Who is Publishing NSA and CIA Secrets, and Why?

There's something going on inside the intelligence communities in at least two countries, and we have no idea what it is.

Consider these three data points. One: someone, probably a country's intelligence organization, is dumping massive amounts of cyberattack tools belonging to the NSA onto the Internet. Two: someone else, or maybe the same someone, is doing the same thing to the CIA.

Three: in March, NSA Deputy Director Richard Ledgett described how the NSA penetrated the computer networks of a Russian intelligence agency and was able to monitor them as they attacked the US State Department in 2014. Even more explicitly, a US ally -- my guess is the UK -- was not only hacking the Russian intelligence agency's computers, but also the surveillance cameras inside their building. "They [the US ally] monitored the [Russian] hackers as they maneuvered inside the U.S. systems and as they walked in and out of the workspace, and were able to see faces, the officials said."

Countries don't often reveal intelligence capabilities: "sources and methods." Because it gives their adversaries important information about what to fix, it's a deliberate decision done with good reason. And it's not just the target country who learns from a reveal. When the US announces that it can see through the cameras inside the buildings of Russia's cyber warriors, other countries immediately check the security of their own cameras.

With all this in mind, let's talk about the recent leaks at NSA and the CIA.

Last year, a previously unknown group called the Shadow Brokers started releasing NSA hacking tools and documents from about three years ago. They continued to do so this year -- five sets of files in all -- and have implied that more classified documents are to come. We don't know how they got the files. When the Shadow Brokers first emerged, the general consensus was that someone had found and hacked an external NSA staging server. These are third-party computers that the NSA's TAO hackers use to launch attacks from. Those servers are necessarily stocked with TAO attack tools. This matched the leaks, which included a "script" directory and working attack notes. We're not sure if someone inside the NSA made a mistake that left these files exposed, or if the hackers that found the cache got lucky.

That explanation stopped making sense after the latest Shadow Brokers release, which included attack tools against Windows, PowerPoint presentations, and operational notes -- documents that are definitely not going to be on an external NSA staging server. A credible theory, which I first heard from Nicholas Weaver, is that the Shadow Brokers are publishing NSA data from multiple sources. The first leaks were from an external staging server, but the more recent leaks are from inside the NSA itself.

So what happened? Did someone inside the NSA accidentally mount the wrong server on some external network? That's possible, but seems very unlikely. Did someone hack the NSA itself? Could there be a mole inside the NSA, as Kevin Poulsen speculated?

If it is a mole, my guess is that he's already been arrested. There are enough individualities in the files to pinpoint exactly where and when they came from. Surely the NSA knows who could have taken the files. No country would burn a mole working for it by publishing what he delivered. Intelligence agencies know that if they betray a source this severely, they'll never get another one.

That points to two options. The first is that the files came from Hal Martin. He's the NSA contractor who was arrested in August for hoarding agency secrets in his house for two years. He can't be the publisher, because the Shadow Brokers are in business even though he is in prison. But maybe the leaker got the documents from his stash: either because Martin gave the documents to them or because he himself was hacked. The dates line up, so it's theoretically possible, but the contents of the documents speak to someone with a different sort of access. There's also nothing in the public indictment against Martin that speaks to his selling secrets to a foreign power, and I think it's exactly the sort of thing that the NSA would leak. But maybe I'm wrong about all of this; Occam's Razor suggests that it's him.

The other option is a mysterious second NSA leak of cyberattack tools. The only thing I have ever heard about this is from a *Washington Post* story about Martin: "But there was a second, previously undisclosed breach of cybertools, discovered in the summer of 2015, which was also carried out by a TAO employee, one official said. That individual also has been arrested, but his case has not been made public. The individual is not thought to have shared the material with another country, the official said." But "not thought to have" is not the same as not having done so.

On the other hand, it's possible that someone penetrated the internal NSA network. We've already seen NSA tools that can do that kind of thing to other networks. That would be huge, and explain why there were calls to fire NSA Director Mike Rogers last year.

The CIA leak is both similar and different. It consists of a series of attack tools from about a year ago. The most educated guess amongst people who know stuff is that the data is from an almost-certainly air-gapped internal development wikia Confluence server -- and either someone on the inside was somehow coerced into giving up a copy of it, or someone on the outside hacked into the CIA and got themselves a copy. They turned the documents over to WikiLeaks, which continues to publish it.

This is also a really big deal, and hugely damaging for the CIA. Those tools were new, and they're impressive. I have been told that the CIA is desperately trying to hire coders to replace what was lost.

For both of these leaks, one big question is attribution: who did this? A whistleblower wouldn't sit on attack tools for years before publishing. A whistleblower would act more like Snowden or Manning, publishing immediately -- and publishing documents that discuss what the US is doing to whom, not simply a bunch of attack tools. It just doesn't make sense. Neither does random hackers. Or cybercriminals. I think it's being done by a country or countries.

My guess was, and is still, Russia in both cases. Here's my reasoning. Whoever got this information years before and is leaking it now has to 1) be capable of hacking the NSA and/or the CIA, and 2) willing to publish it all. Countries like Israel and France are certainly capable, but wouldn't ever publish. Countries like North Korea or Iran probably aren't capable. The list of countries who fit both

criteria is small: Russia, China, and...and...and I'm out of ideas. And China is currently trying to make nice with the US.

Last August, Edward Snowden guessed Russia, too.

So Russia -- or someone else -- steals these secrets, and presumably uses them to both defend its own networks and hack other countries while deflecting blame for a couple of years. For it to publish now means that the intelligence value of the information is now lower than the embarrassment value to the NSA and CIA. This could be because the US figured out that its tools were hacked, and maybe even by whom; which would make the tools less valuable against US government targets, although still valuable against third parties.

