment[.]com closely resembles the legitimate domain for misdepartment.com. Of note, MIS Department Inc. is a technology services provider that lists a variety of clients on its website, one of which is the DNC.”
https://www.threatconnect.com/blog/tapping-into-democratic-national-committee/

Put in plain English, this domain name was supposedly not activated on the Internet until March 24, 2016 when it was moved from the IP address **5.135.183.154** to the IP address **45.32.129.18**5. But in fact, it was used in a hacking attack on March 22, 2016. This two day gap has never been explained. Nevertheless, here is who controls these two “Fancy Bear” IP addresses: http://whatismyipaddress.com/ip-lookup

5.135.183.154 links to a clean server located in France with no apparent purpose. The domain name is similar to the IP address: ip-5-135-183.154.eu. The person and address that owns this domain name according to WHO IS was not disclosed.

45.32.129.185 links to a corporate server in San Jose CA 95113. The organization is called Choopa LLC. Their domain name for this server is vultr.com. This group appears to have several servers and several IP addresses as they use each IP address as a sub domain of their primary domain.
A WHO IS look up of this domain name revealed the following ownership information:
Server Name: VULTR.COM.PROMEDICALEBOOKS.COM
IP Address: 45.32.60.43
Registrar: GODADDY.COM, LLC
Domain Name: VULTR.COM
Name Server: NS1.CHOOPA.COM
Updated Date: 04-sep-2015
Creation Date: 06-oct-2008
Expiration Date: 06-oct-2020

Put in plain English, this domain name was created in 2008 and is paid until 2020. It is registered with a US corporation called GoDaddy which has servers located in Arizona. Given the broad powers given to the FBI over US corporate servers, **it is highly unlikely that Russians would use US servers either to register their domain names or as a host location for their servers**. Like much of the evidence we provide in this report, this evidence has never been disclosed to the public.

Go to https://www.vultr.com/ and you will see that they claim to be a web host with servers in 15 cities around the world. Choopa.com is a web host located in New Jersey with branches in LA, Amsterdam & Toyko.

45.32.60.43 is another of several servers owned by Choopra LLC. But this server is in Tokyo.

Promedicalebooks.com is not an active domain name. However, a WHO IS lookup reveals the following ownership:
Domain Name: PROMEDICALEBOOKS.COM
Registrar: GODADDY.COM, LLC
Name Server: NS1.VULTR.COM
Updated Date: 17-aug-2016
Creation Date: 22-jun-2016
Expiration Date: 22-jun-2017

The June 22 2016 creation date cannot possibly be true as it was active since at least March 2016. Perhaps it had lapsed and was renewed in June 2016 which would reset the clock. Clearly whoever these people are, they like GoDaddy. But there is no need for real web hosts to use GoDaddy since most web hosts are their own domain registrars. So this seems odd. In any case, **since US laws extend to all US corporations, Russian hackers are not only unlikely to use servers located in the US, they are unlikely to use servers owned by any US corporation.**

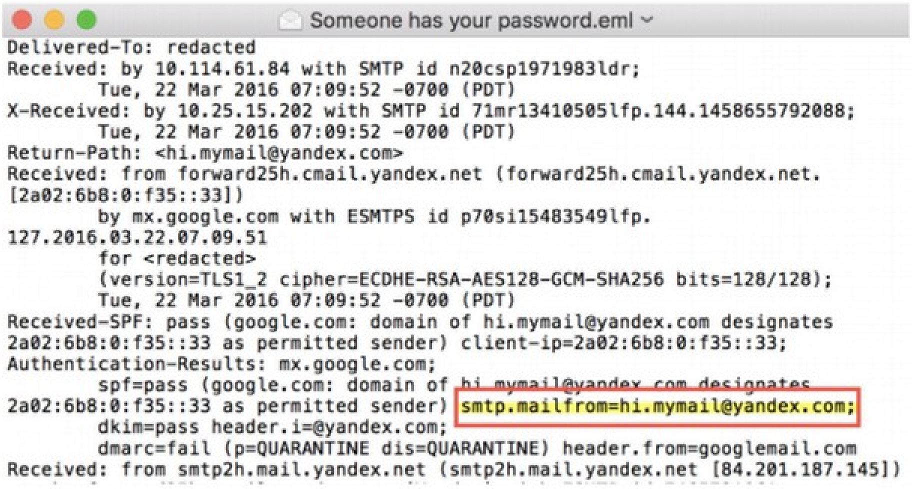
March 22, 2016: Billy Takes the Bait (so did Podesta)

In March 2016, a group called "Fancy Bear" also attacked the DNC Server.

The DNC discovers the attack in late April but instead of bringing in the FBI,
To investigate this crime, the DNC strangely brings in a group called Crowdstrike.

On the same day that Fancy Bear registered the misleading domain name, William "Billy" Rhinehart, a regional field director at the Democratic National Committee, received an email from Google warning him that someone tried to access his account and that he should immediately change his password. He complied. Unfortunately for Mr. Rhinehart, it wasn't Google who sent him that email. He, along with many others, were a victim of Fancy Bear.

The Smoking Gun (TSG) was able to obtain the original spear phishing email directly from Billy Rhinehart and shared it with ThreatConnect, who posted this screenshot of the email's headers and identified the actual sender of the email as a Russian domain: **hi.mymail@yandex.com.**



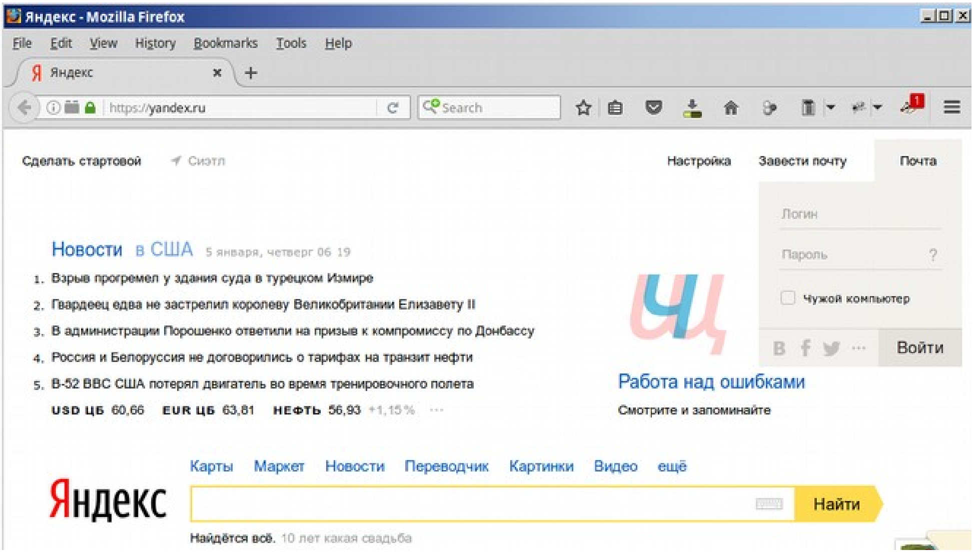
```
Delivered-To: redacted
Received: by 10.114.61.84 with SMTP id n20csp1971983ldr;
        Tue, 22 Mar 2016 07:09:52 -0700 (PDT)
X-Received: by 10.25.15.202 with SMTP id 71mr13410505lfp.144.1458655792088;
        Tue, 22 Mar 2016 07:09:52 -0700 (PDT)
Return-Path: <hi.mymail@yandex.com>
Received: from forward25h.cmail.yandex.net (forward25h.cmail.yandex.net.
[2a02:6b8:0:f35::33])
        by mx.google.com with ESMTPS id p70si15483549lfp.
127.2016.03.22.07.09.51
        for <redacted>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 22 Mar 2016 07:09:52 -0700 (PDT)
Received-SPF: pass (google.com: domain of hi.mymail@yandex.com designates
2a02:6b8:0:f35::33 as permitted sender) client-ip=2a02:6b8:0:f35::33;
Authentication-Results: mx.google.com;
        spf=pass (google.com: domain of hi.mymail@yandex.com designates
2a02:6b8:0:f35::33 as permitted sender) smtp.mailfrom=hi.mymail@yandex.com;
        dkim=pass header.i=@yandex.com;
        dmarc=fail (p=QUARANTINE dis=QUARANTINE) header.from=googlemail.com
Received: from smtp2h.mail.yandex.net (smtp2h.mail.yandex.net [84.201.187.145])
```

While the above screen shot seems to implicate Russian hackers, in fact it really implicates American hackers trying hard to fool people into thinking that the DNC was hacked by Russians.

A skeptical security consultant named Jeffrey Carr has written a detailed analysis of this email address. https://medium.com/@jeffreycarr

Here is a quote from his analysis:

"What's Wrong With This Picture? Yandex is the Google of Russia. Like Google, Yandex is a search engine, and, like Gmail, Yandex's users can open a free email account. When you visit Yandex.ru and create a new email account, the email assigned to you has the .ru domain. However, hi.mymail@yandex.com has a .com domain. So how does our presumed Russian intelligence operative get his Yandex.com email address? He has to click on the Yandex.com link from the Yandex.ru homepage.."



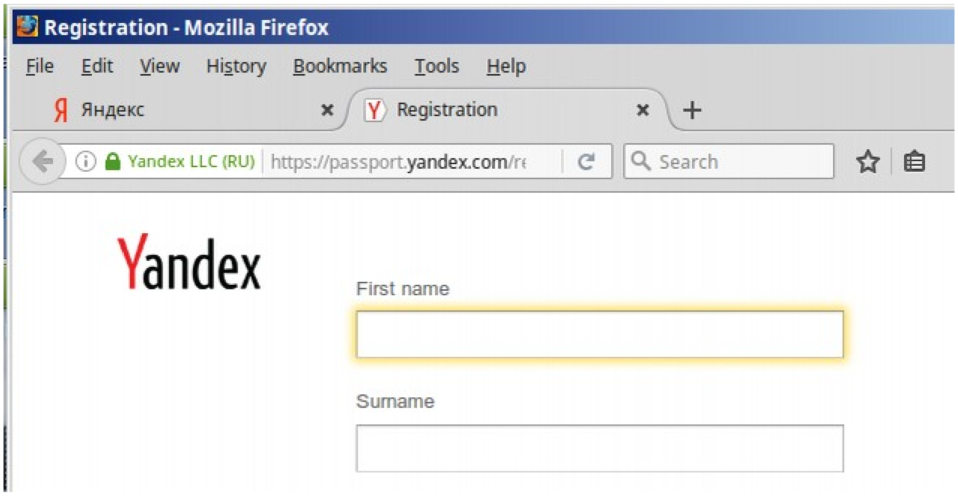
Новости в США 5 января, четверг 06 19

1. Взрыв прогремел у здания суда в турецком Измире
2. Гвардеец едва не застрелил королеву Великобритании Елизавету II
3. В администрации Порошенко ответили на призыв к компромиссу по Донбассу
4. Россия и Белоруссия не договорились о тарифах на транзит нефти
5. B-52 ВВС США потерял двигатель во время тренировочного полета

USD ЦБ 60,66 EUR ЦБ 63,81 НЕФТЬ 56,93 +1,15 %

Найдётся всё. 10 лет какая свадьба

Alternately, if your Russian is not that good, you can just do a Google Search and go to the following link which is conveniently written in English to get your **Yandex.com** free page: https://passport.yandex.com/registration?mode=register

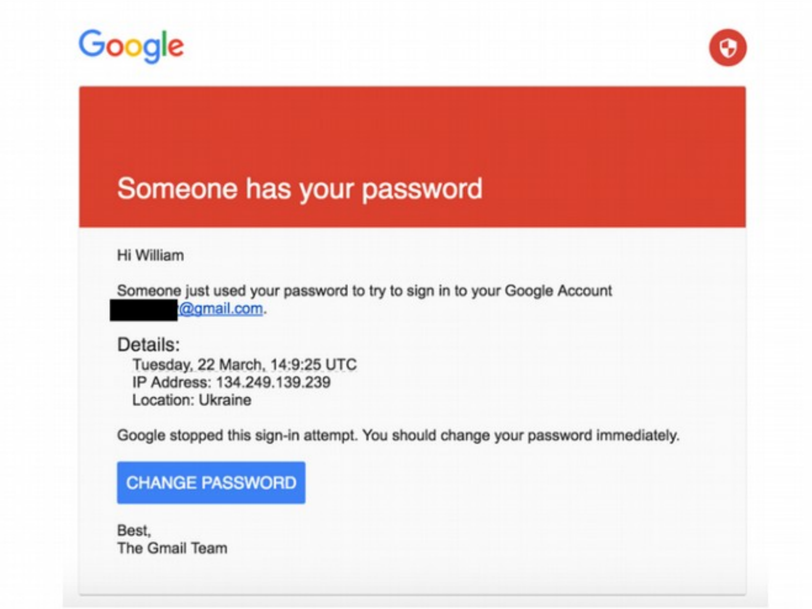

Registration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Яндекс
Registration
Yandex LLC (RU) https://passport.yandex.com/re
Search
Yandex
First name
Surname

Here is the rest of the quote from Jeffrey Carr:
“Everything, including the CAPTCHA, will be in English. The point that I’m trying to make is that if anyone in Russia wanted to spear phish employees of the DNC, then creating a @yandex.com email address instead of a @yandex.ru email address is not only unnecessary extra effort but it makes absolutely no sense. **However, you know what does make sense? That the person who opened the account DOESN’T SPEAK RUSSIAN!** He went with Yandex.com because all analysis stops with merely the name of a Russian company, a Russian IP address, or a Russian-made piece of malware. To even argue that a Russian intelligence officer let alone a paranoid Russian mercenary hacker would prefer a Yandex.com email to a Yandex.ru email is mind-numbingly batshit insane. I have no idea who created hi.mymail@yandex.com to spear phish Billy Rhinehart, but I bet you $100 that he wasn’t Russian.”

The Yandex.com screen shot is strong evidence that the DNC hack was not from a Russian but from a not very bright American pretending to be a Russian. This is only one of at least 20 indicators that the DNC email scam was not carried out by Russians or at the very least that Fancy Bear was not a Russian. The fact that this evidence was completely ignored by so-called security experts at Crowdstrike and elsewhere appears to be evidence of a deliberate plan to deceive the American people as to the real source of Fancy Bear and Cozy Bear. But let’s get back to our Timeline because there is more – a lot more.

March 22, 2016: Fancy Bear used a Ukrainian Server in their Email Attack

On March 22, 2016, Fancy Bear sent out thousands of fake Google Email Notices to all kinds of people, including members of the DNC including John Podesta (whose 60,000 emails were later published by Wikileaks). Here is a copy of this hacking email as published in the New York Times:



Google

Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account [redacted]@gmail.com.

Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

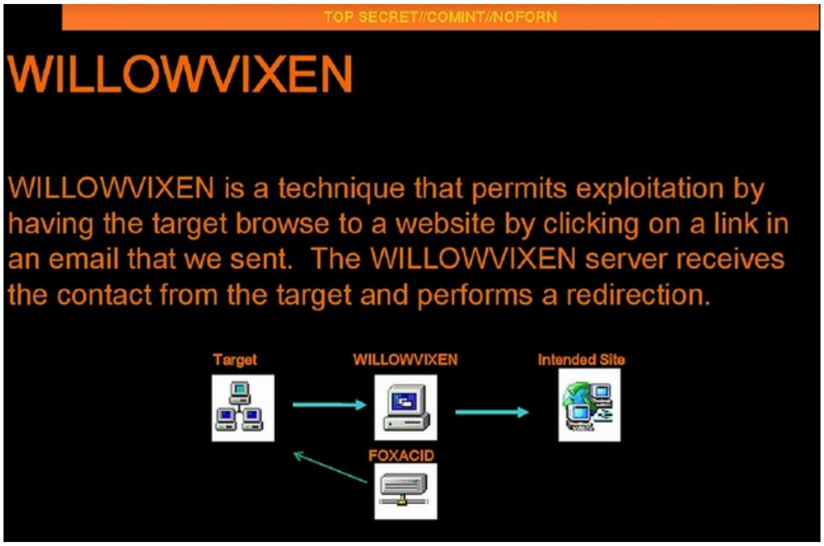
Google stopped this sign-in attempt. You should change your password immediately.

Best,
The Gmail Team

A screenshot of the phishing email that Billy Rinehart clicked on, unknowingly giving Russian hackers access to his account. The New York Times has redacted Mr. Rinehart's email address.

Note that the IP address of the person who supposedly used the password to the Gmail account is located in Ukraine. **IP 134.249.139.239** is a broadband server in Ukraine. This may not seem to be important because the IP is open to easy access. But the fact that the IP address is in Ukraine is significant. **Why would the Russians want to run an email campaign using a Ukrainian IP address? This does not make any sense.**

John Podesta clicked on this link and thought he was resetting his password. In fact, he was sending the password to Fancy Bear because the link redirecting him to a form that may have looked like a Google Password reset form but was in fact a fake form. Here is a 2012 NSA document provided by Edward Snowden in 2013 confirming that **the NSA uses a nearly identical strategy to gain access to a person's email account.**



TOP SECRET//COMINT//NOFORN

WILLOWVIXEN

WILLOWVIXEN is a technique that permits exploitation by having the target browse to a website by clicking on a link in an email that we sent. The WILLOWVIXEN server receives the contact from the target and performs a redirection.

Target
WILLOWVIXEN
Intended Site
FOXACID

April 2016: Cozy Bear and Fancy Bear settle in to their new DNC Home.
Cozy Bear has been hacking the DNC in real time since September 2015. Fancy Bear joined in the feast on March 22, 2016. Both had unlimited access to data until May 1.

May 1, 2016: Crowdstrike kicks Cozy Bear & Fancy Bear Out of DNC Server

The FBI (again) notified the DNC that their network had been hacked. This time, the DNC finally believes the FBI and calls in Crowdstrike, who locate two intrusions and reset the DNC system. Until this time, the hackers were able to read all DNC email and chats. After about two hours of work, Crowd Strike found "two sophisticated adversaries" on the DNC network. The two groups were"APT 28" (Fancy Bear) and "APT 29." (Cozy Bear)

May 2016: Crowdstrike issues report – but does not release it to the public.
Crowdstrike issued their first report but never released it to the public. I spent a great deal of time looking for this report and if anyone has it, I am hoping you will email it to me.

Our Comments on the DNC Hack
There appears to have been some sort of effort to hide the DNC hack from the public perhaps because Clinton had not yet secured the Democratic Party nomination and they worried that yet another email scandal may have further harmed her reputation. This is the only reason I can think of to explain why the FBI failed to examine the DNC servers (something we learned on January 5, 2017). But this still does not explain the actions of the DNC or FBI. As we noted early, hacking the DNC server was a major crime. So why did the DNC call Crowdstrike instead of the FBI? When a crime is committed, you call the police. You do not call some consulting firm to clean up the crime scene before the police arrive because there is the danger that the consultants will destroy important evidence. The FBI should have gone in and taken charge on Day 1.

However, the wheels were about to fall off the DNC bus. At some point, someone gave some information to Wikileaks and they were about to go public with it. It also appears that more than one group hacked the DNC and stole their documents. But another strange thing was about to happen. An entire group of people are about to start blaming the Russians for these hacks. Perhaps this mistake was made because the Russians had falsely been accused of being Cozy Bear and Fancy Bear in the past. But it would not have taken much research to realize that there was more evidence pointing to the NSA than there was pointing to Russia.

So it seems more likely that whoever was behind this massive propaganda campaign did not want to know the truth. Somehow, it served their purpose to have Americans hating Russia. Apparently, this group was so arrogant that they felt they could keep the truth hidden forever. But the truth is a powerful weapon. It will eventually come out either through the evidence presented in this report – or some future leak or hack. When it does, the American people will once again realize they are being lied to by their own government. Hopefully, then, the people will finally vote for real political change.

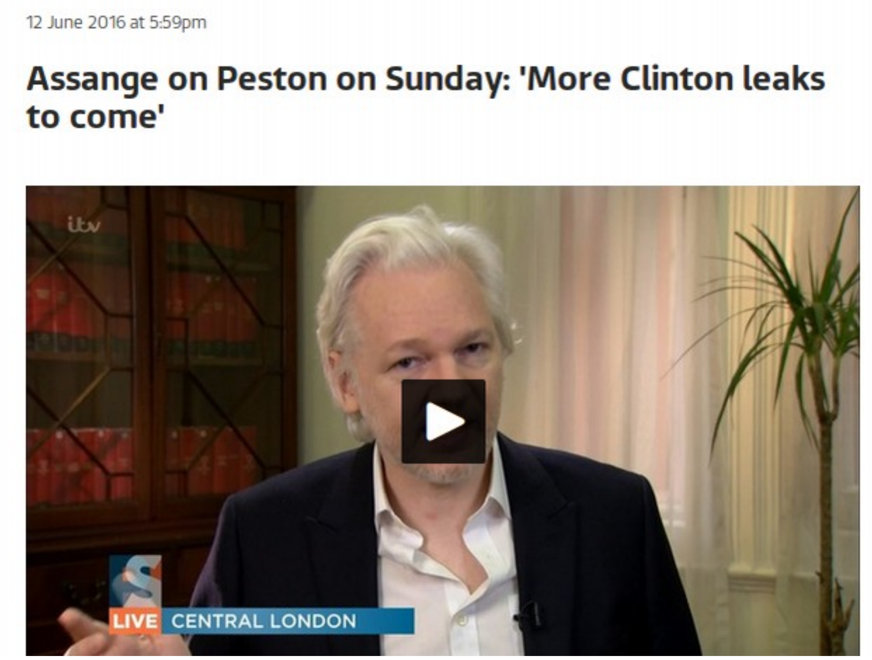
Now back to the timeline because there is a lot more evidence in the coming pages that Russia was not responsible for the DNC hack. The hack may be over. But the spin is about to begin.

Part 3 Summer of Spin...The DNC Hack: June to August 2016

June 03 2016: WikiLeaks creates an insurance file which includes the DNC hack. This seems to indicate that Wikileaks had at least some data by June 3 2016. However, Wikileaks later said that there were two separate leaks from two separate sources. It appears that at least one of the leaks was not until July 2016.

June 12 2016: Wikileaks Announces Clinton Data Release is Imminent

At 5:59 pm, Julian Assange [announces](http://www.itv.com/news/update/2016-06-12/assange-on-peston-on-sunday-more-clinton-leaks-to-come/) that they have documents relating to Hillary Clinton which are pending publication and that it would be **"enough evidence" to indict her**. This appears to be the first public announcement about the DNC leak and/or hack. But he did not reference the DNC… Just the Clinton email private server scandal. He had already posted 32,000 emails from the Clinton private server. He did state that there were more leaked emails to come. Perhaps he did not want to mention the DNC because the DNC hack was not yet public and he wanted to protect his source(s). http://www.itv.com/news/update/2016-06-12/assange-on-peston-on-sunday-more-clinton-leaks-to-come/



12 June 2016 at 5:59pm

Assange on Peston on Sunday: 'More Clinton leaks to come'

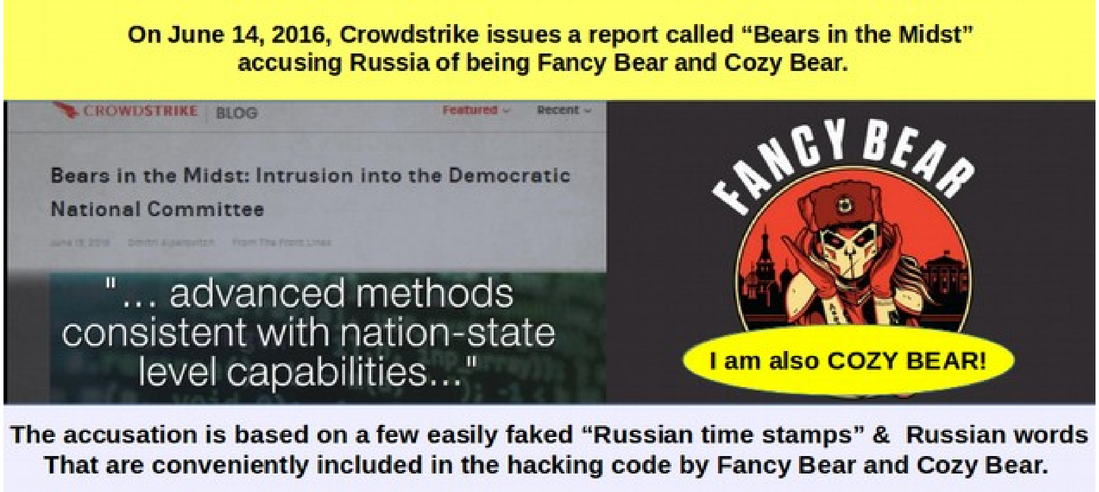
Here is a quote from the June 12, 2016 article:
"Julian Assange, founder of Wikileaks, said on Sunday that the journalist organization is planning to release upcoming leaks in relation to US presidential hopeful Hillary Clinton. Speaking to Peston on Sunday, Mr Assange said Wikileads has further information relating to claims circulating since 2015 that Clinton had in the past used her family's private email server for official communications."

June 12 2016: According to Guccifer 2.0, the DNC resets their network, kicking "him" out of it on this date. But he does not go public until after the Washington Post story three days later. There are several reasons to conclude that this claim by Guccifer is false and that if he ever had access to the DNC, that access ended on May 1 2016.

June 14, 2016: CIA backed Washington Post Breaks DNC Hack to the Public
Apparently in response to the June 12 2016 Wikileaks announcement, the DNC decided to go public with a story posted by their friends at the Washington Post. On June 14th, the *Washington Post* revealed that "Russian government hackers" had penetrated the computer network of the Democratic National Committee."

June 14, 2016: Crowdstrike releases DNC Hack Report

Three hours later**,** CrowdStrike issued a report called **Bears in the Midst** outlining some of the details and IP addresses of both attacks. While referring to their previous report in May, they did not provide a link to it. Dmitri Alperovitch stated: "CrowdStrike stands fully by its analysis and findings identifying two separate Russian intelligence-affiliated adversaries present in the DNC network in May 2016." Of course, if he is so confident in his previous report, then **why didn't he link to the May report so we can all read it?**



On June 14, 2016, Crowdstrike issues a report called "Bears in the Midst" accusing Russia of being Fancy Bear and Cozy Bear.

CROWDSTRIKE | BLOG

Bears in the Midst: Intrusion into the Democratic National Committee

"… advanced methods consistent with nation-state level capabilities…"

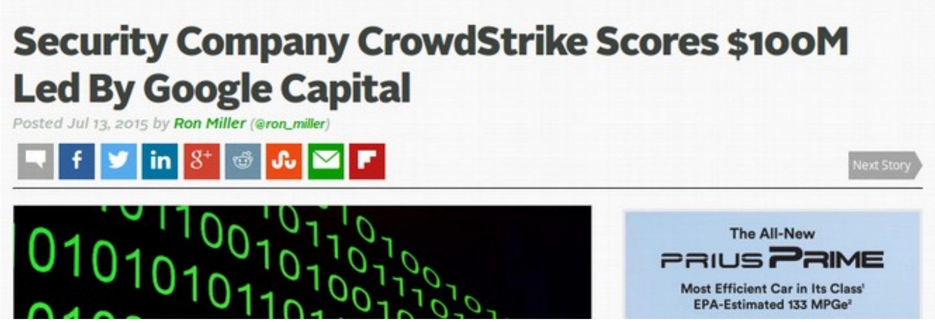
The accusation is based on a few easily faked "Russian time stamps" & Russian words That are conveniently included in the hacking code by Fancy Bear and Cozy Bear.

The main person making this claim of Fancy Bear and Cozy Bear attacking the DNC and being Russian is Dmitri Alperovitch who is one of the founders of Crowdstrike. Crowdstrike rose to the national spotlight in June 2016 because they were handpicked by the DNC to investigate who hacked the DNC servers. Dimitri concluded that not just one but two Russian groups called Cozy Bear and Fancy Bear hacked the DNC. Dimitri "evidence" was finding a malware program called Duke (also known as Cozy Duke) was used in the attack. Dmitri then claimed that Cozy Duke aka Fancy Duke were "known" Russian hacking programs (based on the 2015 F Secure Time stamp assumption).

Dmitri Alperovitch, 32

The cofounder of the security company CrowdStrike wants to help cyberattack victims strike back.

But in order to evaluate whether Crowdstrike is a trustworthy source, we should follow the money. It turns out that Crowdstrike got $100 million in funding from Google who in turn gets hundreds of millions in funding indirectly from the US military.
https://techcrunch.com/2015/07/13/security-company-crowdstrike-scores-100m-led-by-google-capital/



Security Company CrowdStrike Scores $100M Led By Google Capital

Posted Jul 13, 2015 by Ron Miller (@ron_miller)

If you are not yet aware of the close relationships between Google, Facebook, the CIA, DARPA and the NSA, you might want to watch this 53 minute documentary.
https://www.youtube.com/watch?v=5WNkDfxTPbI
As for Crowdstrike. it is not the only fake security firm paid hundreds of millions of dollars to do the dirty work of the US military. There are more than 100 other consultants who would just as gladly point the finger at Russia – especially if it meant getting a one hundred million dollar payoff.

In addition Crowdstrike was the group that made the claim that the Sony Hackers were from North Koreans who "stole administrator credientials" when in fact it turned out to be a disgruntled Sony employee who already had administrator credentials. For those who may not remember, in 2014, Sony was attacked using a malware that prevented them from even turning on their computers.

Here is a December 14, 2014 quote from Dimitri expressing confidence that he knows beyond any shadow of a doubt that the hackers must be North Korean:
"The co-founder of CrowdStrike, a security firm that focuses heavily on identifying attribution and actors behind major cybercrime attacks, said his firm has a "very high degree of confidence that the FBI is correct in" attributing the attack against Sony Pictures to North Korean hackers, and that CrowdStrike came to this conclusion independently long before the FBI came out with its announcement last week.
"We have a high-confidence that this is a North Korean operator based on the profiles seen dating back to 2006, including prior espionage against the South Korean and U.S. government and military institutions," said **Dmitri Alperovitch**, chief technology officer and co-founder at CrowdStrike."
https://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack/

Other cyber security experts almost immediately began poking holes in Dmitri's claim that it was North Korea. Here are some quotes:

"Skeptics note that the few malware samples they have studied indicate the hackers routed their attack through computers all over the world. One of those computers, in Bolivia, had been used by the same group to hack targets in South Korea. But that computer, as well as others in Poland, Italy, Thailand, Singapore, Cyprus and the United States, were all freely available to anyone to use, which opens the list of suspects to anyone with an Internet connection and basic hacking skills. (Also) the attackers used commercial software wiping tools that could have been purchased by anyone.

They also point out that whoever attacked Sony had a keen understanding of its computer systems — the names of company servers and passwords were all hard-coded into the malware — suggesting the hackers were inside Sony before they launched their attack. Or it could even have been an inside job… The simpler explanation is that it was an angry “insider,” Mr. Rogers wrote. “Combine that with the details of several layoffs that Sony was planning, and you don’t have to stretch the imagination too far to consider that a disgruntled Sony employee might be at the heart of it all.”
https://bits.blogs.nytimes.com/2014/12/24/new-study-adds-to-skepticism-among-security-experts-that-north-korea-was-behind-sony-hack/?_r=0

The initial communication from the hacker(s) was about employee grievances due to Sony's restructuring and layoff plan. Here is a quote from a December 24, 2015 CNN article:

“Upon closer examination, security experts, hackers and people familiar with Sony's computer networks are uniting with this disheartening reality: Anyone could have pulled this off. It could have been a disgruntled Sony employee, profit-seeking hackers, North Korea -- or a combination of the three… t**his hack actually started as an extortion attempt on Nov. 21 when Sony executives got emails saying: "The compensation for it, monetary compensation we want."**
http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/

So given that Dimitri was so wrong about the Sony hack, why would the DNC hire him to investigate the DNC hack? And why would anyone believe anything Dimitri has to say? We will reveal more about Crowdstrike as we go along.

Details of the June 15 Crowdstrike Report:
According to CrowdStrike, the COZY BEAR hack in 2015 relied on the SeaDaddy implant while the FANCY BEAR hack in 2016 used X-Agent malware. SeaDaddy was discussed in the 2015 F Secure report. It is associated with Cozy Bear. X Agent is more of a problem. We will review it when we get to December 2016 and the false claim made by Crowdstrike that X Agent was used by Russia to target Ukrainian troops via Android phones. But for now, let’s stay focused on the June 15th report.

Here are the IP addresses Crowdstrike associated with Cozy Bear:
185.100.84.134 is a Romanian broadband server.
58.49.58.58 is a Chinese broadband server.
218.1.98.203 is another Chinese broadband server.
187.33.33.8 is a Brazil broadband server.

Here are the IP addresses Crowdstrike associated with Fancy Bear:
185.86.148.227 is a clean Swedish server that has no listed purpose.
45.32.129.185 is another server from our Choopa LLC friends in San Jose CA.
23.227.196.217 is a corporate server associated with Swiftway Communications located in that hot bed of commies otherwise known as Wilmington Delaware. They are an Internet Service Provider (ISP) in business since 2005 and they have servers in the US, Europe and Asia with customers in over 90 countries around the world. One of their customers seems to be Fancy Bear. Their website is: http://www.swiftway.net/

I could not find anything connecting any of the above servers to Russia. Broadband servers are not evidence of anything. And servers in the US are strong evidence that the hackers are NOT Russians. I do not question these IP addresses being associated with Cozy Bear and Fancy Bear. But I do question these IP addresses somehow being connected to Russian Hackers.

June 15, 2016: Guccifer 2 surfaces and claims to be the lone DNC Hacker
GUCCIFER 2.0 posted a Wordpress blog titled "DNC's servers hacked by a lone hacker." This online persona claimed to have given "thousands of files and mails" to Wikileaks, while mocking Crowdstrike. He claimed to be Romania but could not speak Romanian. He uses the ")))" smiley emoticon used by those using a Cyrillic keyboard. The metadata for the documents that Guccifer 2.0's posts is taken from the founder of the Soviet Union's secret police. He therefore seems to be some kind of plant. He is working for someone. But it is impossible to tell who as he is a pretty bad actor and makes several basic mistakes. For example, he posted a Word document that had the name of a famous Russian in the properties section of the document – thus leading reporters to conclude that he was Russian. But Guccifer could just as easily been the NSA posing as a Romanian but really intended to be exposed as a Russian. Moreover setting up a website for folks to download documents and being interviewed by the press is not exactly how most hackers work. Guccifer may have hacked the DNC and gotten a bunch of files. Security at the DNC was so lax that a teenager could have hacked them.
But based on his statements and actions, I do not think Guccifer 2 is Russian or NSA or Cozy Bear or Fancy Bear. We will not spend much more time on Guccifer for this reason. Also, there are several facts that are much more relevant that we do want to cover – such as who is Fancy Bear and who is Cozy Bear.

June 17, 2016: German Hack Smoking Gun turns out to be Smoke & Mirrors

Another member of the NSA club called Threat Connect issued a brief report on Crowdstrike IP addresses called **Fancy Bears and Where to Find Them**
https://www.threatconnect.com/blog/tapping-into-democratic-national-committee/

This report appeared to provide a "smoking gun" confirming that Fancy Bear was Russian. But like all of the other smoking guns, even a little research reveals it was all smoke and mirrors. In their June 15 2016 report, Crowdstrike claimed that the IP address **176.31.112.10 is controlled and/or used by Fancy Bear as it was hard coded into the malware and was involved in the Fancy Bear attack in Germany in 2015.** As this is the main evidence that the DNC March 22 2016 attack was from Fancy Bear, we need to also look at the Germany attack for evidence of Russian hackers.

First is a quote from a Crowdstrike Cheerleader named Thomas Rid:
"One of the strongest pieces of evidence linking GRU to the DNC hack is the equivalent of identical fingerprints found in two burglarized buildings: a reused command-and-control address—**176.31.112[.]10**—that was hard coded in a piece of malware found both in the German parliament as well as on the DNC's servers. Russian military intelligence was identified by the German domestic security agency BfV as the actor responsible for the Bundestag breach. The infrastructure behind the fake MIS Department domain was also linked to the Berlin intrusion through at least one other element, a shared SSL certificate."
http://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack

It sounds like an open and shut case, doesn't it? There is only one problem. Almost every sentence in the above paragraph is false (kind of like the Vermont Power Grid story was false). But don't take it from me. Here is a quote from security consultant Jeffrey Carr:

"**Problem #1:** The IP address 176.31.112[.]10 used in the Bundestag breach as a Command and Control server has **never been connected to the Russian intelligence** services. In fact, Claudio Guarnieri, a highly regarded security researcher, whose technical analysis was referenced by Rid, stated that "**no evidence allows to tie the attacks to governments of any particular country."**

Problem #2: The Command & Control server (176.31.112.10) was using an outdated version of OpenSSL vulnerable to Heartbleed attacks. **Heartbleed allows attackers to steal data** including private keys, usernames, passwords and other sensitive information. The existence of a known security vulnerability that's trivial to exploit opens the door to the possibility that the systems were used by one rogue group, and then infiltrated by a second rogue group, making attribution even more complicated.

Problem #3: The BfV published a **newsletter** in January 2016 which assumes that the GRU and FSB are responsible because of technical indicators, not because of any classified finding; to wit: "**It is assumed** that both the Russian domestic intelligence service FSB and the military foreign intelligence service GRU run cyber operations."
https://medium.com/@jeffreycarr/can-facts-slow-the-dnc-breach-runaway-train-lets-try-14040ac68a55#.9o758bkf5

But don't take Jeffrey's word for it. Let's go to the source. This is the source document for the May 20 2015 German hack that was reported on June 19 2015 which thankfully was printed in English as my German is a little rusty. .
https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

Here is a quote from the report: "Attributes of one of the artifacts and intelligence gathered on the infrastructure operated by the attackers suggest that the attack was perpetrated by a state-sponsored group known as **APT28**. Previous work published by security vendor FireEye in October 2014 suggests the group might be of Russian origin." So the author relies on the Fire Eye conclusion that APT 28 is Russian which in turn was based on the F Secure Report which in turn was based on easily changed time stamps.