The message that comes with publishing seems clear to me: "We are so deep into your business that we don't care if we burn these few-years-old capabilities, as well as the fact that we have them. There's just nothing you can do about it." It's bragging.

Which is exactly the same thing Ledgett is doing to the Russians. Maybe the capabilities he talked about are long gone, so there's nothing lost in exposing sources and methods. Or maybe he too is bragging: saying to the Russians that he doesn't care if they know. He's certainly bragging to every other country that is paying attention to his remarks. (He may be bluffing, of course, hoping to convince others that the US has intelligence capabilities it doesn't.)

What happens when intelligence agencies go to war with each other and don't tell the rest of us? I think there's something going on between the US and Russia that the public is just seeing pieces of. We have no idea why, or where it will go next, and can only speculate.

This essay previously appeared on Lawfare.com.

Tags: attribution, CIA, Edward Snowden, hacking, intelligence, leaks, NSA, WikiLeaks
Posted on May 1, 2017 at 6:32 AM • 82 Comments

Comments

TS • May 1, 2017 7:30 AM

There's so much "maybe", "could" and "what if" in this article, it reeks of speculation. Makes it really hard to read without a tinfoil hat.

JD • May 1, 2017 7:50 AM

But that's how the vast majority of the intel game is played. Most intel reports actually read this way: "Based on the fragments of evidence we have, here are the ways the pieces might be arranged, and here are the possible resulting pictures, in order of likelihood based on a priori behavior and other reasonable guessitmates". The best kind of intel briefing are only comprised of knowns, but most of the time they are extrapolations, with the knowns being rapidly moving targets.

Kris • May 1, 2017 8:03 AM

Good points, Mr Scheier. I wonder though, why didn't Russia, if they are the real culprit, keep and exploit those tools, or possibly utilize the knowledge of how they work to mislead and manipulate CIA. Letting CIA be convinced of its cleverness and mastery would give Russia the upper hand, wouldn't it ?

"bob" • **May 1, 2017 8:04 AM**

Or maby the tools were purposely left on the server by someone.

The objective of these "leaks" is to disarm before a potential conflict and gain advantages. The exfil material we've seen, like ExtraBacon (not your average 0day) is quite complex, it's gonna take a while to get the initiative back.

WW3 has probably already broken out, but this time the battleground is in our phones, routers and toasters.

---

milkshaken • **May 1, 2017 8:52 AM**

if these are state-organized leak/hack campaigns, it could have started earlier - do you remember BND leaks shortly after Snowden revelations? Merkel was making angry noises, there were investigations. Two low-level US moles in BND were blown, and soon new non-Snowden leaks supposedly originating from Germany made clear the full extent of BND being beholden to NSA (the selector wish-lists from NSA), to a point of parts of BND being declared by German government as "rogue", and the role of american military routing the drone strike control through Ramstein (and violating German law in the process) was uncovered.

Elliot • **May 1, 2017 8:57 AM**

A whistleblower certainly would sit on stuff for years before publishing. The guy who burns down the building didn't just get the idea to do so yesterday.

Sean • **May 1, 2017 8:59 AM**

Any link with the last decision (this week) of Grsecurity to stop providing their security patches to everyone?

When you lose some/most of your weapons, you may start undermine the overall Internet security to some extent to keep your advantage?

999999999 • **May 1, 2017 8:59 AM**

It could be a dead drop. A trove of information that gets auto-published if the control person does not prevent it.
This would explain how someone set up the information and for a while it just sits somewhere. At some point, the person gets caught or otherwise unable to make contact with the server. The outdated information is leaked to a trustee such as wikileaks.

Bruce Schneier • May 1, 2017 9:17 AM

"There's so much 'maybe', 'could' and 'what if' in this article, it reeks of speculation. Makes it really hard to read without a tinfoil hat."

Reeks of speculation? It *is* speculation. That's the point of all of those qualifiers. Leaving them out would be irresponsible.

Speculation is all we can do, since the actual information is classified. I invite those who actually know stuff to correct me.

Bruce Schneier • May 1, 2017 9:20 AM

"Good points, Mr Scheier. I wonder though, why didn't Russia, if they are the real culprit, keep and exploit those tools, or possibly utilize the knowledge of how they work to mislead and manipulate CIA. Letting CIA be convinced of its cleverness and mastery would give Russia the upper hand, wouldn't it?"

Yes, and that is the real question here. Any nation-state that steals this stuff would use it to their advantage, and only release it when the embarrassment/signaling value is greater than its intelligence value. The only conclusion is that the latter is now true. As to why, I don't know.

Maybe the NSA/CIA already knew who took it, and the value is telling the rest of the world. Maybe the attacker is so dominant that it doesn't need the intelligence value. Maybe the exploit/release balance has changed in ways we don't know.

Ph • May 1, 2017 9:21 AM

Any nation state actor would just inventory them, immunise their own systems, and start using it themselves.
Any forensic of used tools would indicate that NSA/CIA is behind them, giving a perfect cover for the usage of the tools.

Only a lone actor or small group would behave like this in my opinion.

Bruce Schneier • May 1, 2017 9:21 AM

"A whistleblower certainly would sit on stuff for years before publishing. The guy who burns down the building didn't just get the idea to do so yesterday."

You're confusing the average of the documents with the age of the most recent document. A whistleblower would collect for a time period, potentially years like Snowden, and then release all at once. The latest release date would be right before he loses access.

I'm looking at the latest timestamp in the documents, not the earliest or the average.

Bardi • May 1, 2017 9:26 AM

With all the "hacking" going on, is there no one who can hack the IRS and reveal Trump's taxes?

The hacking we see seems so one-sided, that one cannot help but think there is a proxy war going on with corporate and state "nationalists".

Winter • May 1, 2017 9:27 AM

What if it is not so much bragging by the "Russians", but retaliation?