But it may be that the hacker of the German server was not Russian or American because the hacker made a very basic mistake. Here is the quote:
"The Command & Control server (176.31.112.10) appears to be using an outdated version of OpenSSL and be vulnerable to Heartbleed attacks. The same C&C server might have been the subject of 3rd-party attacks due to this vulnerability.**"**

Here is one more quote from the German report:
"(German hack) Artifact #2 was compiled by the authors on April 22nd 2015, which suggests that the compromise may only have lasted a couple of weeks...Previous work by security vendor FireEye suggests the group might be of Russian origin, however **no evidence allows us to tie the attacks to governments of any particular country."**

One important final quote: “The address, 176.31.112.10, is a dedicated server provided by the French OVH hosting company, but is apparently operated by an offshore secure hosting company called **CrookServers.com** and seemingly located in Pakistan.
By researching historical data relevant to C&C 176.31.112.10, we discovered that on February 16th 2015, the server was sharing an SSL certificate with another IP address allocated to CrookServers and also hosted at OVH: 213.251.187.145“.

Our Comments on the German Hack Smoking Gun
Whether there was a third party attack or not, using an outdated version of Open SSL with a very widely publicized vulnerability that could destroy the whole apple cart seems like something that only a teenager wannabe hacker would do – not Russian hackers and not NSA hackers. The program was compiled just before the May 2015 hack. This seems to indicate that it was some kid that got hold of a program not even realizing that it suffered from the Heartbleed problem. Moreover, there seems to be little motive for Russia to hack the server of a left leaning political party in Germany. Finally, there is no way Russian hackers are going to be using servers in Pakistan by a hosting company called **Crook Servers**. The only hackers I know that are that arrogant are the NSA Equation Group. I could see the NSA hacking the German server due to their motto to “hack everything.” But there is no way that the Equation group would overlook the Heartbleed problem. So my conclusion is that the German hacker was not even Fancy Bear. It was simply some teenager out for a joy ride. And the smoking gun? It was more like smoke and mirrors.

July 7, 2016: Threat Connect Proves they have no idea what they are talking about
Threat Connect posted a short blog trying to explain the significance of Named Servers being associated with the Russian Hackers. Sadly, during their explanation, they incorrectly claiming that Godaddy uses named servers called GoDaddy. Here is a quote: “For example, if five domains are registered through GoDaddy, all five of those domains by default will use GoDaddy name servers like NS1.GODADDY[.]COM and NS2.GODADDY[.]COM.”
https://www.threatconnect.com/blog/whats-in-a-name-server/

There are two problems with this claim. First, their example is factually wrong. In fact, Godaddy named servers are not under the name Godaddy. They are under the name **Domain Control.** As the millions of people who have GoDaddy accounts know, their named servers use the names **ns38.domaincontrol.com, ns39.domaincontrol.com, etc.** It does not inspire much confidence when these so-called security experts do not even know the names of the world’s most over-crowded servers.

Second, Russian Hackers would never use GoDaddy servers because they are located in the US with a US corporation under draconian US laws. Russian hackers also would not use servers located in Russia. But there are many European countries with strong privacy laws were Russian hackers would be least likely to be caught or disturbed. Switzerland comes to mind as a good place to have one’s data if one did not want to be shut down by the FBI and the NSA.

July 10, 2016: DNC staffer Seth Rich killed in Washington DC

At 4:19 am. Seth Rich, the Voter Expansion Data Director for the DNC was shot twice in the back and killed in a Washington DC suburb. His girlfriend stated " "There had been a struggle. His hands were bruised, his knees are bruised, his face is bruised, and yet he had two shots to his back, and yet they never took anything." Some claimed that Seth Rich was the source of the DNC leak to Wikileaks and that he was shot for betraying the Democratic Party leaders. https://en.wikipedia.org/wiki/Murder_of_Seth_Rich

July 22, 2016: Wikileaks published DNC Leak Documents

Just before the Democratic National Convention, Wikileaks published more than 19,000 DNC emails with more than 8,000 attachments confirming that the DNC had colluded with the Clinton campaign to block Bernie Sanders from the nomination. Many Sanders supporters at the convention walked out in protest. This same day, Guccifer 2.0 claims they gave the files to WikiLeaks, four hours later WikiLeaks says that anyone claiming to know who their source is "has no credibility."

On July 22, 2016, Wikileaks published DNC documents confirming the DNC colluded with the Clinton Campaign to prevent Bernie Sanders from being their Presidential nominee.

WikiLeaks
Custom Search
OPINION

DNC Email Archive

This releases contains 19,252 emails and 8,034 attachments from the top of the US Democratic National Committee (DNC) and is part of our Hillary Leaks series. The leaks come from the accounts of

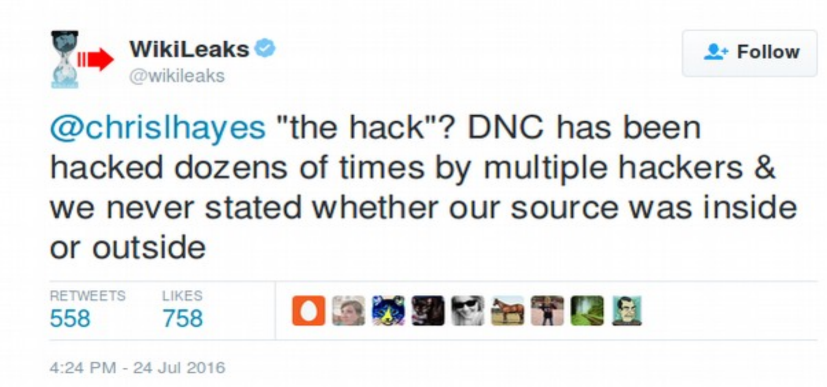
JULY 22, 2016

LATEST WIKILEAKS DUMP PROVES DNC BIAS AGAINST BERNIE SANDERS

The revelations cause chaos at the Democratic National Convention as hundreds of Bernie supporters walk out in protest.

July 24 2016: Wikileaks issues Tweet Implying Source is an Insider

WikiLeaks says their sources do not set the date for releases and that they have more DNC documents coming. Another tweet implies their source may have been an insider.



WikiLeaks @wikileaks

@chrislhayes "the hack"? DNC has been hacked dozens of times by multiple hackers & we never stated whether our source was inside or outside

RETWEETS 558 LIKES 758

4:24 PM - 24 Jul 2016

A later tweet indicated it was an inside job or a leak – not a hack.

July 24, 2016: Debbie Wasserman Schultz, chair of Democratic National Committee, resigned from the DNC and was immediately hired by Clinton.

July 25, 2016: During an exclusive interview with Democracy Now!, Julian Assange, Editor in Chief of the anti-secrecy website WikiLeaks, said that “no one knows WikiLeaks sources. Claiming one source or another is simply speculation.”

July 30, 2016: The Russian Government FSB reports, through RT, that over twenty high profile Russian organizations and government agencies have been hacked by sophisticated malware to give an example that it is not just organizations in the US that are hacked.

July 31, 2016: Former NSA Lead Administrator, William Binney says the Hack was not done by Russians but by the NSA

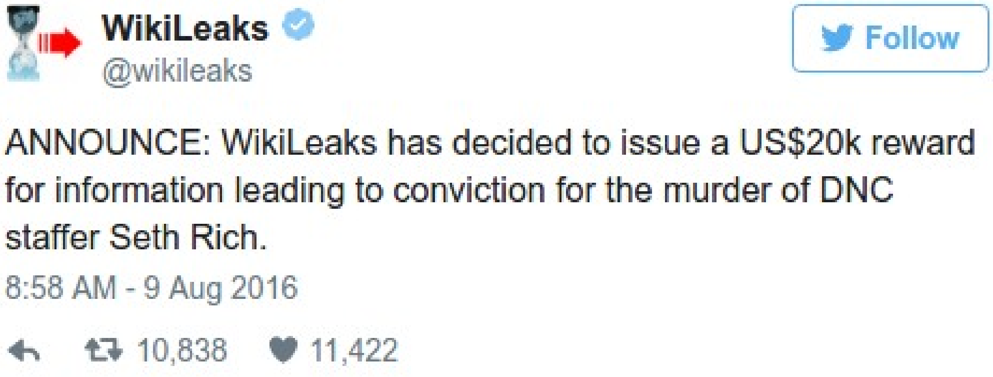
On a New York Radio Show, the person who knows more about the power of the NSA than almost anyone in America, former head spy, William Binney explained why the hack was much more likely to be done by the NSA than by the Russians. William Binney worked for NSA for 36 years, retiring in 2001 as the technical director of world military and geopolitical analysis and reporting; he created many of the collection systems still used by NS

NSA whistleblower says DNC hack was not done by Russia, but by U.S. intelligence
ALEX CHRISTOFOROU
August 1, 2016, 5:23 pm

During the radio program, Binney specifically referred to the fact that the network server log keeps a record of every IP address that contacts every server. It is these server logs that could provide important clues as to who the hackers really are. But they have never been released.

“William Binney threw his hat into the DNC hack ring by stating that the Democratic National Committee’s server was not hacked by Russia but by a disgruntled US. intelligence worker…concern over Hillary Clinton’s disregard of national security secrets when she used a personal email and consistently lied about it. Binney also proclaimed that the NSA has all of Clinton’s deleted emails, and the FBI could gain access to them if they so wished.”
http://theduran.com/nsa-whistleblower-says-dnc-hack-not-done-russia-us-intelligence/

August 10, 2016: Wikileaks offers $20,000 reward for help in finding Seth Rich killer
They issued the following statement: “We treat threats towards any suspected WikiLeaks sources with extreme gravity. This should not be taken to imply that Seth Rich was a source to WikiLeaks or that his murder is connected to our publications.” Later that same day, Wikileaks leader Julian Assange appeared on Dutch television and stated "Whistle-blowers go to significant efforts to get us material and often very significant risks. As a 27-year-old, works for the DNC, was shot in the back, murdered just a few weeks ago for unknown reasons as he was walking down the street in Washington." When the interviewer protested that the murder may have been a robbery, Assange replied “**"**No. There is no finding. So… I’m suggesting that our sources take risks." Here is a link to the interview. https://www.youtube.com/watch?v=Kp7FkLBRpKg



WikiLeaks
@wikileaks

ANNOUNCE: WikiLeaks has decided to issue a US$20k reward for information leading to conviction for the murder of DNC staffer Seth Rich.

8:58 AM - 9 Aug 2016

10,838 11,422

Despite the Wikileaks reward, the Seth Rich murder case has never been solved and remains open today.

Part 4 Ongoing Allegations... September to December 2016

September 15, 2016 Server Company Provides Analysis of Hacker Locations

While nearly all of the servers claimed to be involved in the Russian Hacking attacks were not in Russia and have failed to provide any analysis from their server logs (I really wonder why this is because all servers have server logs), one Russian company that was caught up in the cyber attack did take the time to analyze their logs and issue a press release with their findings. Since this is what every server company should have done, I will quote from an English translation of their press release which was written in Russian. This company has since been attacked as being owned by Russian criminals and I want to make it clear that I have no way of verifying their report. I am simply quoting them to show the public what could be done if a server company wanted to help us discover the truth – namely they should all publish their logs. Also I am certain that the FBI can get a warrant for all logs of all servers in the US. The fact that the FBI has not done this (or has not released information about the logs if they have done this) is a strong indication that the FBI is not really interested in providing the public with additional information about the locations of communications from the hackers to the servers. Here is the source document which will be translated for you if you visit the page with a Chrome Browser. https://chronopay.com/blog/2016/09/15/chronopay-pomogaet-king-servers-com/

Here is an edited version of their press release (I edited to make it shorter by eliminating text that was not related to the server logs. I also **bolded the important parts**):
“King Servers (https://www.king-servers.com), which owns servers from which the hacker allegedly performed attacks on the United States Democratic Party, states the absence of any «Russian trace» in this cybercrime nor its own involvement...King Servers, owned indeed by Russian nationals, provides VPS and VDS rental services of the equipment, **physically located in the Netherlands.** Earlier, after the FBI alert (https://s.yimg.com/dh/ap/politics/images/boe_flash_aug_2016_final.pdf) and analysis from Threat Connect (https://threatconnect.com/blog/state-board -election -rabbit-hole /), the world's leading media were spreading information about the discovery of the so-called «Russian trace» in the attacks on the United States democratic party in Illinois. The «Russian trace» was mostly presented as the use of King Servers services, stating that the company belongs to Russian citizens. As of September 15, neither King Servers received any complaints or appeals for any server misuse or abuse, nor any public authority did any attempts for servers withdrawal. Due to that King Servers found out about the issue related to that attack only on September 15, at 7 am Moscow time, and **immediately shut down identified servers.**

The analysis of the internal data allows King Services to confidently refute any conclusions about the involvement of the Russian special services in this attack. Attackers rented two servers using probably fabricated personal and identification data. After the attack servers were wiped out. However, **King Servers maintains logs of accessing administrative control panel. After log analysis, King Servers obtained a list of about 60 of all possible IP addresses of «hackers», none of which belongs to any Russian ip range. Attackers were logging into administrative control panel mainly from Scandinavian countries (Norway, Sweden) and from the European Union (Italy).**

Payment for servers were done through semi-anonymous Russian payment system, albeit very well-known in Russia for virtually open collaboration with US security agencies at least since 2011, when American security experts close to the state intelligence and counterintelligence agencies in the United States. With high probability, attacker's servers were controlled by one person, since **there are lots of IP matches between two accounts**...King Servers retained all the investigation materials, copies of server log files and correspondence and is ready to provide them to any interested party, law enforcement agencies or media, in accordance with the law."

Many people have asked me what evidence it would take to convince me that Russian government agents did hack the DNC. One of the things it would take would be a pattern of evidence linking the "call home" servers to IP addresses that eventually linked in a chain back to Russia. Note above that they were able to isolate the accounts and ID every single transaction just like a bank can trace a financial transaction. They then provided some useful information – that the hackers were logging in from servers mainly in Norway, Sweden and Italy. I realize that this does not mean that the hackers were actually in any of these countries. But we can go to the servers in those countries and eventually trace the hacker back to their source servers.

I am not saying this would be easy. But I am certain that the NSA has this capability. The American people deserve much better then the nonsense and BS we have been given by the US intelligence agencies. What I am asking for is exactly what William Binney and Edward Snowden are asking for. Real hard evidence. It is a complete lie that providing this evidence would compromise either sources or methods. Server logs are an open book. **Why haven't we been given the server logs of the Fancy Bear servers in San Jose California???** Either give us the logs or stop making these unproven accusations.

October 7 2016: US issues Press Release Blaming Russia for DNC Hack

James Clapper, the person who lied to Congress in March 2013 about the NSA Mass Surveillance Program, issued a press release blaming Russia for hacking the DNC. Once again, there was not one shred of actual evidence. Just a series of unsupported allegations. This is ridiculous.
https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

October to November 2016: Over the course of a month, Wikileaks publishes more than 58,000 emails hacked from the Gmail account of John Podesta.

John Podesta was Clinton's campaign manager. Many are highly incriminating and cast Clinton in a very bad light. Apparently all of the Podesta emails are true.
https://wikileaks.org/podesta-emails/

November 2 2016: Wikileaks says Russia is not the source

Wikileaks has repeatedly refused to name any of their sources. However, **on November 3 2016, Julian Assange told a reporter John Pilger "We can say that the Russian government is not the source."**
http://theduran.com/julian-assange-is-on-the-record-we-can-say-that-the-russian-government-is-not-the-source/

In October 2016, Wikileaks publishes the Podesta emails.
These emails quote Clinton telling Wall Street Bankers
She has one position in public but another position in private.

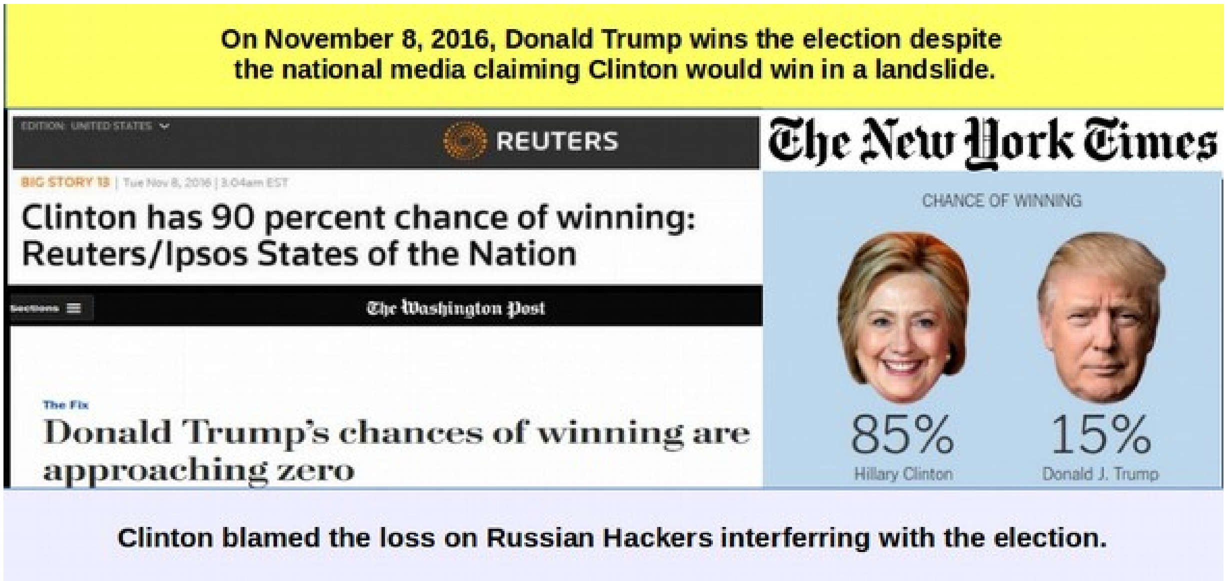
CLINTON SAYS YOU NEED TO HAVE A PRIVATE AND PUBLIC POSITION ON POLICY

Clinton: "But If Everybody's Watching, You Know, All Of The Back Room Discussions And The Deals, You Know, Then People Get A Little Nervous, To Say The Least. So, You Need Both A Public And A Private Position."

Wikileaks repeatedly denies that Russia is their source claiming instead that their source is a "disgusted Democratic Party insider."

November 8 2016: Media claims odds of Hillary winning as high as 90%.

But in a surprise (at least to the main stream media), Trump wins. Clinton was predicted to win Pennsylvania, Michigan and Wisconsin. She lost all of these Rust Belt states and several other states she was supposed to win. A fact rarely reported In the media is that folks in the rust belt states reported voting for Trump because he promised to get their jobs back while Clinton largely ignored the unemployment problem by falsely claiming their had been an economic recovery. It is not likely that the email scandal played more than a minor role in these Rust Belt states. Americans are not going to vote for Trump just because Putin wants them to. They voted for Trump because they thought he would help them get their jobs back. Here is the prediction from one news source on the day of the election predicting a Clinton win.



On November 8, 2016, Donald Trump wins the election despite the national media claiming Clinton would win in a landslide.

EDITION: UNITED STATES

REUTERS

BIG STORY 13 | Tue Nov 8, 2016 | 3:04am EST

Clinton has 90 percent chance of winning: Reuters/Ipsos States of the Nation

Sections ☰

The Washington Post

The Fix

Donald Trump's chances of winning are approaching zero

The New York Times

CHANCE OF WINNING

85% Hillary Clinton

15% Donald J. Trump

Clinton blamed the loss on Russian Hackers interferring with the election.

November 24, 2016 The Washington Post issued a story claiming that Russian propaganda help spread fake news through a list of 200 fake news websites.

CIA backed WaPo linking to a list by an anonymous group called Propornot – a group which was later confirmed to be associated with the US military. Some of the news websites on the list threatened to sue the Washington Post which amended the article on December 7 2016 by stating that they could not vouch for the credibility of the list. https://www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af66098fe_story.html?utm_term=.52946c5d5643

November 30 2016: Congress passed bill authorizing Ministry of Truth for 2017

Congress approved a measure within the National Defense Authorization Act for US State Department to act against propaganda with. The legislation authorized funding of $160 million over a two-year-period. While some claimed that the bill was a response to Russian hacking, the bill appears to have first been written in March 2016.

December 9, 2016: President Obama ordered US Intelligence Agencies to conduct an investigation into Russia's attempts to influence the 2016 US. election — and provide a report before he leaves office on January 20, 2017.

December 14 2016: Craig Murray, one of their leaders of Wikileaks said that their source was not a Russian but rather a "disgusted Democratic party insider."

http://www.dailymail.co.uk/news/article-4034038/Ex-British-ambassador-WikiLeaks-operative-claims-Russia-did-NOT-provide-Clinton-emails-handed-D-C-park-intermediary-disgusted-Democratic-insiders.html
Here is a quote from the Wikileaks Daily Mail article: 'Neither of [the leaks] came from the Russians,' Murray said. 'The source had legal access to the information. The documents came from inside leaks, not hacks. The leakers were motivated by 'disgust at the corruption of the Clinton Foundation and the tilting of the primary election playing field against Bernie Sanders."

December 16 2016: Digital Fingerprints Turn Out to be Paw Prints

US intelligence officials say that newly identified "digital fingerprints" indicate Moscow was behind the DNC hacks. The administration traced the hack to the specific keyboards -- which featured Cyrillic characters -- that were used to construct the malware code.

Apparently, the experts forgot that the NSA undoubtedly has Cyrillic Keyboards and uses them whenever they want to fool folks into thinking they are Russians Meanwhile, Russians are most likely to be using American key boards. http://abcnews.go.com/Politics/video/russias-digital-fingerprints-election-hacking-code-44248807

Cyber Security Analyst Justin Harvey claimed that the hack "called home to Russia and had a Russian signature." (Justin never bothered to provide the IP addresses confirming that the hackers called Russia – everything we have seen so far is hacks calling servers in countries friendly to the US). But back to Justin "It was written in Moscow's time zone and seemed to have gaps on Russian holidays. "**We saw the Cyrillic alphabet being used**." The beacon transmitted the hacked information to an IP address overseas that had been used in other Russian attacks. (an apparent reference to the Pakistan Crook Servers we debunked earlier. Justin Harvey has written several reports going back to June 2016 all of which agreed with Dimitri at Crowdstrike and one of which made the Godaddy server error. His background is with Fidelis, FireEye and Mandiant – all part of the NSA cyber network cheer leading for Crowdstrike).

Harvey said, the clearest evidence was the IP address that that malicious software used to phone home. "It was an IP address that had been previously seen in other Russian-attributed attacks, including the German parliament, the Bundestag, they encountered a breach last year with the same malware, the same IP address, and then also attributed to the Russians". (Another reference to the Pakistan Crook Servers we debunked earlier. Of course, no one would ever believe Justin if he explained that **the server being used was in Pakistan and run by a group called Crook Servers.)**

December 22, 2016: Smoking Gun Alert…Dimitri, Crowdstrike & Ukraine

Dimitri issued another fake report, this time claiming that Fancy Bear Russian Hackers who attacked the DNC had also used a Android App to infect Ukrainian military cell phones to target and kill them. Dimitri was actually interviewed by the PBS News Hour and NBC News about this. As we noted earlier, Dimitri is with the Atlantic Council. Here is a quote from another article about the hawkish nature of the Atlantic Council: "The Atlantic Council is funded in part by the US State Department, NATO, the governments of Latvia and Lithuania, the Ukrainian World Congress, and the Ukrainian oligarch Victor Pinchuk—has been among the loudest voices calling for a new Cold War with Russia. As I pointed out in the pages of *The Nation* in November, the Atlantic Council has spent the past several years producing some of the most virulent specimens of the new Cold War propaganda." https://www.thenation.com/article/is-skepticism-treason/

Once again, it turns out that Dimitri's claims are not just not supported, they have been proven to be false. The guy who actually made the Android App called the Crowdstrike report "delusional" noting that if the App was infected it would easily have been spotted. A technical advisor to the Ukrainian military then tracked down the Ukrainian units that used the App and found that **they "reported no losses"** - thus completely contradicting the claims made by Dimitri of massive losses. Here is a quote from the Ukrainian military advisor: "I personally know hundreds of gunmen in the war zone. **None of them told me of D-30 losses caused by hacking or any other reason,"** Narozhnyy stressed to the

VOA. The article noted that some malware was found on some Android phones. But instead of the malware reporting to Russian servers, it was reporting to servers in the US! http://www.voanews.com/a/skeptics-doubt-ukraine-hack-link-to-dnc-cyberattack/3649234.html

Here is what security consultant Jeffrey Carr has to say about Dimtri's delusional report: "Crowdstrike's latest report regarding Fancy Bear contains its most dramatic and controversial claim to date; that GRU-written mobile malware used by Ukrainian artillery soldiers contributed to massive artillery losses by the Ukrainian military. "It's pretty high confidence that Fancy Bear had to be in touch with the Russian military," Dmitri Alperovich told Forbes.

Crowdstrike's core argument has three premises:
#1: Fancy Bear (APT28) is the exclusive developer and user of X-Agent [1]
#2: Fancy Bear developed an X-Agent Android variant specifically to compromise an Android ballistic computing application called Попр-Д30.apk for the purpose of geolocating Ukrainian D-30 Howitzer artillery sites[2]
#3: The D-30 Howitzers suffered 80% losses since the start of the war.[3]

If all of these premises were true, then Crowdstrike's prior claim that Fancy Bear must be affiliated with the GRU [4] would be substantially supported by this new finding. Dmitri referred to it in the PBS interview as "DNA evidence". In fact, none of those premises are supported by the facts. This article is a summary of the evidence that I've gathered during hours of interviews and background research with Ukrainian hackers, soldiers, and an independent analysis of the malware by CrySys Lab. My complete findings will be presented in Washington D.C. next week on January 12th at Suits and Spooks.

X-Agent Is In The Wild
Crowdstrike, along with FireEye and other cybersecurity companies, have long propagated the claim that Fancy Bear and all of its affiliated monikers (APT28, Sednit, Sofacy, Strontium, Tsar Team, Pawn Storm, etc.) were the exclusive developers and users of X-Agent. We now know that is false.

No GPS functionality in the malware or the original application
The first iteration of the POPR-D30 Android app designed by Ukrainian military officer Jaroslav Sherstuk (and the only iteration allegedly impacted by this malware) was a simple ballistics program that calculated corrections for humidity, atmospheric pressure, and other environmental factors that determine accuracy of the D-30 Howitzer. It did not have the capability to connect to WiFi, nor to receive or transmit any data.[6]
The Android APK malware doesn't use GPS nor does it ask for GPS location information from the infected phone or tablet.[7] That's a surprising design flaw for custom-made malware whose alleged objective was to collect and transmit location data on Ukrainian artillery to the GRU.

In Eastern Ukraine, mobile phone service was poor even before the war. It has only grown worse since. In fact, Crowdstrike hasn't provided any evidence that the malware-infected Android app was used by even a single Ukrainian soldier.

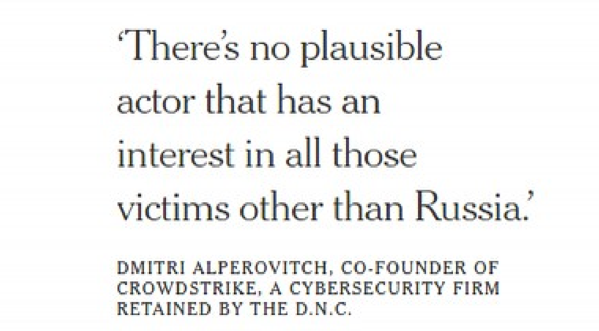
Conclusion
Part of the evidence supporting Russian government involvement in the DNC and related hacks (including the German Bundestag and France’s TV5 Monde) stemmed from the assumption that X-Agent malware was exclusively developed and used by Fancy Bear. We now know that’s false, and that the source code has been obtained by others outside of Russia. The GRU, according to Crowdstrike, developed a variant of X-Agent to infect an Android mobile app in order to geolocate and destroy Ukraine’s D-30 howitzers. To do this, they chose an artillery app which had no way to send or receive data, and wrote malware for it that didn’t ask for GPS position information? Crowdstrike never contacted the app’s developer to inform him about their findings. Had they performed that simple courtesy, they might have learned from Jaroslav Sherstuk how improbable, if not impossible, their theory was.

Major media outlets including the The Washington Post, CNN, NBC News, and PBS Newshour ran the story without fact-checking a single detail. Motherboard, Forbes, SC Magazine, and other media did the same. Only VOA and Bloomberg took the time to question Crowdstrike’s claims and do some of their own investigating. Crowdstrike invented a “devastating” cyber attack out of thin air and called it DNA evidence of Russian government involvement.

https://medium.com/@jeffreycarr/the-gru-ukraine-artillery-hack-that-may-never-have-happened-820960bbb02d#.whzgobmeu

In short, the primary basis for claiming that Fancy Bear is Russian (the monopoly of X Agent) has been proven to be false.

If you need still more evidence that Dimitri is not trustworthy, here is some more information about Dimitri and Crowdstrike:
Here is Dmitri claiming that the only nation interested in hacking people is Russia.
http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0



‘There’s no plausible actor that has an interest in all those victims other than Russia.’

DMITRI ALPEROVITCH, CO-FOUNDER OF CROWDSTRIKE, A CYBERSECURITY FIRM RETAINED BY THE D.N.C.

I guess Dmitri is unaware that the NSA motto is **“Hack Everything.”** This is strange because Dmitri is also a group linked to the FBI and CIA called the Atlantic Council. President Obama’s National Security Advisor, James Jones is the former head of the Atlantic Council. Other members include famous war hawks like Chuck Hagel, Susan Rice and Richard Holbrooke. As for funding, Crowdstrike not only gets funding from Google but also from the US State Department. (Just go to their donor page to see the entire list).

This brings up an important question: Why is the US State Department funding this obviously war hawk group?

If this were not enough, the President of Crowdstrike, Shawn Henry was the former head of the FBI Cyber Division. No wonder the FBI agrees with and promotes Crowdstrike!

Perhaps that is just a coincidence. But news articles about and by CrowdStrike suggest they exist to ratchet up cyber-war tensions with Russia, China, and North Korea based on hyped-up network security «vaporware» products they sell at top dollar prices to tech-ignorant government customers.
http://www.strategic-culture.org/news/2016/12/25/obama-halloween-temperamentally-president-war-with-russia.html

We will get back to this "Cyber Warfare as a Business Model" in a minute. First, we need to review the Grizzly Steppe Report.

Part 5 DHS/FBI Grizzly Steppe Report..December 29 & 30, 2016

December 29 2016: The DHS/FBI Grizzly Steppe Report Turns out to be Proof that the NSA does not like the TOR Project

The Department of Homeland Security and the FBI release a joint report which they claim provides evidence of Russian Hacking of the US Election. In fact, there is no evidence in the report linking Russia to anything. But there is plenty of evidence linking the attacks to the NSA.
https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

The "alternative names list" for the Russian hacking programs on page 4 specifically referred to in the DHS/FBI report included the following: Cozy Bear, Cozy Duke, Cosmic Duke, Fancy Bear and MiniDuke.

On December 29, 2016, the US government published Grizzly Steppe accusing Russia of hacking the DNC in a plot to "affect the US election."
Putin is Cozy Bear & Fancy Bear!
NO I'M NOT!
GRIZZLY STEPPE "OFFICIAL REPORT"
Putin denies the allegations and calls Obama a sore loser who is making stuff up.

As justification for launching a cyber war against Russia, on page 5 of their press release, the US government also falsely accused the Russians of creating a hacking program called **PAS_TOOL_PHP_WEB_KIT.** This web kit is a commonly available hacking program that even you can download. The following article claims that this program was made by Ukrainians not Russians.
https://www.wordfence.com/blog/2016/12/russia-malware-ip-hack/

The DHS/FBI press release and numerous main stream media reports also noted that several private cyber security consultants agreed that the Russians were responsible for hacking the DNC and specifically that Fancy Bear and Cozy Bear were involved in the DNC attacks. For example, see the following fake news from NBC:
http://www.nbcnews.com/news/us-news/cozy-bear-explained-what-you-need-know-about-russian-hacks-n648541

NEWS SEP 15 2016, 7:18 AM ET

Cozy Bear Explained: What You Need to Know About the Russian Hacks

December 30 2016 Glaring Problems with the Grizzly Steppe Report

Beginning on December 30, 2016, several articles were written exposing problems with the Grizzly Steppe report. I wrote an article with screen shots of the data file and an analysis of many of the IP addresses. This analysis showed that the IP addresses had no link to the Russians. You can read this short report at this link: https://turningpointnews.org/exposing-political-corruption/dhs-fbi-claim-of-russian-hacking-is-fake-news

TOR Exit Nodes… The Real Smoking Gun

In my report, I provided research on several domain names and IP addresses provided in the Grizzly Steppe report. My research showed that none of the domain names or IP addresses had any relationship to Russian hackers. But one of the IP addresses was a TOR Exit Node. Here is a quote from my report:

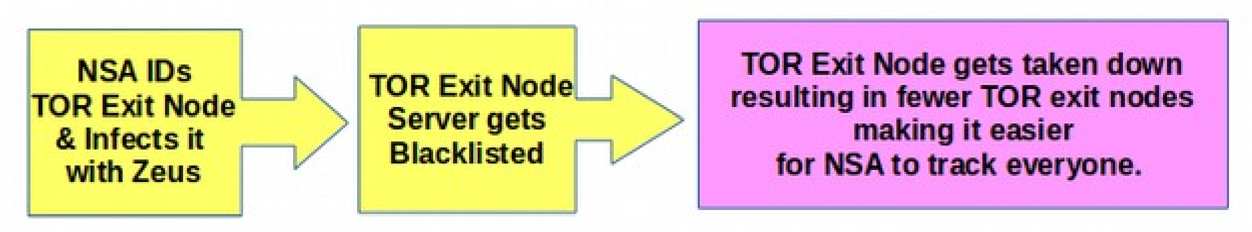
“178.20.55.16 is a proxy server with no known location but has been used as a TOR router exit node. A proxy server is another name for a mirror or server used to bounce information from one server to another in order to hide the true location of the original server. This proxy server is associated with the domain name **nos-oignons.net**. This domain name was registered on December 31 2012 and is valid until December 31 2017. In other words, whoever got this domain name paid for its use for 5 years. But they did registered the domain name anonymously. The website associated with this server appears to be a group in France promoting the TOR router. They became an association in May 2013 – 5 months after getting the domain name. The group currently has 5 members and it costs one Euro to join this group. Their website was reported 9 days ago as having been infected with the Zeus virus. This infection does not leave tracks on server logs. So it is difficult to tell where it came from. **Removal of this virus requires a complete rebuild of the server.** In short, some agency decided to take out this server and then use it to make a cyber attack on some US government agency and thus have the IP address listed on the DHS-FBI list as one of 895 indicators of Russian hacking.”

As discussed earlier in this report, research by others has now confirmed that there were 426 TOR exit nodes on the Grizzly Steppe list. Thus about half of the Grizzly Steppe list were TOR exit nodes. More important, since there are only about 1,000 TOR exit nodes in the entire world, about 42% of all TOR exit nodes were on the Grizzly Steppe list. Since the general public has no idea what TOR is and why this is important in terms of linking the NSA to the DNC hacks, we will provide a brief explanation of TOR.

What is TOR?
TOR stands for the **The Onion Router.** The Onion Router is a web browser, similar to Firefox or Google Chrome. But it is also a network of proxie servers used to hide the idenity and location of the person visiting the TOR web browser. The route taken by the data is passed through several TOR IP addresses bouncing the signal all around the world. The only thing that can be confrimed is the final step in this path. The final step is called a TOR exit nodes. Anyone, including the NSA can tell the location and identity of the server at the final step. Because the NSA does not like people hiding from them, the NSA does not like TOR. The NSA therefore has a long and ugly history of attacking TOR exit nodes (as well as attacking the TOR home website). TOR exit nodes take great risks in that they stand in the way of the most powerful hacking group in the world – the NSA.

How the NSA attacks TOR exit nodes is very devious. But I did briefly explain this in my previous article on December 30, 2016. Basically, the NSA attacks the server that the exit node website is located on and infects the server with a very bad virus. Zeus is only one of several viruses used by the NSA. Also the NSA is not the only one using Zeus to infect websites and servers as Zeus is readily available on the Internet.

As I stated in my prior article, once the server is infected, folks begin to file complaints about it to blacklisting agencies. The servers are quickly blacklisted and their content is no longer shown. The company owning the infected server needs to take it off line and clean it up (not an easy process) before putting it back up. The server then needs to prove to the black listing agencies that it is completely clean before traffic is restored. Here is a diagram of this NSA TOR server take down process:



This is why the presence of such a huge number of TOR exit nodes in the Grizzle Steppe list is so alarming. It is clearly a smoking gun that **the Grizzly Steppe list is a list of servers being targetted by the NSA.** Since this is also a list of IP addresses that have been associated with Fancy Bear and Cozy Bear, we can conclude that there is some relationship between Fancy Bear and Cozy Bear to the NSA. If Russia were really Fancy Bear or Cozy Bear, they would not be using TOR exit nodes for the simple reason that TOR is one of the biggest threats to total NSA domination of the Internet. In addition, they would not use TOR exit nodes because they are certainly aware that TOR Exit Nodes are being targeted and taken down by the NSA. Russian hackers know which servers are TOR exit node servers because TOR publishes a list of these servers. Here is a link to this list: https://check.torproject.org/exit-addresses

It would be a simple matter for Russian hackers to use servers that are not TOR exit node servers. Thus, the Grizzly Steppe IP list is proof that Cozy Bear and Fancy Bear are not related to Russian Hackers. They are NSA hackers. Here is a link to the TOR website where you can download TOR and learn more about it. https://www.torproject.org/

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

What is Tor?