Say, for stuff related to the accusations around the November elections?
I remember some news last year or the year before where US intelligence published private pictures of Russian politicians and government officials (I cannot find the link again). So this could have been going on for a few years.

Bruce Schneier • May 1, 2017 9:28 AM

@ Ph

"Only a lone actor or small group would behave like this in my opinion."

I have trouble believing it because of the skill/access it would require. I just don't see a small group being able to pull this off.

Plus, this stuff is intelligence-community plutonium. Anyone doing this would realistically be terrified of retaliation by the US, or third-party operations by another country. I can't imagine someone sitting on this stuff for years. I would be terrified.

But let's spin out the scenario. How do you imagine this all happening?

Sean • May 1, 2017 9:35 AM

Any nation state actor would just inventory them, immunise their own systems, and start using it themselves.

It would have given the NSA or the CIA the ability to undercover who you were. I don't believe they would have secured their systems, the gain would probably have been more significant in misleading them with wrong intelligence.

On the other hand, if they didn't worry about attribution, it means they were not allies.

---

ab praeceptis • May 1, 2017 9:43 AM

Bruce Schneier

The latest release date would be right before he loses access.

Is that so? I'm not so sure. From what I see, your assumption (or statement; anyones choice) is based on the assumption that exfiltration, even (or particularly) over long periods is not noticed (yes, it looks like that) but that once those data are published the exfiltrator can be identified.

I submit that that assumption isn't solid. If you were right, then the agency had to have the capability to identify the "thief" based on a) the fact that he did publish and b) the set of data he did publish. It

seems that that is not easy and probably not even feasible to do.

What if the thief continues to work and to do all the right and normal things (incl. maybe even hunting himself)?

One major reason for my doubts is the very structure of that whole cancer. It's, for instance, *not* just agencies; it's also many, many outsiders plus the fact that almost certainly those systems can be accessed from outside, too (subcontractors, etc).

Last point: Why do we assume there is some (s)he who did it? Shouldn't we also consider the case of multiple persons in multiple departments, one of which, or yet someone else, actually published the data?

My Info • **May 1, 2017 9:47 AM**

They've been doing this for a long time.

Those leaks are sanctioned by public servants and/or military personnel high up, with a lot of rank. They know what they are doing and they know how to cover themselves from liability.

- 1.5 million Americans have TOP SECRET clearance.
- 3.6 million have Confidential or SECRET clearance.
    - **As of 2013:** https://www.washingtonpost.com/news/the-switch/wp/2014/03/24/5-1-million-americans-have-security-clearances-thats-more-than-the-entire-population-of-norway/

From the number of job ads requiring such "clearance," I have little reason to think these numbers are that far off. Something is wrong here. There is massive classification inflation: if that many people have access or clearance to it, it's not even confidential or secret, in the usual dictionary (rather than U.S. Code) definition of those words.

Then they throw around "need-to-know" and "SCI" like rice at a wedding in the park.

My conclusion is that "they" are forming an inner bubble of government secrecy and allowing the outer bubble to burst in a controlled manner. Or all hell is breaking loose.

Jarda • **May 1, 2017 10:00 AM**

There's just one possible solution to plug the unknown leak: execute every single employee of NSA and CIA (of course after extensive waterboaring, as is fashionable in USA nowadays). The Russian and Chinese should do the same on their side. Among all those people there's not a single one with whom I'd go for a beer, anyway.

---

wumpus • **May 1, 2017 10:05 AM**

@My Info:
You are basically assuming that the "inner circle" of the security world wants to break their own empire. Having control over the jobs of 5 million Americans (there is a "confidnetial" clearance? I've only heard of Secret and above) is real power. You don't throw it away lightly.

@Bruce Schneier
"Countries like North Korea or Iran probably aren't capable", while North Korea likely lacks the technical infrastructure, I wouldn't put anything past the Iranians and similar nations (Cuba?). Consider just what lolzsec pulled out of Palentir: there's a lot of low-hanging fruit hanging once you hand out 1.5 million "Top Secret" clearances. Scoop it up and run. It is entirely possible that scooping this up is easy, and they are relying on either the "millions of eyeballs" or simply established malware protection companies to close the holes US spy agencies are using.

Stuxnet probably taught the "minor league" intelligence agencies a few things about what a worm can do. Make a worm that tries to find the Hal Martins of the world (which would include a Clinton-era CIA director if memory serves. Something about putting CIA documents on a computer that connected to the internet via AOL).

---

wumpus • May 1, 2017 10:14 AM

One thing that might allow nations like Iran to get a jumpstart on such things would be to grant modern "letters of marque" to hacker groups. The government helps the hackers learn their skills in return for a cut and government espionage. Now why such a nation would want to dump US tools is still a mystery (possibly Iran might, but still).

Note that the nations willing to dump such secrets are also likely to be willing to tolerate or even want a significant [black hat*] hacker industry in their nation.
* I'm assuming that "black hat" works for those with a letters of marque. Presumably enough on this board would say the same of the NSA/CIA.

Kevin • May 1, 2017 10:14 AM

I find it hard to believe that the US or the UK are capable of hacking into the Russian Intelligence Agency that easily. US might, the UK though? I don't think so.

Das Boinken der Anderen • May 1, 2017 10:21 AM

Now that is how you write CIA propaganda.

Fixate on the Whodunit aspect, with 'it' defined as disclosure. Meanwhile, toss off an unsupported assertion, 'hugely damaging for the CIA.'

Yes, let's talk about that. Just how hugely damaging is public disclosure of CIA capability for illegal privacy interference? Hey, it might do them some good.

CIA is famously inept at HUMINT because commuter life at Langley beats diarrhea and bumbling around in a language you can't talk so good. HUMINT is also much harder and dicier when CIA brass routinely instructs you to break universal-jurisdiction law and peremptory norms. Remember 'chalk in their cleats?' Good times.