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Learn more about Tor »

Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Recent Blog Posts

Tor at the Heart: The Tor Project
Sat, 31 Dec 2016 Posted by: ssteele

Tor at the Heart: Firefox
Fri, 30 Dec 2016 Posted by: ssteele

Tor at the Heart: Notes from a B...
Thu, 29 Dec 2016 Posted by: ssteele

Tor Messenger 0.3.0b2 is released
Thu, 29 Dec 2016 Posted by: sukhbir

Tor at the Heart: Qubes OS
Wed, 28 Dec 2016 Posted by: ssteele

View all blog posts »

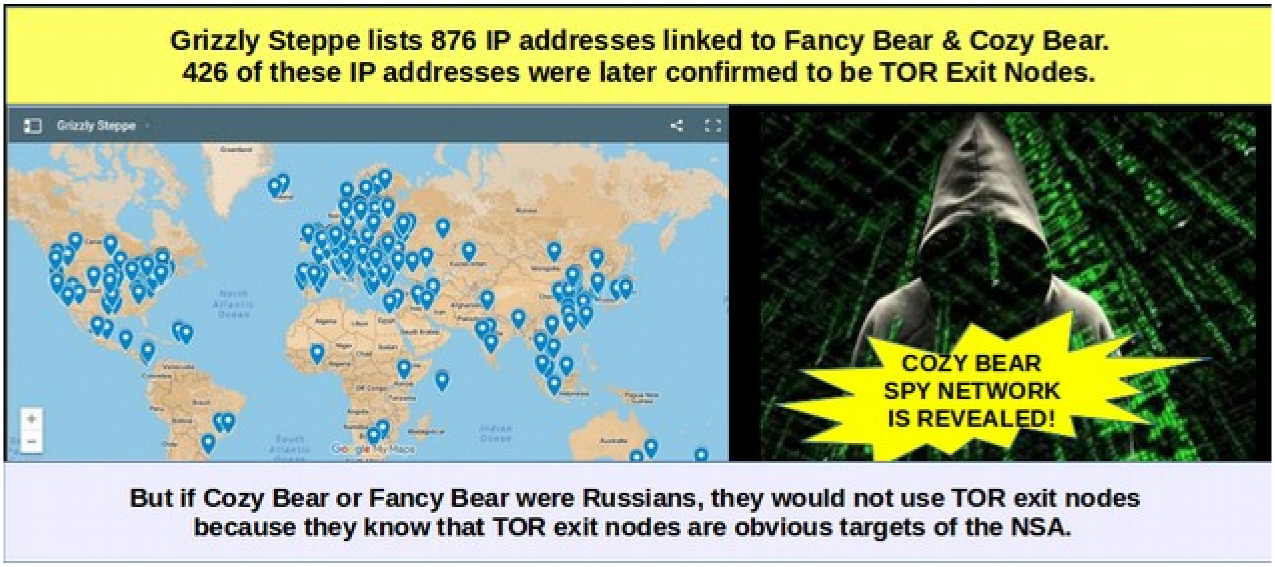
Who Uses Tor?

Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet.

There were several other excellent articles shooting holes in the DHS/FBI report. This is a brief summary of two of the best that provided very strong evidence that Russia was not involved in the hacking of the DNC:

#1 TOR EXIT NODES IMPLICATE NSA AS THE DNC HACKER: The 876 alleged Russian Hacking attacks in the DHS/FBI report come from IP addresses in 62 countries all over the world. Nearly half of them (49%) are TOR Exit nodes. Here is a map of attacks:



Grizzly Steppe lists 876 IP addresses linked to Fancy Bear & Cozy Bear.
426 of these IP addresses were later confirmed to be TOR Exit Nodes.

But if Cozy Bear or Fancy Bear were Russians, they would not use TOR exit nodes because they know that TOR exit nodes are obvious targets of the NSA.

http://jerrygamblin.com/2016/12/30/grizzly-steppe-ip-and-hash-analysis/

As I noted in my first report, these IP addresses are mostly outside of Russia with the US being the most common location. 367 of these IP addresses (or 42% of the total in the report) are now or in the past were TOR Exit Nodes meaning that anyone can use them. https://theintercept.com/2017/01/04/the-u-s-government-thinks-thousands-of-russian-hackers-are-reading-my-blog-they-arent/

Here is a quote from the above link:
"I found out, after some digging, that of the 876 suspicious IP addresses that the Department of Homeland Security and the Department of National Intelligence put on the Russian cyber attacker list, at least 367 of them (roughly 42%) are either Tor exit nodes right now, or were Tor exit nodes in the last few years...(using a more complete data set of historical TOR exit nodes), it turns out that **426 of the IP addresses in the Grizzly Steppe report are historical Tor nodes, so it's actually 49%** rather than 42%."

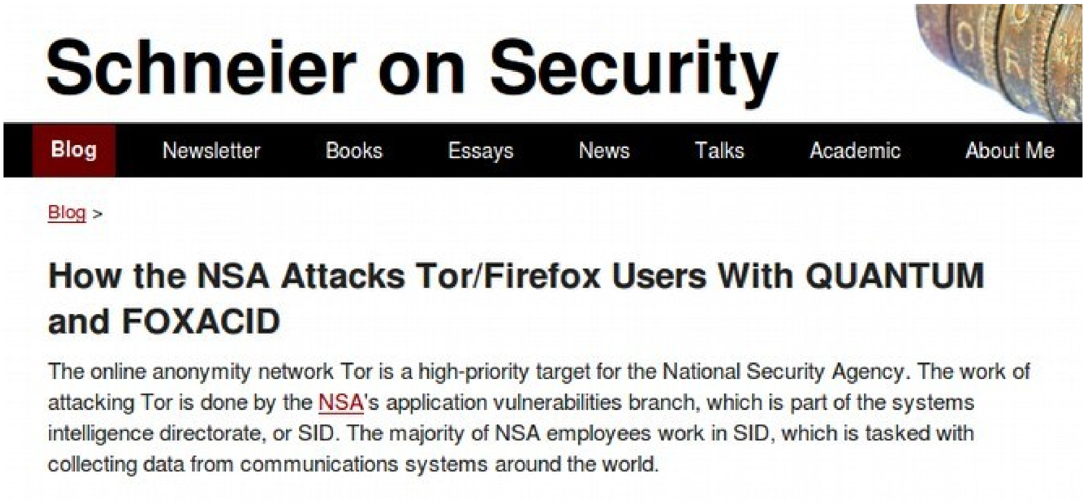
Many more of these Grizzly Steppe IP addresses are public broadband servers also easily accessed by almost anyone. I understand that hackers can create bot nets which combine thousands of hacked servers together to make Denial of Service attacks. But that is not what the DHS/FBI report is alleging. They are alleging 876 separate hacking attacks from 876 separate servers.

Our prior article diligently reviewed many of these Grizzly Steppe IP addresses and could not find any link at all to the Russian government. But we did find some links to the NSA. For example, we provided a link to a hacked TOR node in France. Over 300 of the IP addresses provided in the DHS/FBI report are from **hacked** TOR Exit nodes – meaning that these exit nodes have been blacklisted and will soon be taken off line. Such a massive attack against the TOR project is devastating because there are only about 1000 TOR exit nodes in the entire world. https://metrics.torproject.org/relayflags.html

Whoever Cozy Bear and Fancy Bear are, they seem to be interested in taking down the TOR project. Who in the world would want to get rid of so many TOR exit nodes??? TOR exit nodes provide an important public service by allowing folks to surf the Internet anonymously. The TOR anonymous web browser has about 1.5 million daily users. Getting rid of the exit nodes would be the end of the line for the Tor Project.

It turns out that the NSA does not like TOR because it makes hacking harder for the NSA. The NSA has been known to attack the TOR project in the past. In fact, according to documents leaked by Edward Snowden, the NSA uses three or more cyber weapons to attack the TOR project and has referred to the TOR project as one of their biggest obstacles in their drive for "Total Awareness." These weapons are called Quantum, Foxacid and XkeyScore.

Here is an article that discusses these attacks calling TOR a "high priority target of the NSA":
https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html



Schneier on Security

Blog >

How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID

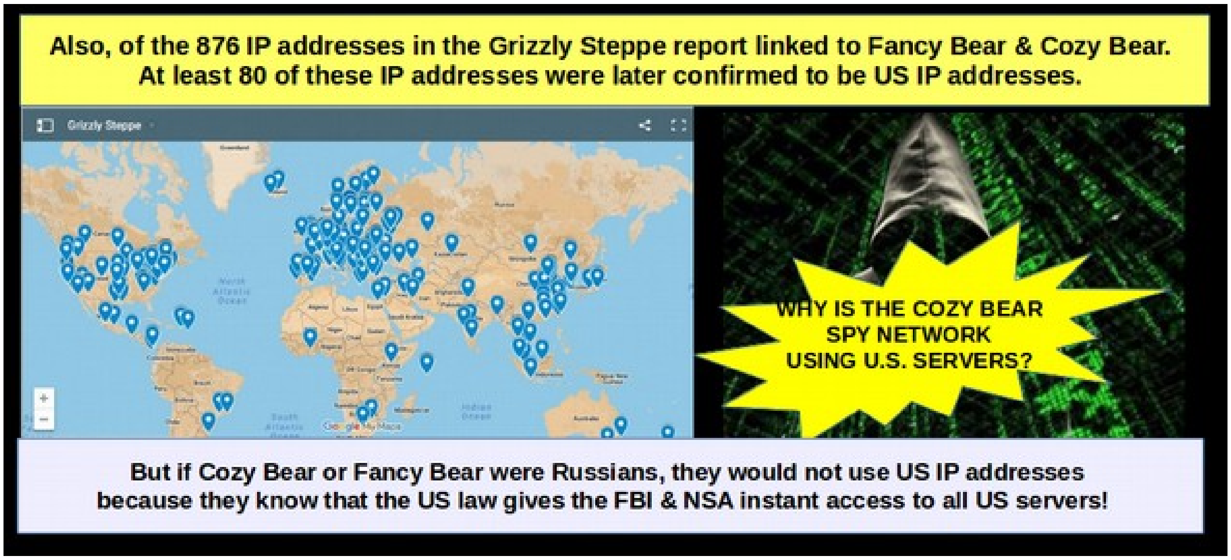
The online anonymity network Tor is a high-priority target for the National Security Agency. The work of attacking Tor is done by the NSA's application vulnerabilities branch, which is part of the systems intelligence directorate, or SID. The majority of NSA employees work in SID, which is tasked with collecting data from communications systems around the world.

The fact that 426 of the IP addresses are or were TOR exit nodes most of which were hacked is further strong indication that the above IP map implicates the NSA rather than the Russians. The NSA has been attacking TOR exit nodes for years in an attempt to get rid of TOR. The list of 876 IP addresses provided in the DHS/FBI report does confirm that Cozy Bear and Fancy Bear have been active. But this list also supports my claim that Cozy Bear and Fancy Bear are NSA hacking projects – not Russian hacking projects.

Moreover, the NSA has the money to be hacking sites in 62 countries whereas the Russians have a more limited budget and cannot afford to be hacking computers in 62 countries.

Why Russian Hackers would not use US Servers to Call Home

In addition to 426 of the Cozy Bear/ Fancy Bear servers being TOR exit nodes, over 80 servers had IP addresses located in the US.



Also, of the 876 IP addresses in the Grizzly Steppe report linked to Fancy Bear & Cozy Bear. At least 80 of these IP addresses were later confirmed to be US IP addresses.

But if Cozy Bear or Fancy Bear were Russians, they would not use US IP addresses because they know that the US law gives the FBI & NSA instant access to all US servers!

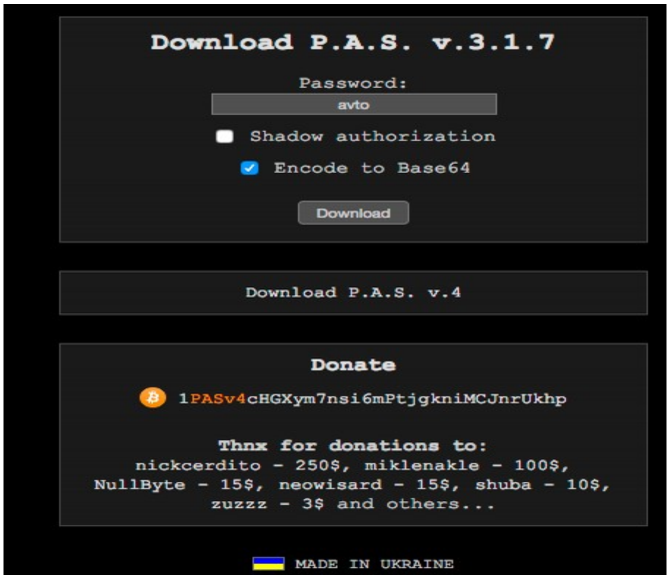
In addition, over 90% of the IP addresses were in countries friendly to the US. Even the IP addresses located in Russia were found to be broadband addresses available to the general public. It is unlikely that Russian hackers would be using any of these IP addresses for their spy network.

Let us be clear. We are not at all saying that the Russians never hack US computers. We have no doubt that the Russians try to access US government computers on a daily basis (as do many other governments and as do a bunch of teenagers from from across the US). Talk to any hacker at a hacker conference and you will find out that nearly all of them would like to hack US government servers. This is just how hackers are. They like a challenge. We are simply reviewing the evidence for Cozy Bear and Fancy Bear because the DHS/FBI report claimed that they were both Russian hacking programs. Our review of the evidence indicates that these programs are not Russian programs but NSA programs.

#2 The DHS/FBI claim that a PHP script was evidence of Russian hacking proven to be false

On page 5 of their press release, the US government falsely accused the Russians of creating a hacking program called **PAS_TOOL_PHP_WEB_KIT.** Here is a link to a report which goes into detail on why this PHP script cited by DHS/FBI was not evidence of Russian hacking.
https://www.wordfence.com/blog/2016/12/russia-malware-ip-hack

The authors easily obtained the PHP script by googling it which led to this download link:
http://profexer.name/pas/download.php



Download P.A.S. v.3.1.7

Password: avto

□ Shadow authorization

☑ Encode to Base64

Download

Download P.A.S. v.4

Donate

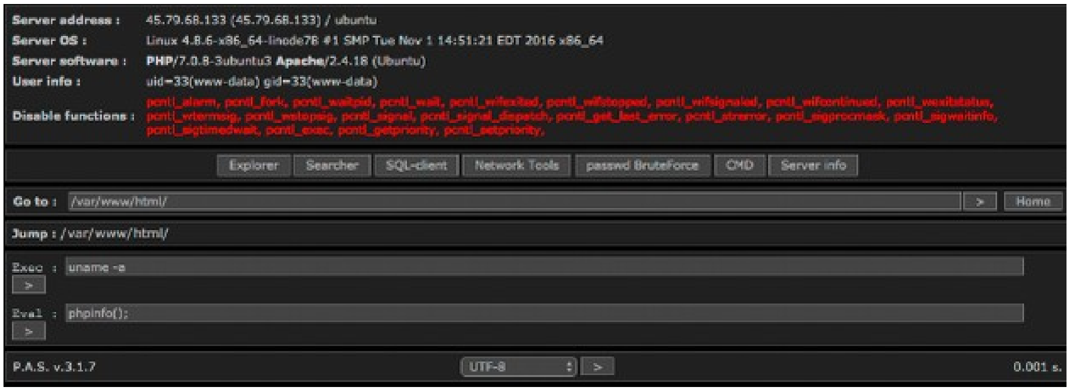
₿ 1PASv4cHGXym7nsi6mPtjgkniMCJnrUkhp

Thnx for donations to:
nickcerdito - 250$, miklenakle - 100$,
NullByte - 15$, neowisard - 15$, shuba - 10$,
zuzzz - 3$ and others...

MADE IN UKRAINE

Note the Ukrainian flag and the claim it was “Made in Ukraine”. This is pretty typical of the NSA coders sense of humor. You can make a donation to the hacking team by clicking on an anonymous Bitcoin link. This is also typical NSA humor. The latest version of this hacking program, which is intended to hack Wordpress websites, is version 4.1.1.

Here is what the control panel of this hacking program looks like:



```
Server address :    45.79.68.133 (45.79.68.133) / ubuntu
Server OS :         Linux 4.8.6-x86_64-linode78 #1 SMP Tue Nov 1 14:51:21 EDT 2016 x86_64
Server software :   PHP/7.0.8-3ubuntu3 Apache/2.4.18 (Ubuntu)
User info :         uid=33(www-data) gid=33(www-data)
                    pcntl_alarm, pcntl_fork, pcntl_waitpid, pcntl_wait, pcntl_wifexited, pcntl_wifstopped, pcntl_wifsignaled, pcntl_wifcontinued, pcntl_wexitstatus,
Disable functions : pcntl_wtermsig, pcntl_wstopsig, pcntl_signal, pcntl_signal_dispatch, pcntl_get_last_error, pcntl_strerror, pcntl_sigprocmask, pcntl_sigwaitinfo,
                    pcntl_sigtimedwait, pcntl_exec, pcntl_getpriority, pcntl_setpriority,

Go to : /var/www/html/
Jump : /var/www/html/
Exec : uname -a
Eval : phpinfo();
P.A.S. v.3.1.7                    UTF-8                    0.001 s.
```

This free and handy open source hacking program includes a file browser, a file search function, a database to download the contents of a hacked site database, a scanner, a tool to view server configuration files and a tool to brute force attack passwords. Best of all, all of the instructions and the control panel itself are written in English – no need to learn Russian!

Every American should be disgusted and alarmed that this easily available program was attributed to the Russians in the DHS/NSA Report and this same program is now being used as an excuse to launch a cyber warfare attack against Russia. This madness has to be stopped. Please share this information with everyone you know!

December 30, 2016 Security Expert John McAfee Explains why he is certain the Russians did not hack the DNC

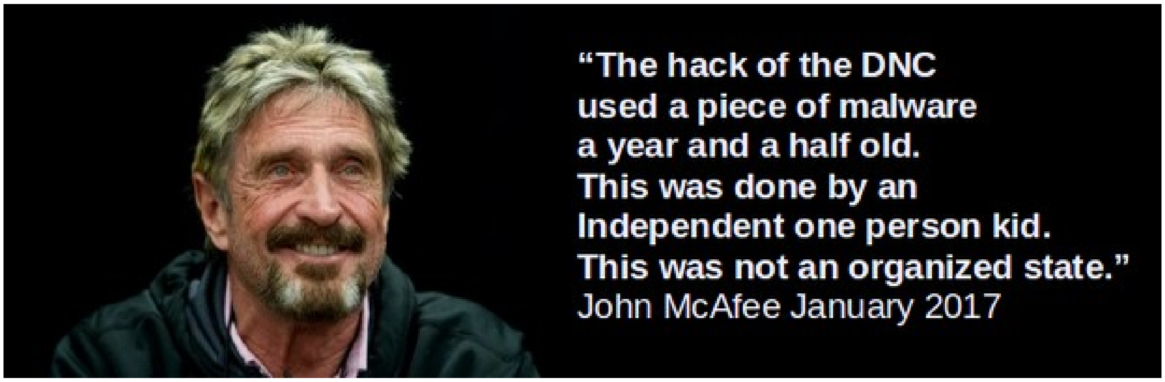
This is a quote from a TV interview:
"When the FBI or any other agency says the Russians did it or the Chinese did it, or the Irans did it, that is a fallacy. Any hacker capable of breaking into something is capable of hiding their tracks. If I were the Chinese and I wanted to make it look like the Russians did it, I would use Russian language within the code. I would use Russian techniques for breaking into an organization. So there is simply no way to assign a source for any attack. This is a fallacy. This is what the FBI wants us to believe so they can manipulate our opinions. I can promise you this. If it looks like the Russians did it, then I can guarantee you it was not the Russians."
https://www.youtube.com/watch?v=aDTKKmBjlwE

John then appeared on another show and said he thought it might be a 15 year old boy since the person made some basic errors. Here is a quote from John:

"The hack on the DNC used a piece of malware a year and a half old. This was done by an independent one person kid. This was not an organized state that did this. "We have many cyber weapons but we have no protection. We have no security. If we did, our country could not have been hacked by a 15 year old boy."

“The Grizzly Steppe Report is not just flimsy. It is propaganda intended to incite the American people.”
https://www.youtube.com/watch?v=C2jD4SF9gFE
https://www.rt.com/usa/372219-larry-king-mcafee-cybersecurity/#.WGaDFP9c4q4.facebook

John has been interviewed on several TV and Radio shows and is likely the leading proponent of the theory that the DNC was really attacked by teenagers.



In fact, it was the 2015 German hack that used a piece of malware a year and a half old and therefore was likely done by a teenager. We have no idea what version of software was used in the DNC hack because the FBI never did an investigation and Crowdstrike has never released the source data (merely making claims about the source data that it was linked to the German attack).

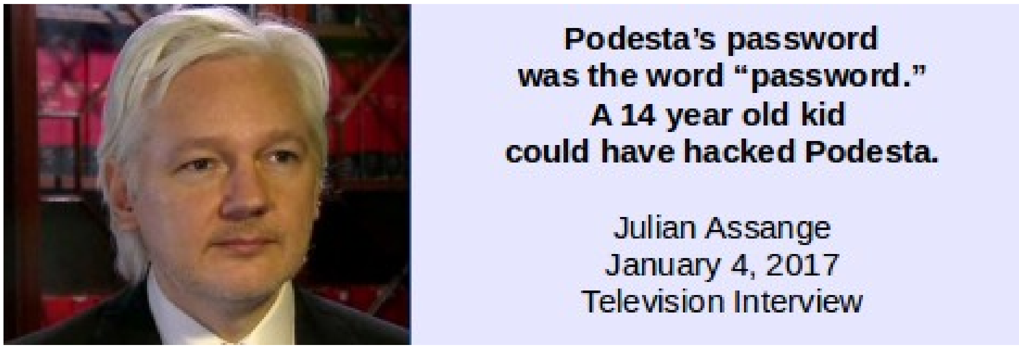
We have great respect for John and will consider his argument in more detail later in this report.

Part 6 The Rush to War... January 2017 to Present

Things have only gone from bad to worse in the first weeks of January 2017. Nearly every day we are told that there is “new evidence” of Russian hacking. But the new evidence is never released.

January 3, 2017: Julian Assange Explains Why a 14 Year Old Could Have Hacked Podesta’s Email

Julian Assange of WikiLeaks says that the Russian government did not provide him with the hacked DNC emails during a televised interview. Julian Assange stated that Podesta’s password for his Gmail account was “password.” For those who may not know, the word password is the most common password and is the first password checked by hackers when trying to access any login screen. Here is a quote from the interview: **"Podesta gave out that his password was the word ‘password’ ... a 14-year-old kid could have hacked Podesta."**
http://www.foxnews.com/politics/2017/01/04/wikileaks-assange-14-year-old-kid-could-have-hacked-podesta-emails.html



Podesta’s password was the word “password.” A 14 year old kid could have hacked Podesta.

Julian Assange
January 4, 2017
Television Interview

Assange also repeatedly stated that Wikileaks gained access to the Podesta emails from a leak and not a hack and that the source of the leak was not Russia. Assange, who is a former computer security consultant, also stated that Hillary Clinton made “almost no attempt” to protect the private server that stored her State Department emails. I have previously written about how insecure the Clinton server was and that any teenager could have hacked it using programs and methods available through a simple Google search. While the main stream media claims that the Clinton server was hacked by Guccifer and that Guccifer was Fancy Bear or Cozy Bear and therefore a Russian spy, the fact is that Guccifer could just have easily been a bored American teenager with too much time on his hands.

January 5 2017: John McCain, who has called for a Declaration of War against Russia, holds a Senate Armed Services Committee hearing

Called “Foreign Cyber Threats to the US.” John Brennan (CIA), James Clapper (ODNI), Michael Rogers (NSA) and Marcel Lettre (Undersecretary of Defense for Intelligence) were given a chance to make their case for Russian hacking. However, no new information was released during this hearing. However all agreed that Julian Assange is a dirtbag criminal who has cost American lives and should not be trusted. (In fact, there has never been a showing of a single life lost as a result of Wikileaks disclosures).

But as we have seen in this report, the truth does not appear to matter to US leaders in their attempts to drum up hatred towards Russia.

January 5, 2017 DNC says FBI never asked to access hacked computer servers

Despite the fact that not one but two major crimes had been committed on the DNC server, the DNC stated today that the FBI "never requested access" to the servers the White House and intelligence community say were hacked by Russia.
https://www.buzzfeed.com/alimwatkins/the-fbi-never-asked-for-access-to-hacked-computer-servers?utm_term=.ycBJbXdoz#.ws75WGR9O
Here is a quote: "Six months after the FBI first said it was investigating the hack of the Democratic National Committee's computer network, the bureau has still not requested access to the hacked servers, a DNC spokesman said. No US government entity has run an independent forensic analysis on the system, one US intelligence official told BuzzFeed News."

January 6, 2017: FBI claims DNC Refused to Give them Access to Hacked DNC Server

A day later, the FBI disputed this claim by stating that they had asked to examine the DNC server logs in May 2016 – but the DNC refused their request.
https://www.wired.com/2017/01/fbi-says-democratic-party-wouldnt-let-agents-see-hacked-email-servers/

Here is a quote: "According to the FBI official, this left the FBI no choice but to rely upon a third party for information. These actions caused significant delays and inhibited the FBI from addressing the intrusion earlier."

This is an important issue. So I will repeat my questions about this from earlier in this report: **Since when does the FBI have to get anyone's permission, other than a judge, to seize evidence after a major crime has been committed?** Had the FBI gotten the server and the DNC taken steps to clean the server, we would not today be faced with the difficult task of figuring out who hacked the DNC – and possibly the DNC would not have lost the national election – an election on which they spent over one billion dollars trying to win. The failure of the FBI to take this action is one of many questions that has never been adequately addressed.

January 6, 2017 Hackers try to break into DNC on New Years Eve

This proves beyond any reasonable doubt that these people have no idea what they are talking about. Hackers likely are trying to break into the DNC server and every other server in the US on a daily basis. Yet the DNC appears to be shocked, shocked, that someone is still trying to break into their servers. That is like being shocked to discover that people are gambling in Las Vegas. Please. Join the modern world.
www.buzzfeed.com/alimwatkins/hackers-tried-to-break-into-dnc-computers-right-before-new-y?utm_term=.tv0OnNM9B#.aqWxZBGlV

Here is a quote: “Officials told BuzzFeed News that hackers had been trying to infiltrate the DNC as recently as five days ago...The FBI alerted the Democratic National Committee as recently as New Year’s Eve that hackers were once again trying to break into their computer systems… there have been “multiple attempts” to hack into the DNC since the Nov. 8 elections. Many of these attempts are not serious… hackers are trying to re-enter the DNC system but as far as we understand their attempts have not been successful.”

Given that nearly every website in the US is subjected to hacking attacks on almost a daily basis, it is absurd for either the FBI or the DNC or the press to think there is something news worthy about the fact that the DNC hacks are ongoing.

January 6 2017 US Intel Report claims to ID Russian who gave emails to Wikileaks
Here is a quote from the article. “The CIA has identified Russian officials who fed material hacked from the Democratic National Committee and party leaders to WikiLeaks at the direction of Russian President Vladimir Putin through third parties, according to a new U.S. intelligence report, senior U.S. officials said on Thursday. The officials, who spoke on condition of anonymity, said the Central Intelligence Agency and others have concluded that the Russian government escalated its efforts from discrediting the U.S. election process to assisting President-elect Donald Trump's campaign.”
http://www.reuters.com/article/us-usa-russia-cyber-celebrate-idUSKBN14P2NI

See anything at all that looks remotely like actual evidence? Neither did I. The report did state that there would be another report later in the day providing some evidence. But still no evidence. Plenty of allegations. No evidence. Check that. Apparently the evidence was that some Russians in Moscow were drinking champagne when Trump won on November 8 2016. One drunken Russian claimed that he helped Trump win. Well I guess that does it. In a moment, we will reveal who the drunken Russian was.

January 6 2017 US Intelligence Groups Issue the Dumbest Report I Have Ever Read

It was called “Assessing Russian Activities and Intentions in the Recent US Elections.” If you are a glutton for punishment, then feel free to read the US Intelligence Agencies Report claiming Russia hacked not just the Clinton servers but engaged in a massive propaganda campaign to influence the US election in 2016. Here is the link:
https://www.dni.gov/files/documents/ICA_2017_01.pdf

We do not have the space or time to review all of the errors and omissions in this report, so we will only discuss four of their ridiculous claims.

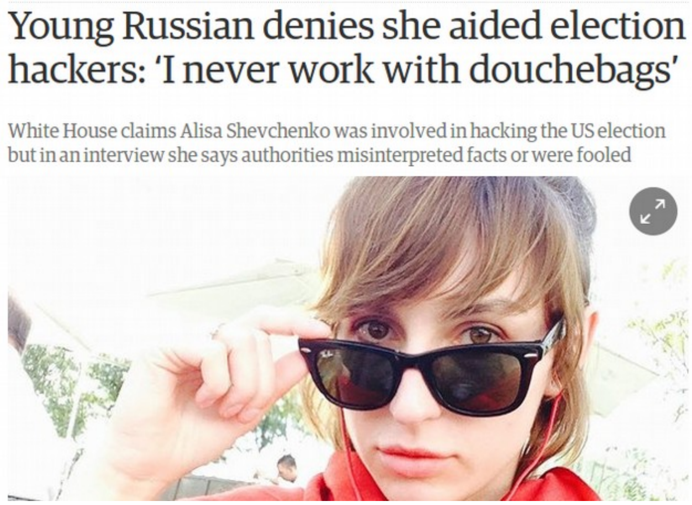
First, the report notes that **Dmitry Kiselyov**, an RT commentator (the Kremlin’s “chief propagandist”) has treated Donald Trump sympathetically on his television show and that somehow this influenced the US election. But someone please explain this: how does a television show in Russian for Russians indicate the Kremlin’s intention to meddle in the U.S. democratic system? The RT channel is only carried on 15% of US cable providers. It is likely that less than one percent of all Americans watches anything at all on RT. I bet less than one percent of all Americans have ever even heard of Kiselyov. I know I haven’t ever heard of him – and I watch several shows on RT! The idea that some completely unknown Russian commentator had any influence on the US election is absurd.

Second, the report claims that a girl named **Alisa Shevchenko** was involved in hacking the US election but in an interview she says they “misinterpreted facts or were fooled.” https://www.theguardian.com/world/2017/jan/06/russian-hacker-putin-election-alisa-shevchenko

Here is a quote from the article: “Alisa Shevchenko is a talented young Russian hacker, known for working with companies to find vulnerabilities in their systems. She is also, the White House claims, guilty of helping Vladimir Putin interfere in the US election. Her company was a surprise inclusion on the US sanctions list released last week, alongside top officers in Russia’s GRU military intelligence agency and two well-known criminal hackers. The company “provided the GRU with technical research and development”, according to the fact sheet released by the White House. No further details were given.” “Shevchenko has spoken out to decry the sanctions against her. Shevchenko told the Guardian she was furious at her company’s inclusion on the list, and denied ever having knowingly worked for the Russian government. In answers that were defiant, and occasionally abrasive, she decried the “insane level of hysteria around the entire ‘Russian hacking’ story”. She suggested that the US authorities were guilty either of “a technically incompetent misinterpretation of the facts” or had been fooled by a “counterfeit in order to frame my company”. Those who could have had an interest in framing her could include competitors, US intelligence or Russian intelligence, with the goal of screening the real culprits, Shevchenko said.

“A young female hacker and her helpless company seems like a perfect pick for that goal. I don’t try to hide, I travel a lot, and am a friendly communicative person. And most importantly, I don’t have any big money, power or connections behind me to shrug off the blame. So really, it could be anyone.”

Shevchenko described herself as “a typical introverted computer geek” who is largely self taught. She declined to say how old she was, deeming it an “impolite question”, saying instead: “If you really need a number then go ahead and make it up based on my photographs”. Here is a picture of Alisa in case you want to guess her age:



Young Russian denies she aided election hackers: ‘I never work with douchebags’

White House claims Alisa Shevchenko was involved in hacking the US election but in an interview she says authorities misinterpreted facts or were fooled

She said she dropped out of three different universities, as she was passionate about learning, but did not enjoy the structure of a university course. **Around 2004, she joined Kaspersky Lab, a high-profile Russian cybersecurity firm. She** left to set up her own company, initially called Esage Lab ("I was thinking of something 'sage', as in a wizard or a magician," she said). Later, she changed its name to ZOR. Both names are on the US sanctions list.

Shevchenko specialiizes in finding so-called "zero-days", previously undisclosed software bugs that could leave companies vulnerable. "We have not only searched for bugs but exploited them, but only with the customer's sanction," she said. "She never hired anyone she knew to have a criminal background for her companies.
"Shevchenko said she had been approached repeatedly by people she believed to be from the Russian government. She insisted, however, that she had always rejected the advances. She said she had not been threatened or intimidated as a result.

"A 2014 profile of Shevchenko in Russian Forbes magazine noted that she worked with DialogNauka, a Russian company that listed among its clients the Russian ministry of defence and parts of the security services. Questioned by the Guardian, she insisted that none of her own work for DialogNauka "was even remotely possible to use as a nation-state attacks supply". Shevchenko said she had turned down plenty of offers of work on ideological grounds: "I never work with douchebags. I only work with honest and open people that I feel good about." Asked directly if she had ever worked on a government contract in any capacity, she answered "not that I know of".

"Shevchenko said ZOR was closed more than a year ago, because it was difficult and expensive to do the requisite public relations work required to drum up business. She now works as a "one-man army", she said. Shevchenko said she assumes it is "not possible" for her to travel to the US now, and she does not particularly want to. On the other hand, she allowed, there was apparently a certain cachet in being named as someone who hacked a US election. "I have received a number of employment, business partnership or collaboration offers" in the days since the sanctions list was released."
Our comments about Alisa: She must be very smart to get a job at Kaspersky. But thus far, there is no evidence either that she or Kaspersky are Russian spies.

Third, the report claims that a guy named **Vladimir Zhirinovsky is a "pro-Kremlin proxy"** who opened a bottle of champagne and toasted Donald Trump on the night of the election. Here is the problem. The election was called about 10 pm in the evening in the US – or about 10 am in the morning Moscow time. Who would be drinking at 10 am in the morning? Also, according to the Moscow Times, "**Zhirinovsky is the same man who traveled to Baghdad in 2003, ahead of the U.S. invasion, and delivered a drunken tirade against President Bush, threatening to sink the United States under the oceans, using secret Russian gravitational weapons."**
https://themoscowtimes.com/articles/american-unintelligence-on-russia-op-ed-56746

This guy seems to have a drinking problem which is why he no longer has much influence in Moscow. But somehow, US Intelligence Agencies have concluded that he is the guy who leaked documents to Wikileaks and stole the US election – despite the fact that Wikileaks has repeatedly stated that their source as no connection at all to any Russians. For example, see the following:

January 7 2017 Wikileaks Craig Murray says source is Washington Insider

Craig Murray with Wikileaks called the Jan 6 report nonsense… not from Russian
I know who the source….they are on the American side, a Washington insider.
https://www.youtube.com/watch?v=w3DvaVrRweY

Fourth, the January 6th report claims that Wikileaks is a Russian puppet connected to RT. Their "evidence" is that in August 2013, the editor of RT met with Julian Assange at the Ecuadorian Embassy in London. So apparently, this plot to influence the American election has been in the works ever since August 2013.
Also, the head of RT met directly with Putin in 2010. So perhaps that was when they hatched the plot to steal the US election. RT also covered the Occupy Wall Street protests. And they use Facebook and Twitter.

The US Intelligence Report also specifically mentioned the fact that RT has a show called **"Breaking the Set"** that often criticizes US leaders as being "corrupt." Here is a picture of Abby Martin, the host of Breaking the Set. She would often interview people.

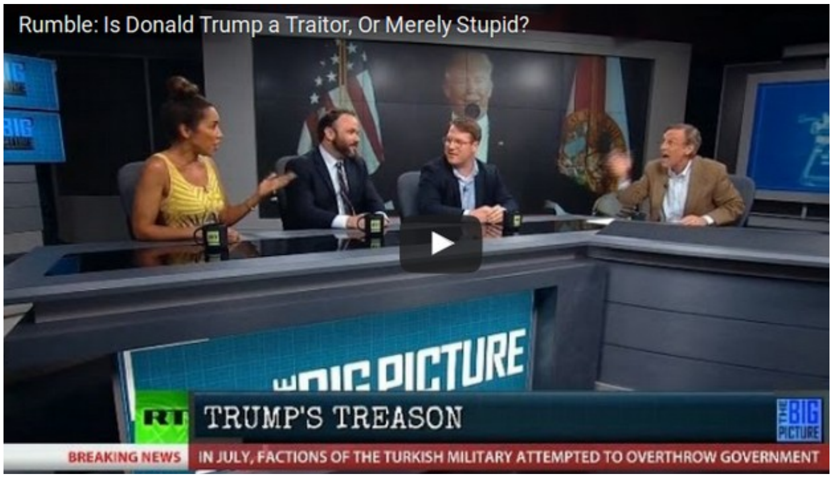
Abby Martin was listed in the January 6th Report as an Example of RT trying to Influence the US 2016 election.

Problem is… her final show was on February 27 2015… A full year before the election!

But there is only one problem with the claim that somehow Abby Martin was used to influence the US elections in 2016. **The final episode of Breaking the Set aired on February 27, 2015.** "On this final episode of Breaking the Set, Abby Martin, discusses the power of grassroots activism in getting the FCC to uphold net neutrality." Net Neutrality. Now there is a dangerous topic. You can watch her final program here: https://www.youtube.com/watch?v=dLVMKuZHbug

132,000 people watched Abby's final episode. But if RT really was trying to win the 2016 election and Abby was such an effective propaganda person, then why did RT cancel the show a year and a half before the US Presidential Election? More important, how in the world, did Breaking the Set make the list of dangerous programs when it is no longer even on the air? This shows how utterly ridiculous the January 6th report was.

But the January 6th Report not only blamed the Clinton loss on RT programs that had been cancelled more than a year before the election, they ignored 2016 RT programs that were highly critical of Donald Trump. Most notable of these was the Thom Hartmann Show which blasted Donald Trump on almost every episode – **including calling Donald Trump a Traitor.**


Rumble: Is Donald Trump a Traitor, Or Merely Stupid?
THE BIG PICTURE
RT
TRUMP'S TREASON
THE BIG PICTURE
BREAKING NEWS
IN JULY, FACTIONS OF THE TURKISH MILITARY ATTEMPTED TO OVERTHROW GOVERNMENT

It defies belief that RT was trying to elect Donald Trump and yet running programs that called Trump a trator. https://www.youtube.com/watch?v=duU9Hkai2Rk

Other crimes committed by RT include hosted debates between US Third Party candidates such as the US Libertarian Party and the US Green Party in 2016. There is a smoking gun if ever I saw one. RT seems to be more popular than the BBC on Youtube (probably because young people wanted to hear what the Libertarian and Green Party candidates had to say). But no mention was made in the report about the BBC, CCN, NPR, ABC, NBC, CBS or FOX NEWS trying to influence US elections or about the hundreds of news papers and radio stations in the US (all owned by billionaires) trying to influence the election. Propaganda is OK as long as it is not Russian propaganda.

In short, the January 6 2017 US Report blamed a TV station with a one percent market share and a bunch of people no one has ever heard of for “trying to influence the US election.” My questions are these: What about the fact that the US main stream media spend billions of dollars trying to influence the US elections? What about the fact that billionaires in our country sent out millions of deceptive mailers to voters in an effort to influence elections all over the US? Just about every group I can think of did something to try to influence US elections in 2016. As for Wikileaks, the emails they released were both true and shocking. What the Democratic Party needs to do is stop blaming Alisa and other Russians and start reforming the Democratic Party to be more responsive to the needs of the American people.