You could imagine circumstances in which exposure of illegal sources and methods might motivate an organization to replace the PTSD-addled jarhead washouts so that it can do more intelligence, less foreign interference, and less systematic and widespread torture and murder. Those circumstances won't occur at Langley, of course, or at the Farm or Camp Swampy or No Man's

Island or at the US fusion centers. That's because CIA is a criminal enterprise that controls the 3 ceremonial branches of government. Susan Rice told you as much - CIA chooses the administration you thought you vote for:

"Every previous administration had an expectation and an obligation to vet to their satisfaction, those individuals that the president was appointing to high positions, which is a separate and much more elaborate process than a security clearance. It gets into the financial information. It gets into your relationships and contacts. It gets into your behavior. It's a much deeper vet than what is done solely for the purpose of a security clearance."

As former spook Robert Steele told you, the real purpose of CIA surveillance is kompromat and control of VIPs. That's the damage. Without surveillance, how is CIA going to catch Jan Schakowsky in hot XXX lezzy sex so she plays ball? How is CIA going to purge a loose cannon like Flynn, or Kucinich? Or keep junior spook cadet and future presidential spokesmodel Barack H. Obama in line? Or keep crazy fat pervs like Scalia and Hastert and Foley out of trouble? Russ Tice told you about all that.

DM • May 1, 2017 10:21 AM

It is always tempting to spin conspiracy theories. But my own experience of more than 40 years has shown that people are just not capable of sustained conspiratorial behavior. The level of a crowd (i.e., more than 1) sinks rapidly to lowest common denominator.

It could be a false flag effort on the part of the IC, but that would imply that they have even greater capabilities than they are giving away. That seems doubtful to me.

OTOH, the heavy reliance on OTS components and outsourced work efforts could easily have led to massive compromise in systems, and so maybe an adversary feels confident in showing what has been garnered, believing that he has an ace up his sleeve for ever greater bounties. That works both ways...

DM • May 1, 2017 10:25 AM

... or, it could all simply be the compounded effect of institutional ineptitude...

---

daliroot • May 1, 2017 10:27 AM

This morning, May 1st, SpaceX launched it's first NRO payload. As a teaser to the viewers the best camera footage ever was used of the launch and landing. Comments were that that quality of imagery had existed in the past but never been shown to viewers before.
I am not sure if this fits into the theme of the post but it is a new revelation to the public.

My Info • May 1, 2017 10:32 AM

@wumpus

> You are basically assuming that the "inner circle" of the security world wants to break their own empire. Having control over the jobs of 5 million Americans (there is a

> "confidnetial" clearance? I've only heard of Secret and above) is real power. You don't throw it away lightly.

Confidential clearance? I'm just referring to the graphic in the Washington Post article. (WaPo isn't that far off, either: if 5 million people have that kind of clearance, I certainly wouldn't call it anything higher than "confidential" in the usual meaning of the word.)

The "control" over 5 million jobs? When that is not pursuant to lawful and constitutional authority, then it is pursuant to foreign influence. Remember Mme. Archuleta?

Methinks all hell is breaking loose.

Curious • **May 1, 2017 10:35 AM**

I think that Bruce underestimates the odds that this could be a lone wolf or a small private group. To be sure, I still don't think the odds of that are high; I think it probably is not a lone wolf. One of the reasons that Bruce underestimates the odds of a lone wolf is because I don't think the NSA strikes fear into the hearts of hackers the way Bruce seems to think it does. We have seen before with lulsec and others that small groups are capable of penetration and doing sufficient damages. True, the expertise need at this level is much greater than anything lulsec could have dreamed of pulling off but that isn't the point. The point is that if lulsec could organize privately then it is certainly true that more sophisticated private players--even an inside group--can organize too.

The second reason I am more inclined to think of a private group is that these leaks don't strike me as the type of thing a nation state would do. They have more of an anarchical feel: the kind of thing someone does because they just don't give a damn who they hurt so long as they hurt someone. Whoever did this could not be oblivious to the fact it would do more than embarrass the USA. Many of those tools are now in the hands of criminals and petty dictators world-wide. If one wants to blame Russia one has to believe that not only was Russia out to embarrass the USA (possible) one has to believe that Russia also did not care who got caught in the crossfire (much more dubious). Whatever one may say about Putin being a loose cannon isn't his style.

Bernd Paysan • **May 1, 2017 10:37 AM**

I'm not convinced.

1. Manning, Snowden, and Hal Martin show that you don't need super-capabilities to take a lot of secret documents home. Any smart individual inside the agencies can do it.

2. Bragging is something very typical for Americans. It's neither part of the Russian nor Chinese culture to wildly brag about what you can do. Being underestimated is very handy. So I guess both Vault 7 leakers and Shadow Brokers are Americans.

3. There is a motivation to disarm your opponent by releasing his weapons, and thereby causing a frantic fixing of the 0days. You could however sell these 0days to the criminals and get the same effect. No need to expose your mole or the access you got by hacking into the NSA or CIA.

4. There is a big loyalty problem in the NSA and CIA: People were already disappointed by Obama (see Snowden), but now, Trump seems to be hated by many people in the IC.

5. Manning didn't take a lot of precaution. Snowden did take more precaution, but revealed his identity, and quickly got #1 on the "Enemy of State" list. The pressure against whistleblowers got up, and it is very likely the next generation of whistleblowers is going to use all opsec tactics in the books (and they have the books). The recent Vault 7 leaks about the document identifier beacon shows that the leakers know how they are tracked, and can do something against it.

So I think it's very likely that we have insiders, and that they maybe pretend to be Russians, because in the current climate of "blame the Russians", this is a very good distraction. The Shadow Brokers already write in a fake Russian accent, seems to be on purpose.

From a "what would I publish if I were Putin" point of view, I'd rather publish the lies and deception about past wars and coup d'etat. Show how the CIA financed ISIS. Show how Turkey's MIT supported ISIS with chemical weapons. Show how the coup in Ukraine was organized - leak more phone calls like the Nuland "fuck the EU" one. That's what would directly support their agenda, and that would be what benefits them most.

Sidenote: If the NSA hacks your cameras in your hacker building, wearing these stupid black ski masks actually starts to make sense ;-).

Andreas the Kraut • **May 1, 2017 10:59 AM**

DM, did your own experience of 40 years include the Special Forces training on the JFK assassination as a successful application of a standard CIA coup template? Evidently not. When an agency like CIA has impunity, you don't need to conspire. You just do what you want. Your experience sounds more like warmed-over 1035-960 catchphrases.

Douglas Knight • **May 1, 2017 11:09 AM**

> The dates line up

The WaPo seems to say that the CIA seems to say that the leak caused them to clean house, and that's how they found Martin, so that's why the dates line up.

> No country would burn a mole working for it by publishing what he delivered. Intelligence agencies know that if they betray a source this severely, they'll never get another one.

If you don't know whether they burned a mole, potential moles don't know, either, so maybe it isn't such a big cost.

Ph • **May 1, 2017 11:38 AM**

I am a strong believer in hanlon's law.
Do not attribute to malice that which can be attributed to incompetence.

I've worked long enough in ICT that know that this is especially there.
Somehow someone got a backup of that stuff, lost usb key, misplaced backup copy, stolen laptop, not cleansed harddrive etc.

With already a good knowledge of networks, he investigates some more into how to remain anonymous, and uses that knowledge to contact a broker.

The broker is promised a part of the cut, but they misjudge how hot the stuff is and how to sell it well (just in bugbounties they could have become rich)

The last dumps are just out of frustration.

A nation state actor just has to much interest in keeping it for their own nation, these were if kept secret the equivalent of the new age hydrogen bomb.

---

mark • May 1, 2017 11:45 AM

Bruce, I've got two other possibilities for you to consider: first, much closer to home, someone in either agency, or an actual conspiracy, as in two to three individuals who are buddies, work on both agencies... and extreme libertarians.

The other... you missed one country who be ecstatic is US and Russia fight: the Ukraine. Certainly, they have enough good hackers (as I note from reading Krebsonsecurity).

mark

Scott • May 1, 2017 11:53 AM

Occam's Razor leads me to ask: Which state actor(s) have the Means, Motivation, and Opportunity?

- Russia
- Israel
- Russia & Israel working together

---

keiner • May 1, 2017 12:07 PM

Somebody wants to humiliate NSA and CIA. Who is on the short list?

FBI

:-)

Grauhut • May 1, 2017 12:16 PM

@Bruce:

What about an external mic company that tries to generate more revenue from NSA and CIA because they need the money?

If such a company burns tools, they create demand for new tools...

Imho this is an easier explanation than evil Russians burning sources and showing off their capabilities.

Ask Occam. :)

Reben • **May 1, 2017 12:32 PM**

I am still confused

Grauhut • **May 1, 2017 12:45 PM**

@mark: If i had to hunt that mole i'd look for a lone wolf first, an external consultant who worked for the NSA first, then for the CIA and was promoted after that to some kind of key account management job.

Someone who is afraid to loose his new beloved position because of lack of success in generating new income from these accounts.

Someone who is politically active and likes to troll Trump.

https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1

---

me • **May 1, 2017 12:55 PM**

I like how you all keep assuming everyone in these organizations, both domestic & foreign, is working together, lockstep in perfect harmony to create a better world. You never believe anyone is going to be out for themselves, making a career out of throwing bodies under the nearest bus.

You might consider not just who may be jailed for these leaks, but how the internal power structures change when the guy in charge of the department that had all these tools no longer has them. And perhaps, if that guy had too much power, or if he was a threat to those who did have power, that's a good thing. From a certain point of view...

Tell me, have you ever seen the move Hopscotch, 1980, with Walter Matthau?

Drone • **May 1, 2017 3:30 PM**

Well, look at the up-side: If they ever catch who did it and lock him or her up in a U.S. Federal Prison, at least they'll get affordable health care. Gawd knows - the rest of us won't.

Tim! • **May 1, 2017 4:10 PM**

@Grauhut: fascinating that this author proclaims support for Trump, and also uses progressive tense almost universally.

DM • **May 1, 2017 6:04 PM**

@AtK

Let's see here... 2017 - 40 = 1977. I was only 12 years old when Kennedy was shot. I had to go look up what 1035-960 even refers to.

Reminds me of my co-worker, Chuy, who daily would come up to me to discuss von Daniken's subterranean men and ask about the possibilities... Heh!

Chuy • **May 1, 2017 9:08 PM**

So, DM, you were only a stripling then, you're saying that's why you internalized CIA propaganda so faithfully? Did you read paragraph 4(c) of 1035-968? Because that's where your opinion up there came from. Practically verbatim. Next time just say, 4c! and we'll know.

Would you believe in Van Daniken's underground men if CIA put out a memo about that? Cause there's lots of CIA memos proving they shot your unauthorized presidential candidates and saintly civil rights heroes and smuggled drugs to top up their serious crime slush fund and blew up OKC and the WTC (twice!)

http://www.justice-integrity.org/1250-time-magazine-history-channel-ramp-up-oswald-jfk-fake-news
http://www.washingtonsblog.com/2014/05/dont-fooled-conspiracy-theory-smears.html

---

aboniks • **May 1, 2017 11:05 PM**

"The State Department had to shut down its unclassified email system for a weekend, ostensibly for maintenance purposes. That was a “cover story,” to avoid tipping off the Russians that the government was about to try to kick them out, said one former U.S. official."

But now we're going to tell everyone The Truth about it to help some people sell ad space in a paper? Riiight.