January 6 2017: Congress officially approved the Electoral College results making Donald Trump officially our next President.
Trump got 304 electoral votes, compared with 227 by Hillary Clinton, according to the vote tally read by Vice President Joe Biden.

January 6 2017: Donald Trump met with the Intelligence Agencies.
Trump “struck a conciliatory tone with US intelligence officials after meeting with their leadership, but did not publicly support their conclusion that Russia interfered in the 2016 US presidential contest. In a statement issued after the meeting, Trump pledged to task his administration with creating a 90-day plan to “combat and stop cyber attacks”.

January 10, 2017: David Spring with Turning Point News publishes “Hack Everything, A Detailed Timeline of the DNC Hack.”

My hope is that some one close to Donald Trump will give him or a member of his staff a copy of this report.

January 10 to 20: Clapper and his friends are schedule to meet with several committees. He has already made it clear there will be no new information. But this will not stop them from using the Russian Hacking Scare to manipulate Congress into funding an expanded cyber warfare campaign against Russia. One of the primary reasons we have written this report is to inform the American people about what really happened with the hope that the American people will oppose any expansion of the cyber war against Russia.

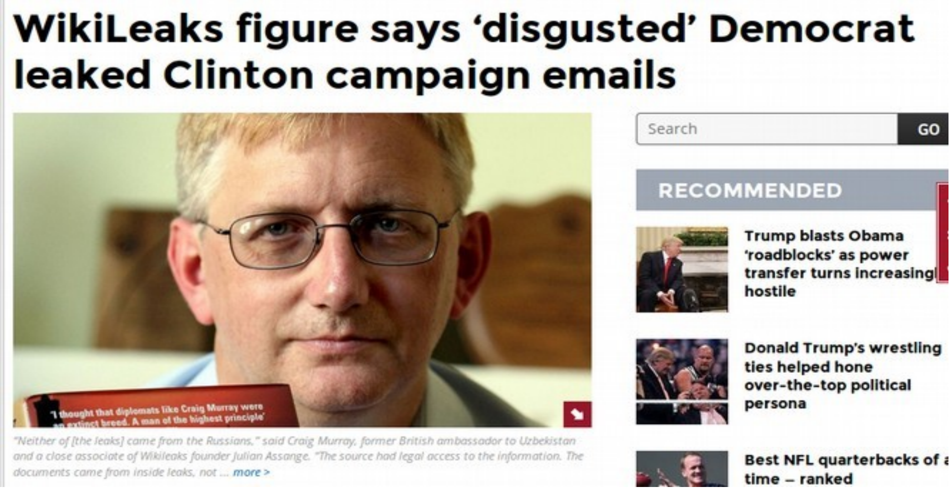
We will now look more closely at a couple of theories about who hacked the DNC and who gave what to Wikileaks before concluding with a section examining the corrupting influence of massive amounts of money being made in American cyber warfare.

Part 7 Who Really Hacked the DNC

If the Russians did not hack the DNC servers, then who gave the data to Wikileaks?

This leads to the important question of how Wikileaks got all of the emails and other data it released which certainly did influence the outcome of the US elections. According to both of the major sources in Wikileaks, Julian Assange and Craig Murray, they got the data from "a disgusted DNC Democrat" who was mad about how the DNC treated Bernie Sanders.

http://www.washingtontimes.com/news/2016/dec/14/craig-murray-says-source-of-hillary-clinton-campai/



WikiLeaks figure says 'disgusted' Democrat leaked Clinton campaign emails

'I thought that diplomats like Craig Murray were an extinct breed. A man of the highest principle'
Search
GO
RECOMMENDED
Trump blasts Obama 'roadblocks' as power transfer turns increasingl hostile
Donald Trump's wrestling ties helped hone over-the-top political persona
Best NFL quarterbacks of a time – ranked

"Neither of [the leaks] came from the Russians," said Craig Murray, former British ambassador to Uzbekistan and a close associate of Wikileaks founder Julian Assange. "The source had legal access to the information. The documents came from inside leaks, not ... more >

Both Murray and Assange have repeatedly stated that they did not get the information from the Russians. We therefore conclude that if the DNC was hacked (which it likely was), then it was hacked by the NSA using Cozy Bear and Fancy Bear as a cover – knowing that Cozy Bear and Fancy Bear were specifically written to fool consultants like Dimitri and Cloudstrike into thinking that it was a Russian hacking program. Obviously, the NSA is not going to give any of its information to Wikileaks. But in addition to these two hacks by Cozy Bear and Fancy Bear, a disgusted member of the DNC also got the information directly from the DNC database, put it on a jump drive and handed the jump drive to Craig Murray. In other words, we conclude that **the DNC was hacked and also subjected to an insider leaker.** Thus, Wikileaks claim that it was a leak is true. But their claim that it was not a hack may not be accurate as there is evidence of a hack.

The Difference Between a Leak and a Hack

Here is a link to a group called Veteran Intelligence Professionals for Sanity who outline the capability of the NSA and explain the difference between a leak and a hack:

https://consortiumnews.com/2016/12/12/us-intel-vets-dispute-russia-hacking-claims/

Here is a quote from this group of US Intelligence veterans:

"Leak: When someone physically takes data out of an organization and gives it to some other person or organization, as Edward Snowden and Chelsea Manning did.

Hack: When someone in a remote location electronically penetrates operating systems, firewalls or any other cyber-protection system and then extracts data.

All signs point to leaking, not hacking. If hacking were involved, the National Security Agency would know it – and know both sender and recipient. Any data that is passed from the servers of the Democratic National Committee (DNC) or of Hillary Rodham Clinton (HRC) – or any other server in the U.S. – is collected by the NSA."

Here are the signers of this statement:
For the Steering Group, Veteran Intelligence Professionals for Sanity (VIPS)
William Binney, former Technical Director, World Geopolitical & Military Analysis, NSA; co-founder, SIGINT Automation Research Center (ret.)
Mike Gravel, former Adjutant, top secret control officer, Communications Intelligence Service; special agent, Counter Intelligence Corps and former United States Senator
Larry Johnson, former CIA Intelligence Officer & former State Department Counter-Terrorism Official
Ray McGovern, former US Army infantry/intelligence officer & CIA analyst (ret.)
Elizabeth Murray, Deputy National Intelligence Officer for Middle East, CIA (ret.)
Kirk Wiebe, former Senior Analyst, SIGINT Automation Research Center, NSA (ret.)

These are six of the leading NSA whistleblowers and everyone one of them knows the full horrific power of the NSA. If only all Americans knew what these six people know (The main reason I am writing this article is to help increase the awareness of the American people about the true power of the NSA). Sadly, most Americans are not even aware of the difference between a leak and a hack and thus are easily misled by the current campaign to blame Russia for whatever cyber attacks are occurring in the US.

Were either Cozy Bear or Fancy Bear Teenage Hackers?

Since the DNC hackers made some rather basic mistakes, some have concluded that either or both of the hacks could have or must have been done by bored teenagers. There are many recent examples of teenagers hacking computer systems much more secure than the DNC server to support this theory.

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY
15-YEAR-OLD BOY ARRESTED OVER FBI COMPUTER HACKING CASE

On February 19, 2016, a 15 Year old boy arrested for hacking the FBI on February 16, 2016. He was part of a group that repeatedly attacked the FBI and CIA over a period of several months.
http://thehackernews.com/2016/02/fbi-hacker-arrest.html

Here is a quote: “Another 15-year-old teenager got arrested in Scotland, by British Police for breaking into the FBI Systems on 16th February. Under the Britain’s anti-hacking law, *Computer Misuse Act 1990*, the boy has been arrested for his role in hacking and unauthorized access to the digital material. Another member of the same group got arrested from the United Kingdom last week. The 16-year-old British teenager was suspected of hacking into the CIA and the FBI.

The two boys had downloaded more than 200 Gigabytes of top secret data on tens of thousands of FBI agents and other high level officials in the FBI, CIA and DHS. The boys also hacked into AOL emails of CIA director John Brennan and hacked into the personal phone accounts and email accounts of the US spy chief James Clapper of the FBI Deputy Director Mark Giuliano.

Here is another article about this attack: How did a couple of boys bring down the entire US Intelligence system? They claimed that they got into the US Department of Justice email account. From there, it was simply a Sunday joy ride through all of the data of the FBI, CIA and DHS. This was all done on line through their home computer using information readily available on the Internet.
http://thehackernews.com/2016/02/fbi-dhs-hacked.html

Nor is this an isolated incident. In 2015, a 14 year old boy began shutting down government and corporate computers all over the world from the comfort of his bedroom. He eventually got caught after using Skype (which has a direct link to the NSA). The judge decided not to send him to jail reasoning that jail would destroy him and he had “just gotten carried away thinking he was cool.” She did order that his computer be destroyed to reduce the chances of any future attacks.
http://www.telegraph.co.uk/news/2016/07/20/teenage-hacker/

Here is a link to a story about 10 teenage hackers:
http://www.huffingtonpost.com/2012/07/18/teen-hackers-10-stories-o_n_1683387.html

Here are some quotes from the article:
“Over the past two years, we’ve seen a ton of stories about teenage tech geniuses who have pushed legal boundaries by cracking the codes of governments and other major institutions, sometimes from their own bedrooms. From a 15-year-old who broke into over 250 websites to the 18-year-old who took down Lady Gaga, click through the slideshow below for some of the most unbelievable teen hackers who have made headlines recently.”

“In 2011, British teens Ryan Cleary, 20, and Jake Davis, 19, made headlines for targeting the CIA, the Pentagon, NHS, Sony, Nintendo and *The Sun*. Most notably, the pair - known as "LulzSec" online - pranked *The Sun* by replacing its homepage with a spoof of Rupert Murdoch's obituary.”

“18-year-old hacker, who called himself DJ Stolen, hacked into the personal computers of several pop stars. He stole multiple unreleased tracks from Lady Gaga, Ke$ha, Leona Lewis, Justin Timberlake, and Mariah Carey over the course of two years and sold them online.”

“In April, 2012, the Austrian police arrested a 15-year-old for hacking into a shocking 259 companies. He is the country's youngest arrested hacker and is estimated to have broken into an average of three sites per day.”

“A Greek teenager was arrested last year for allegedly hacking into websites of the U.S. government and Interpol, ending a two-year chase. A raid of his house revealed 130 fake credit cards. Allegedly, his back is tattooed with the statement, "Capitalism is opportunity and opportunity is freedom."

“Two Norwegian teens were arrested in connection to a string of computer attacks. The BBC alleges that the targets may have included the British Serious Organized Crime Association, the Norwegian lottery, and a German newspaper.”

My point in telling these stories is to demonstrate how poor Internet security really is right now. Those who claim that teenage boys could not possibly hack into the DNC server simply do not know what they are talking about. As noted earlier X Agent is out in the wild and available to be used by anyone. Windows computers and servers are particularly susceptible to hacking due to the always open NSA back door. Until adults do a better job of demanding secure computers and servers, we are going to see even more stories of teenagers hacking into government and corporate computer systems.

Earlier I explained why I concluded that the 2015 German Parliament Fancy Bear attack must have been a teenager. The heartbleed problem with Open SSL is simply too well known for either the Russians or NSA to be that dumb. Without more accurate research and information, it would be impossible to tell for sure who hacked the DNC in September 2015 and March 2016.

However, in the preceding pages I have analyzed many IP addresses that all lead to what look to me to be NSA servers. Ironically, what really tipped the scales towards this conclusion was the list of IP addresses in the December 2016 Grizzly Steppe Report. There is no other rational explanation for so many TOR exit nodes appearing in any list other than concluding it was the NSA trying as usual to get rid of TOR. Teenagers would have no interest in attacking the TOR project. In fact, they would have a strong interest in protecting the TOR project as it would be the main thing reducing the chances of being captured.

How Many Leaks or Hacks Were There and How Many Data Dumps Were Given to Wikileaks?

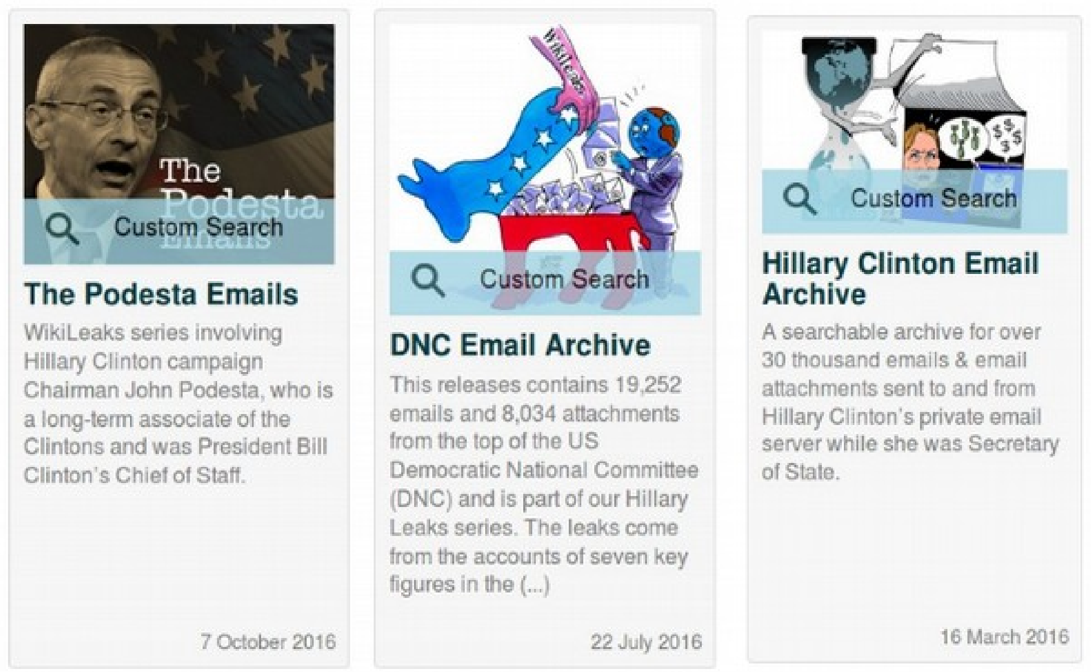
Wikileaks has stated at various times that their source was a disgusted Democratic Party insider who leaked information they had gotten directly from the DNC server. But Wikileaks has also stated at other times in other interviews that their source was a disgusted US Intelligence Agent – meaning someone from the NSA, CIA or FBI got data indirectly through a hack and then gave the data to Wikileaks.

In researching our detailed timeline of events, it appears that Wikileaks was actually given as many as four sets of data at various points in time. First, they were given data from the Clinton private server which they published on March 16, 2016.

Then they were given data from the DNC server which they published on July 22, 2016 (this is what led to the resignation of the DNC Chair and the walk out of Bernie delegates at the Democratic National Convention). They appear to have had this data since some time in May 2016.

Then they published the Podesta emails and Clinton Wall Street speeches beginning on October 7, 2016. According to Craig Murray and others, they seem to have been given this information from one or more sources in September 2016. Thus, there was a combination of leaks and hacks involving several servers and several sources and that the answer to the question of who provided information to Wikileaks is “All of the above.”

The following is the timing of Wikileaks Data Dumps as taken from the Wikileaks website: **https://wikileaks.org/-Leaks-.html**



The Podesta Emails

WikiLeaks series involving Hillary Clinton campaign Chairman John Podesta, who is a long-term associate of the Clintons and was President Bill Clinton’s Chief of Staff.

7 October 2016

DNC Email Archive

This releases contains 19,252 emails and 8,034 attachments from the top of the US Democratic National Committee (DNC) and is part of our Hillary Leaks series. The leaks come from the accounts of seven key figures in the (...)

22 July 2016

Hillary Clinton Email Archive

A searchable archive for over 30 thousand emails & email attachments sent to and from Hillary Clinton’s private email server while she was Secretary of State.

16 March 2016

As just one possible example, the Clinton emails could have come from a teenage hacker, the DNC emails could have been a leak from a digusted Democratic Party insider and the Podesta emails and Wall Street speeches could have come from a disgusted NSA agent using the Cozy Bear and/or Fancy Bear hacks on the DNC and or Podesta Gmail accounts.

What would help clarify who gave what and when would be the release of the DNC server logs. I am really disappointed that the FBI has not released the server logs and that they failed to do a proper investigation in September 2015. But even without this information, we have provided at least 20 reasons in this report to conclude beyond any reasonable doubt that it was not the Russians who attacked the DNC. Thus, there is no honest reason to start a cyber war against Russia. However, I think our government will try to start a cyber war against Russia for the simple reason that a lot of corporations will make a boat load of money. We will cover that problem in our final section.

Part 8 Cyber Warfare as a Business Model

Nearly 100 years ago, an American war hero named General Smedley Butler wrote a book called War is a Racket. He claimed that wars were being deliberately provoked in order to increase corporate profits. He said that the American people were being lied to by wealthy people who controlled the American press in order to provoke fear and get them to agree to go to war. Here is a link to his book. https://www.ratical.org/ratville/CAH/warisaracket.html

50 years later, another American war hero, General (and then President) Dwight Eisenhower, warned of a growing “military industrial complex” that was a threat to our democracy. Here is a link to his speech. https://www.youtube.com/watch?v=8y06NSBBRtY

Today, the US has more than 700 military bases around the world and numerous bases here in the US. Including secret spending for our new Global War on Terror, as mentioned at the start of this article, the US spends more than one trillion dollars per year on war – much more than the rest of the world combined. http://www.globalresearch.ca/the-worldwide-network-of-us-military-bases/5564

The purpose of this worldwide network of chaos is not to protect Americans but simply to increase corporate profits by sucking one trillion dollars a year out of the American economy – money that could have been used to provide free higher education and health care for every American. Because of this annual feast of a trillion dollars being shelled out, our elected officials have been corrupted with a vast bribery and kickback scheme that has turned our elections into a “pay to play” bidding war between various wealthy corporations. These same corporations monopolize the American media with the goal of scaring the American people into supporting this war machine into voting for war hawks willing to do the bidding of their corporate masters. This same “warfare as a business” model is now being used to create Permanent Cyber War on the Internet. Folks with websites need to be aware of this because you will certainly be caught in the crossfire of this cyber warfare machine.

U.S. Defense Contractors Tell Investors Russian Threat Is Great for Business

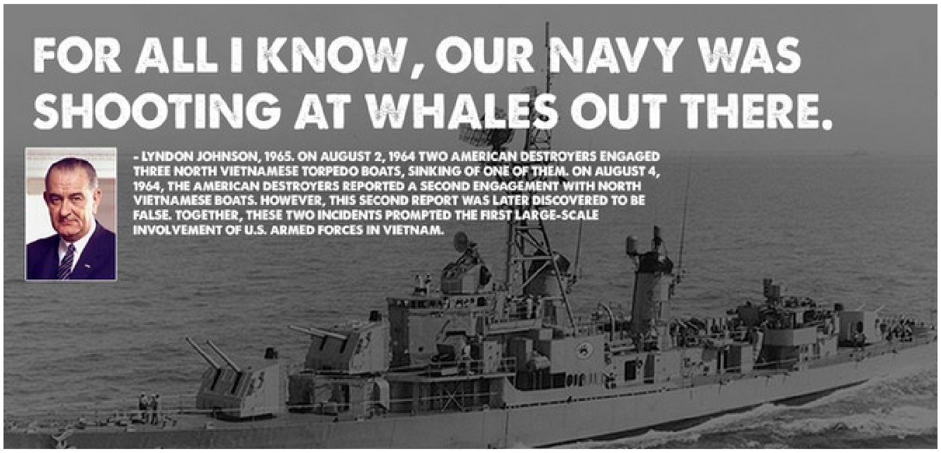
Lee Fang

August 19 2016, 7:20 a.m.