"Fortunately, Ledgett said, the NSA, whose hackers penetrate foreign adversaries’ systems to glean intelligence, was able to spy on the attackers’ tools and tactics. “So we were able to see them teeing up new things to do,” Ledgett said. “That’s a really useful capability to have.”"

Or a really useful capability to make people *think* you could/have/will deploy, even if maybe you can't, didn't, or won't.

That whole WaPo story reeks of domestic US propaganda and poorly designed offensive signaling. Not only is there no reason to believe that any of that half-attributed Tom Clancy fanfic happened the way it was described, there's also no reason for it ever to have been published if it *had* happened as described.

Ham-fisted and absurd, yes, but still propaganda. Using it as any part of an attempt to understand how and why tools are being released is laughable. You might as well just tweet Trump and ask him what happened. It's good clickbait for certain segments of the social media chum bucket though, so let's at least give the Post credit for business savvy.

DM • **May 2, 2017 12:35 AM**

@Chuy

...probably stupid to continue this, but it is mildly entertaining...

I'm saying that on the basis of 40+ years working amongst human organizations, I have seen so many instances where groups of people were incapable of pulling off even simple plans.

I'm hardly a CIA defender, and even they demonstrated repeatedly around the time of Kennedy that they were incapable of truly performing to plan - Bay of Pigs, Golytsin, Gang of Five. You really believe that they pulled off the Kennedy assassination so perfectly well?

When I worked for IBM I used to marvel at the internal stupidity of the company, and I could only assume that all of their competitors simply screwed up even more than IBM did, leaving the appearance that IBM was a hugely successful company. Several decades later the internal rot finally began to show.

It must be that, because we are all born as helpless infants and our parents are the super-humans that have all the answers for our survival, that we all grow up with some subconscious tendency to believe that there must be someone out there more powerful and all knowing. But in fact, everyone puts on their pants the same way. There is no person master of the universe...

I think I'll stick with Occam's Razor, and go with what the evidence really elicits - human frailty.

Clive Robinson • **May 2, 2017 3:03 AM**

@ DM,

> You really believe that they [CIA] pulled off the Kennedy assassination so perfectly well?

The actuall assassination was improbable for a whole host of reasons as were the events that followed. And as others have pointed out since then the response of the authorities at every step and turn was not what one would hope for in fact almost the opposite. Thus the whole event is ripe for a myriad of interpretations, which have as night follows day been presented and no doubt will continue to be presented as with "Jack The Ripper".

However one set of facts remains, Firstly a siting US President was killed. Secondly others who might have shed light on the issue were killed. Thirdly nobody has been viably --as in proof-- presented as being behind the assasination.

Thus logically if it was not the lone gunman at the book depository window (which appears improbable) then somebody did indeed not only "Get away with it" but has also "kept it secret"...

As far as I'm aware none of the US IC has been 100% successfull, and logicaly if they were we would not have heard about them. So that drops into the "trying to prove a negative" slot. However some such as Hoover managed to keep the lid on their bad practice whilst they were alive and arguably much of it has yet to come out (if it ever will).

The thing is whenever you get "power families" such as the Kennedy, Bush, Clinton and other families they become targets for other "power interests" only some of whom we ever get to see (Koch

Brothers) due to their almost total ineptitude...

Orpheus Rocker • **May 2, 2017 3:55 AM**

I'm tending to Occam's Razor. And Hanlon's Razor as well.

Businesses specialize in incompetence. Spy agencies, being immune to even the rudimentary form of accountability that manage to keep the likes of Microsoft and Oracle "transparent" according to differing definitions of "transparency", are also likely to haemorrhage information at the least opportune moments.

When I was a young whippersnapper I read about a member of the Austro-Hungarian Secret Service who sold the Russian Empire a fair amount of the details of the Austro-Hungarian Imperial Armies. The Russians had leverage, and the Austro-Hungarians were proverbial for incompetence, much like the Tsarists.

I mean, a writer like franz Kafka could get famous writing about the Austro-Hungarian iron ceiling in several novels and people everywhere else proclaimed he was writing about their situation.

One of the constant themes - memes you might say - of commenters on this blog has been the uselessness and therefore senselessness of the various Big Brother schemes to keep us "safe" with differing definitions of "safe" ... this I would argue, is just another of those situations. Neither the **CI**A nor the NSA can keep their own data safe, so why does everyone assume they have anything even remotely resembling that skill when it comes to anyone else?

Orpheus Rocker • **May 2, 2017 4:17 AM**

Addendum to above:

I just remembered one Hugo Cornwall and his book The Hacker's Handbook. He had this to say about Network Penetration:

> A note for journalists: any hacker who offers to break into a system on demand is conning you--the most you can expect is a repeat performance for your benefit of what a hacker has previously succeeded in doing. Getting to the 'front page' of a service or network need not imply that everything within that service can be accessed. Being able to retrieve confidential information, perhaps credit ratings, does not mean that the hacker would also be able to alter that data. Remember the first rule of good reporting: be sceptical.

I think that applies to one NSA Deputy Director Richard Ledgett and his boasts of penetration into the Russian FSB networks. The general rule would appear to be: those who can, do; those who can't, pose.

Grauhut • **May 2, 2017 4:56 AM**

@Tim!: "fascinating that this author proclaims support for Trump, and also uses progressive tense almost universally."

Smells a little like LulzSec style nihilism, doesn't it?

I think @Bruce could and should ask someone like cDc's Mudge who's style this could be. :)

https://theintercept.com/2016/07/29/a-famed-hacker-is-grading-thousands-of-programs-and-may-revolutionize-software-in-the-process/

---

r • May 2, 2017 6:55 AM

So, even now an Intel AMT vulnerability is burned.