Thus, the most important thing to know about the current campaign to launch a cyber war against Russia is that it will create massive corporate profits. In the summer of 2016, there was a conference on how to profit from the coming cyber war. This conference was documented in the following article:
https://theintercept.com/2016/08/19/nato-weapons-industry/

False Allegations have been used before to start wars… Doesn't Anyone Remember the Gulf of Tonkin Incident?

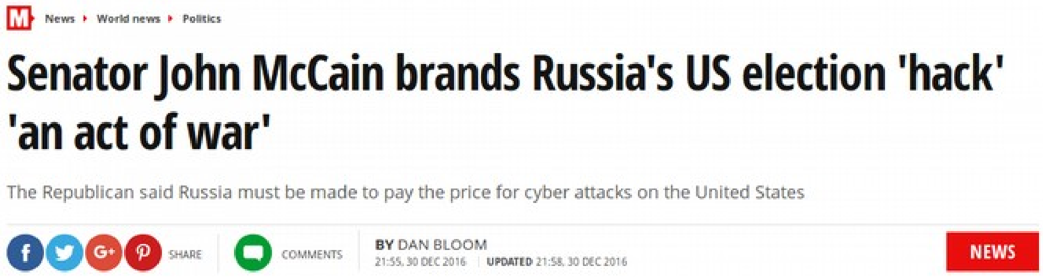
This means that the US is about to start a cyber war with Russia over a hacking incident created by our own NSA. This is nearly identical to the Gulf of Tonkin incident that was used as an excuse by the US military to go to war against Vietnam in the 1960s. That incident turned out to be completely false. Yet millions of people died. The NSA claimed that there was a North Vietnamese attack on August 4 1964. But in 2003, former US Secretary of State Robert McNamara admitted that the the August 4 1964 attack never happened. Moreover, there is substantial evidence that it never happened. The Vietnamese leaders also have confirmed that it never happened. The entire Vietnam War disaster was based on a lie – just like the Iraq War was based on a lie.
https://en.wikipedia.org/wiki/Gulf_of_Tonkin_incident


FOR ALL I KNOW, OUR NAVY WAS SHOOTING AT WHALES OUT THERE.
- LYNDON JOHNSON, 1965. ON AUGUST 2, 1964 TWO AMERICAN DESTROYERS ENGAGED THREE NORTH VIETNAMESE TORPEDO BOATS, SINKING OF ONE OF THEM. ON AUGUST 4, 1964, THE AMERICAN DESTROYERS REPORTED A SECOND ENGAGEMENT WITH NORTH VIETNAMESE BOATS. HOWEVER, THIS SECOND REPORT WAS LATER DISCOVERED TO BE FALSE. TOGETHER, THESE TWO INCIDENTS PROMPTED THE FIRST LARGE-SCALE INVOLVEMENT OF U.S. ARMED FORCES IN VIETNAM.

Why Would Our Own Government Lie to Us?

Many readers protested to our previous article asking why our own government would lie to us. I am not certain but I think it has something to do with making money. The Cyber Warfare Industry has become BIG BUSINESS accounting for billions of dollars in corporate sales and profits since 911. All of the attacks on US corporations have forced all of them to hire cyber consultants and buy expensive cyber products to protect their computers and data. There is a danger in developing such a business model as it could lead to nuclear war with Russia. It could also lead to some former NSA employees deciding to take down the US electric grid or US nuclear power plants. We therefore should understand cyber warfare and a business model and take steps to provide real security for our computers, databases and websites.

This is why we should all question the assertion of government officials and their paid consultants like Dimitri at Crowdstrike when they claim that the only possible explanation for the data breach at the DNC or the Podesta email account is highly trained Russian Hackers. When the government or paid consultants make such ridiculous claims, we should all be able to immediately recognize that they are not telling us the truth. Sadly, many American hawks have called for a cyber war against Russia based on these false allegations:



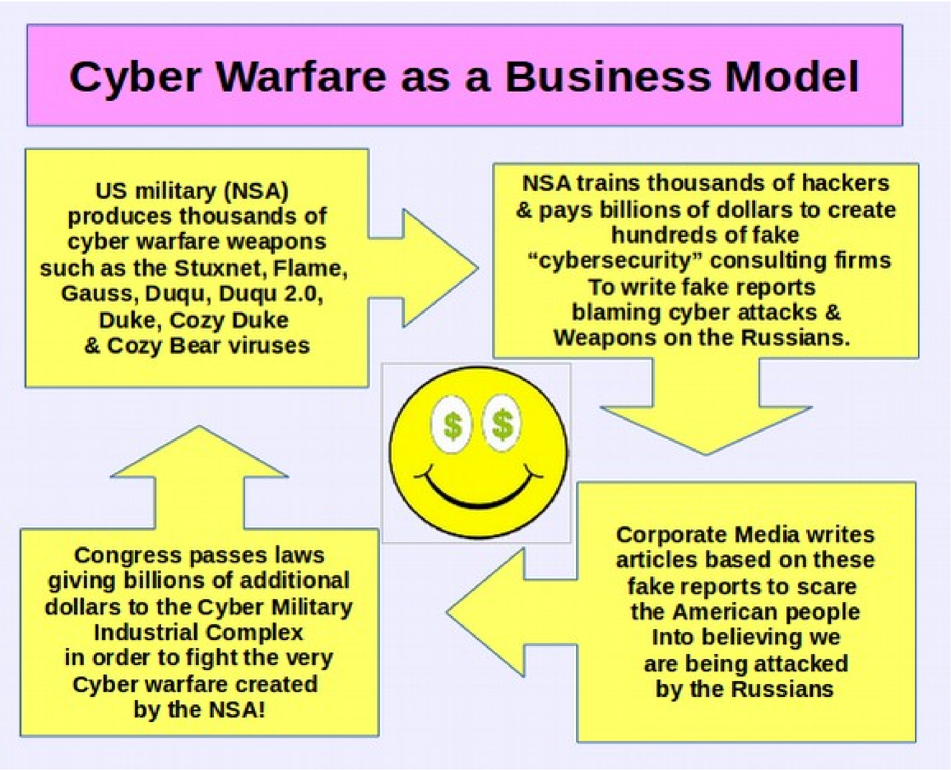
News ▸ World news ▸ Politics

Senator John McCain brands Russia's US election 'hack' 'an act of war'

The Republican said Russia must be made to pay the price for cyber attacks on the United States

BY DAN BLOOM
21:55, 30 DEC 2016 | UPDATED 21:58, 30 DEC 2016

Here is a diagram of how this cyber warfare as a business model works:



Cyber Warfare as a Business Model

US military (NSA) produces thousands of cyber warfare weapons such as the Stuxnet, Flame, Gauss, Duqu, Duqu 2.0, Duke, Cozy Duke & Cozy Bear viruses

NSA trains thousands of hackers & pays billions of dollars to create hundreds of fake "cybersecurity" consulting firms To write fake reports blaming cyber attacks & Weapons on the Russians.

Corporate Media writes articles based on these fake reports to scare the American people Into believing we are being attacked by the Russians

Congress passes laws giving billions of additional dollars to the Cyber Military Industrial Complex in order to fight the very Cyber warfare created by the NSA!

The plan to drum up fear of Russians hiding under our beds was in the works long before the November election. Here are a couple of quotes from the article:
"Retired Army Gen. Richard Cody, a vice president at L-3 Communications, the seventh largest U.S. defense contractor, explained to shareholders in December 2015 that the industry was faced with a historic opportunity (to make massive profits off frightened Americans)."

“Speaking to investors at a conference hosted by Credit Suisse in June, 2016, Stuart Bradie, the chief executive of KBR, a military contractor, discussed “opportunities in Europe,” highlighting the increase in defense spending by NATO countries in response to “what’s happening with Russia and the Ukraine.”

“The Aerospace Industries Association, a lobby group for Lockheed Martin, Textron, Raytheon, and other defense contractors, argued in February that the Pentagon is not spending enough to counter “Russian aggression on NATO’s doorstep. Think tanks with major funding from defense contractors, including the Atlantic Council, have similarly demanded higher defense spending to counter Russia.”

What a minute... Don’t we know someone on the Atlantic Council? Now I remember, our friend Dimitri the founder of Crowdstrike is with this war hawk group – the guy who is absolutely certain that Russia is behind Cozy Bear and Fancy Bear stands to make huge profits from scaring the hell out of Americans. That is after all part of the Cyber Warfare Business model. First comes fear based on false claims. Then comes massive profits. As long as we allow people to make billions of dollars from telling lies, we should expect to see more lies being told.

Who has a very long history of hacking elections is not Russia – but the US CIA
The best predictor of future behavior is past behavior. If we look at the past behavior of the NSA and CIA, it is neither good or honest. Instead of pointing the finger at Russia, we need to take a closer look at our own government. There is a Wikipedia page devoted just to the number of countries whose elections were hacked by the CIA.
https://en.wikipedia.org/wiki/United_States_involvement_in_regime_change

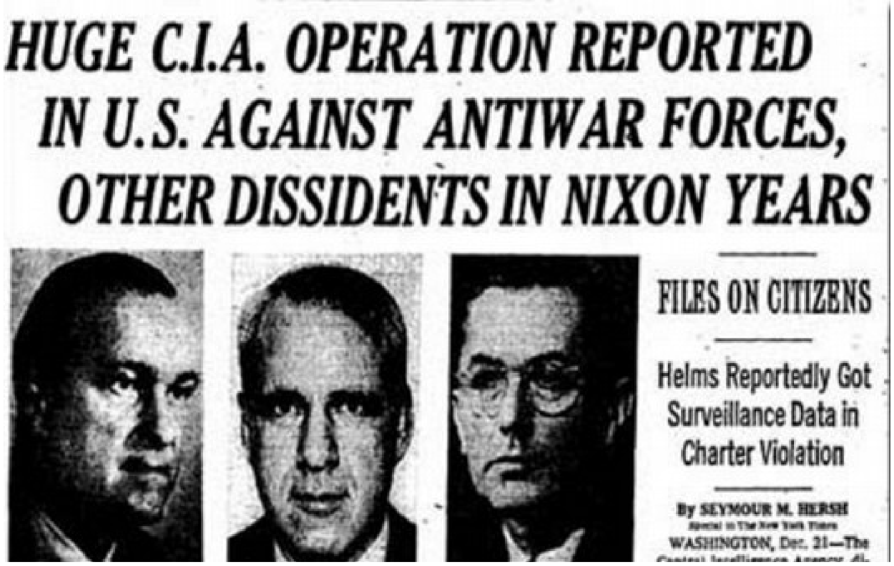
Whole books books have been written about this. Just since World War II, our leaders have not only hacked elections in at least 56 other countries, but they have kidnapped and killed the elected leaders of some of these countries. This is much more evil than having Abby Martin say bad things on a talk show two years before an election.

Here is just a partial list (* indicated a successful overthrow):
China 1949 to early 1960s, Albania 1949-53, East Germany 1950s, Iran 1953 *, Guatemala 1954 *, Costa Rica mid-1950s, Syria 1956-7, Egypt 1957, Indonesia 1957-8, British Guiana 1953-64 * Iraq 1963 * North Vietnam 1945-73 Cambodia 1955-70 * Laos 1958 *, 1959 *, 1960 * Ecuador 1960-63 * Congo 1960 * France 1965 Brazil 1962-64 * Dominican Republic 1963 * Cuba 1959 to present Bolivia 1964 * Indonesia 1965 * Ghana 1966 * Chile 1964-73 * Greece 1967 * Costa Rica 1970-71 Bolivia 1971 * Australia 1973-75 * Angola 1975, 1980s Zaire 1975 Portugal 1974-76 * Jamaica 1976-80 * Seychelles 1979-81 Chad 1981-82 * Grenada 1983 * South Yemen 1982-84 Suriname 1982-84 Fiji 1987 * Libya 1980s Nicaragua 1981-90 * Panama 1989 * Bulgaria 1990 * Albania 1991 * Iraq 1991 Afghanistan 1980s * Somalia 1993 Yugoslavia 1999-2000 * Ecuador 2000 * Afghanistan 2001 * Venezuela 2002 * Iraq 2003 * Haiti 2004 * Somalia 2007 to present Honduras 2009 Libya 2011 * Syria 2012 Ukraine 2014 *
https://williamblum.org/essays/read/overthrowing-other-peoples-governments-the-master-list

What is not mentioned in the above list is the CIA “Dirty Tricks” campaign in the 1996 Russian election.
Here is a quote from a December 18, 2016 article explaining what happened:

“(Current CIA Director) Brennan and his cabal of dark players know fully well that it is the CIA that has pioneered in the art and science of election manipulation. In 1996, it was Russia that bore the brunt of CIA election manipulation with its agents-of-influence in Moscow and other large cities, namely the National Endowment for Democracy (NED) and George Soros’s Open Society Institute and Foundation, engaged in political dirty tricks aimed at undermining the electoral chances of the Russian Communist Party presidential candidate Gennady Zyuganov. The CIA, Soros’s operatives, and the NED printed and distributed fake campaign flyers claiming to have originated with the Zyuganov's campaign. The flyers advocated returning Russia to Stalinism and re-launching the Cold War against the West. The CIA and their allies also helped to manipulate election returns and shaved votes from Zyuganov's total, particularly in Tatarstan and Bashkortostan. This helped the favored U.S. candidate, Boris Yeltsin, achieve a second-round victory of 54-to-40 percent over Zyuganov. In 2012, then-President Dmitry Medvedev said, «There is hardly any doubt who won [the '96 election]. It was not Boris Yeltsin».”
http://www.strategic-culture.org/news/2016/12/18/cia-meddles-us-election-as-has-countless-foreign-polls.html

Can you image the outrage that would occur in the US if Russian agents had passed out fliers in major US cities and rigged the actual vote count in several states in 2016? Sadly, the CIA, has not limited itself to kidnapping and killing foreign leaders, it has also conducted “disinformation” campaigns against antiwar protesters here in the US (especially during the opposition to US bombing in the Vietnam War).



HUGE C.I.A. OPERATION REPORTED IN U.S. AGAINST ANTIWAR FORCES, OTHER DISSIDENTS IN NIXON YEARS

FILES ON CITIZENS

Helms Reportedly Got Surveillance Data in Charter Violation

By SEYMOUR M. HERSH
Special to The New York Times

WASHINGTON, Dec. 21—The

Not surprisingly, the CIA is now one of the chief cheerleaders for launching a cyber warfare attack against Russia. What is really needed is an end to the CIA and the NSA. In the meantime, we all need to learn how to protect ourselves against the crazy people currently running the US government.

Conclusion… How to Really Protect Yourself from NSA Cyber Weapons

The first step in protecting yourself from the NSA is to stop using Windows or Apple computers and start using Linux computers. According to Edward Snowden, the NSA has direct access to both Apple and Microsoft (both of whom are NSA Prism Partners). I explain this open back door problem in greater detail in a book called “Free Yourself from Microsoft and the NSA” which you can download for free at the following link:
https://freeyourselffrommicrosoftandthensa.org/phocadownload/Free%20Yourself%20from%20Microsoft%20and%20the%20NSA%20Complete%20Book%2016%20MB.pdf

If you do not have time to read the entire 435 page book, it basically explains that Microsoft placed an internet browser inside the core of its operating system in 1997 allowing Microsoft access to your computer whenever you are online so they can check to make sure you have a valid current license. The NSA later demanded and got access to this backdoor. Unfortunately, hackers also have access to this backdoor – which is why there is no such thing as a secure Microsoft computer.

Since Apple is also a PRISM partner, the NSA is able to directly access Apple and Microsoft computers whenever they connect to the Internet (using pre-installed backdoors). This is why Edward Snowden uses Linux computers and programs.

Having confirmed that Windows and Apple computers are not secure, I have written a free book and website on how anyone can convert an inexpensive Chromebook computer into a Linux computer. Here is a link to this website:
https://learnlinuxandlibreoffice.org/

In addition to placing backdoors in Windows and Apple computers, it appears that the NSA has also placed backdoors in the most popular website building program called Wordpress. I have therefore written a free book and website on how to build a more secure website and database system using the Joomla web building platform. Here is a link to this website:
https://createyourowninteractivewebsite.com/

But both of these are only temporary solutions. The real problem is the NSA itself and the entire Cyber Industrial Complex. We will not have real security until we get rid of the NSA. Here is a quote from former CIA Agent Robert Steele who has been a consistent critic of the claim that Russia hacked our elections: “I am deeply offended by the lies being told by the US Government – and more specifically, by the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and Department of Homeland Security (DHS) with the explicit approval of the Director of National Intelligence (DNI) and the President – with respect to the Russians “hacking” the US election… **The only intelligence services that persistently spy on US politicians across every device they own are the US intelligence services, specifically NSA.”**

From: **The Russians Did Not “Hack” the US Election – a Few Facts from a Former CIA Spy, Global Research, January 08, 2017**
http://www.globalresearch.ca/the-russians-did-not-hack-the-us-election-a-few-facts-from-a-former-cia-spy/5567215

How are we going to get rid of this NSA Cyber Warfare monster?
I think the solution is to stop reading the corporate controlled main stream media and start reading the Independent Alternative media. This was one reason we started Turning Point News – to promote Independent News Websites. There is strength in diversity. As far as we are concerned the more independent websites there are, the harder it will be for the NSA to shut us all down. For a list of our favorite independent news websites, see the following link.
https://turningpointnews.org/our-favorite-independent-media-sources

Finally, please share the link to this article with everyone you know who is interested in learning the truth about the Russian hacking allegations. Together, we can and will take back our democracy.

The Grizzly Steppe Report is actually proof that
Grizzly Bear and Cozy Bear are NOT Russian!

Hack Everything…

A Detailed Timeline of the DNC Hack

David Spring M. Ed.

Turning Point News.org

January 10, 2017

The NSA Motto is
Collect Everything…

But in order to
Collect Everything,
Your have to
Hack Everything.

David Spring M. Ed.
Turning Point News.org

Read our full report "Hack Everything" to find out who
Cozy Bear & Fancy Bear really are & who really attacked the DNC.

As always, we look forward to your questions and comments.

Regards,
David Spring M. Ed.
Turning Point News.org

About the Author

David Spring has a Master's Degree in Education from the University of Washington. He has taught adult education courses for more than 20 years at several colleges in Washington State including Bellevue College, Seattle Central Community College and Shoreline Community College. In recent years, David has gotten more deeply involved in computer and website security. He has written extensively about the history of Microsoft and the NSA. Here are links to his three most recent books:

Free Yourself from Microsoft and the NSA
https://freeyourselffrommicrosoftandthensa.org/

Learn Linux and LibreOffice
https://learnlinuxandlibreoffice.org/

Weapons of Mass Deception… The Billionaires Plan to Take Over Our Public Schools
https://weaponsofmassdeception.org/

David lives near Seattle Washington with his daughter Sierra Spring, his wife Elizabeth Hanson, her son Chris Hanson, several cats and four free gnomes.

David Spring, Elizabeth Hanson and our four free gnomes.

You can contact David at the following email address:
david@turningpointnews.org