---

keiner • May 2, 2017 7:38 AM

@Clive Robinson

As usual, very good analysis! Make an educated guess: what is the percentage of "information" on public (!) issues (politics in the widest sense) that EVER surface to the so-called "public"?

5%?
10%

...and the rest is locked away.

So based on these 5% to 10% the so-called "press" has to construct (more or less) viable stories to explain to the public the phenomena they see, e.g. somebody gets elected/blown off political power, "terror", name it.

And this is the dilemma press and all the readers/watchers face: try to establish a more or less stringent story on what we see, knowing we see only very little of what is really going on.

CIA: If it happened, cover it up. If it didn't happen, make it up.

Besides the Kennedy murder, consider the 911 Boeing in the Pentagon. No photos showing it. Photos that could show what impacted not shown. Hundreds, literally, must have seen what happened really. And if you ask in the Pentagon, they don't even EXPECT you to believe the airplane hit, you get told Hawk batteries shot it down, only an engine hit the building.

Tell me: What to believe nowadays?

Clive Robinson • May 2, 2017 8:08 AM

@ Keiner,

> So based on these 5% to 10%...

Hmm I'd move the decimal point atleast a couple if not four decimal places.

Look at it this way, how much money is sloshing about in lobbying, hospitality etc, then have a look at how many politicos and senior civil servants find nice cushy jobs with $10,000/hour pay rates to attend a few meetings a year...

And that would be one small fraction of what people in the general public might consider corruption. Realy just the minnows in the pond, when you start thinking about the amount of money the sharks

are playing with, you can start thinking about the levels of "persuasion" that might command.

Look at it another way, if you are going to put your hand in your pocket for a billion USD to put a body in the Whitehouse for four years, just to get a half percent shaved off some tax... Just how much money would you likely be shoveling around to make it worth while? Then factor in other things like profit and risk and it might not be a supprise if your eyes start spinning like the wheels on a "One armed bandit".

Kai • **May 2, 2017 8:45 AM**

Apologies if someone posted a similar theory already, but I see another possibility: the leak is intentional and orchestrated by the NSA. Before you cry "tinfoil hat", hear me out.

We're taking it as a given that NSA and CIA (or their foreign partners) have some level of access to their Russian and Chinese counterparts. (I'm going with Russia for the sake of brevity, but it might as well be China or a number of other US-unfriendly nations) We don't know how much access, and chances are that neither do the organisations thus infiltrated.

If the inside source had delivered a dump of tools they discovered to the NSA, then the NSA faces a dilemma: it's their duty to protect US interests, which would mean to publish those things so fixes can be rolled out, but that would almost certainly burn their source, by the same logic that a source inside the NSA would be burned. This "leak" is their way out.

It's not an entirely unreasonable assumption that the NSA knows about many of the same security issues their Russian counterparts do, so a leak from inside the NSA revealing those same issues isn't too suspicious. It's a bit of a gamble how much they can reveal before someone on the other side wonders why they seem to have exactly the same tool set, but if they include only the most dangerous ones in their leak, season it with some of their own stuff for authenticity, then it might go unnoticed. Voila, warnings issued, their source does not end up in front of a brick wall with a last cigarette, and no real harm done to the NSA because they know that the Russians already had all the good stuff that was leaked.

Thoughts?

TM • **May 2, 2017 9:32 AM**

Agree with aboniks. Why would anybody believe Ledgett's tall tale about being able to watch the opponent hackers live? It seems extremely unlikely, and if it were true, why tell it to the Wahington Post? How credulous are people, really?

G0 • **May 2, 2017 10:18 AM**

Yes, TM, it's funny to see all the security savants in a tizzy over corny spy-movie tidbits while the whole point goes over their heads.

No one would hack a functioning State Department. They would just ask their diplomats what the US wants or what they think. But this is not a real Department of State. It's a mole-infested appendage of CIA that's been put to work fabricating war propaganda and knocking over governments. Ledgett's fanciful cyber thing occurred while NATO was faking a Syrian sarin gas release as a pretext for

armed attack. Russia winds up treating DoS like the criminals they are. NSA catches Lauri Love picking his nose at the keyboard. And Langley's useful idiots avidly suck up to get in on the fakewar fun.

Bruce Schneier • **May 2, 2017 10:56 AM**

@ Kai

I thought about the possibility that the NSA might be self-publishing to deny an attacker use of what they stole. I do know they flirted with the idea of doing that with the Snowden documents.

I have trouble believing it, though. I think they would do it differently, and not spend so much effort making it look like the Russians are doing it.

Troutwaxer • **May 2, 2017 10:58 AM**

As to the idea that only the U.S., the Chinese, Russians, and a few other rich countries can afford to accumulate a big collection of zero-days... I have to call bullshit.

Hackers are cheap. Compare them to a missile program, a nuke program, or a new fighter jet and the cost may as well be nothing. Hackers are cheap and the leak could have come from any of a hundred countries.

I'll note one other thing in passing. A few years ago someone managed to get the Linux kernel up and running on the electronics of a hard drive. Any smart intelligence agency would follow that up and also figure out how to do it to their own hard drives (if only for defensive purposes.)

Maybe we've reached the end-state on that particular hack and nobody needs zero-days anymore.

JohnT • **May 2, 2017 12:38 PM**

Who's released these tools is the question. I have been dealing with the NSA for three years. Everything happens for a reason with these people. They are far more capable than they would lead you to believe. Rumor has it that the NSA wants to infect ever Computer in the world, what if that's already happened? Better yet, what if you could control them? Wired or air gapped it doesn't matter its all part of a Network. New Computers are easy, they are infected before they are purchased. The old ones are the hard ones, but Intel made that much easier. Now you install a ghost beacon that bypasses everything and takes you right into the firmware. What's the next step? Slowly expose what you have already took advantage of before some else steals your idea.

Fredric Rice • **May 2, 2017 1:40 PM**

This is a good thing. :)

The NSA is a domestic terrorist organization which has been recording (and continues to record) all on-line and off-line electronic-based activities of all 380 million Americans, and has been doing so since Day #1 of their formal creation (November 4, 1952.) They are the enemy insofar as they are an entity which attacks us citizens without warrant, without subpoena, and without any Judicial court order or, for that matter, any political or Judicial oversight.

The CIA is a global terrorist organization that conducts murder on a global scale, the assignation of foreign heads of government, and the toppling of Democratically-elected governments world wide. The CIA is also the enemy of the United States inasmuch as the CIA collaborates with foreign governments inimical to our nation's civil and Constitutional rights, freedoms, and liberties.

What matters here is the *motivation* of the domestic or foreign third party which seized the NSA's internationally-recognized-as-illegal software tools and have been making them widely public for anyone -- just anyone -- to download and make use of, again for their own motives, financial or political.

At core here is the light of Sunshine and Trvth being shone down upon what the NSA and CIA have been doing to U.S. citizens as well as to citizens of the rest of the world. This is a good thing, the truth really does make one free -- and drives lawful correction against such crimes against humanity -- only when the truth is disseminated among the victims of such State-sponsored crimes.

Fredric Rice • **May 2, 2017 1:50 PM**

"A whistle-blower would act more like Snowden or Manning, publishing immediately..."

That's not always true, someone exposing such State-sponsored crimes might archives the evidence for years prior to release to the light of sunshine specifically to attempt to disconnect date/time stamping of computer records of the person's access of the evidence from the date of disclosure of said evidence, plus the person(s) responsible would consider holding off the publication of the evidence long enough to secure other employment or, for that matter, to flee to a Democratic country where the CIA / NSA criminal enterprises could not retrieve them lawfully.

There are many reasons why a whistle-blower or civil rights / human rights advocate might hold off the publication of such evidence.

Fredric Rice • **May 2, 2017 1:57 PM**

"The list of countries who fit both criteria is small: Russia, China, and...and...and I'm out of ideas."

You left out the United States in your list. The United States isn't a unified political entity, there are warring political factions within the U.S. governmental entities, and various factions certainly have the means to hack-n-crack the CIA's and NSA's systems to seize such evidence, there to make them public as said entities vie for dominance and budgets over the others.

The NSA claims to have 30,000 employees working for it. The CIA claims to have 22,000 employees working for it. Just those two entities alone with over 50,000 employees has *got* to have citizens with the courage and technical know-how to make evidence of these organization's crimes against society public if only on moral grounds, yet in organized efforts conducted by one such political entity against another, the motivation would be financial and budgetary.

What we can't ignore is the likelihood that U. S. governmental agencies do direct recruitment of NSA and CIA employees for purposes of developing leaders and whistle-blowers, motivated by the desire to strengthen their own agencies.

Dan H • May 2, 2017 2:30 PM

Bashing the CIA and NSA is popular today, just like bashing the police.

Yet, if some catastrophic world event happens, such as a terrorist attack, then everyone will be blaming the CIA and NSA.

"Why were you all asleep?" "You aren't doing your jobs." "What were you people doing to let that occur?"

Same thing happens to the police. Riots in Baltimore and castigating the police, so they relent and pull back and crime increases, then people scream the police aren't protecting them. Yet they didn't want the police there.

Rita the Artist • May 2, 2017 3:37 PM

@Dan H, thank you for that groveling ritual kowtow to every authority figure you can think of. You should all be purged, cops, NSA voyeurs, and drug dealing murdering torturing CIA spooks. You cops we can replace with unarmed women social workers. There will no more extrajudicial killings and none of this constant piteous cop whining. NSA we don't need to replace, they're useless as tits on a bull. CIA we put them all in prison for ten years. Then there will be no wars, cause CIA starts them all, so you don't need intel, you need diplomats who aren't idiots. That's the hardest part, only immigrants can do that job because Americans are so hopelessly brainwashed.

Gerard • May 2, 2017 4:15 PM

@ Dan H,

Yet, if some catastrophic world event happens, such as a terrorist attack, then everyone will be blaming the CIA and NSA.

First, in the last 100 years none of the terrorist attacks haven't even come close to catastrophic world events. You are orders of magnitude off. I am not saying that they can, but the last 100 years they haven't. I am talking about civilian casualties of course.

Second, catastrophe in the world. If you mean human suffering at large scale, that is caused by roughly three reasons. One is exploitation (with tyranny), second by military intervention and third by nature. The first two are caused by people who want to become rich at the expense of others. The CIA has a criminal track record "a mile long" when it comes about this.

DanH • May 2, 2017 9:49 PM

@Rita the Artist, LOL no comment needed.

@Gerard, 9/11 was a coordinated attack, so it is perfectly within the realm of possibility that coordinated attacks could happen in New York, London, and Paris simultaneously. I'd say that is a horrendous event. 9/11 was a catastrophe. The November 2015 Paris terrorist attacks were coordinated. Egypt has had coordinated terrorist attacks. July 7, 2005 in London there were 4 coordinated bomb attacks.

Perhaps you don't know the definition: "an event causing great and often sudden damage or suffering."

Apparently you prefer to have these events happen, or you believe Stalin, Mao, Kim, Pol Pot, Castro and others are a preferable form of government and examples of leadership. I'm sure you'd much rather live in Russia under Putin too, who kills political rivals.

Are the NSA and CIA perfect? Of course not, there are faults, but they work to protect America and the free world. Now say thank you while you sleep peacefully and securely tucked into your bed tonight.

John Goodwin • May 3, 2017 1:08 AM

@Bardi - cui bono is almost always a good question to ask.

Here's another good thing to do: In a case such as this, with high uncertainty of the truth of basic facts and reliability of sources, it is almost always informative to think about the *most* inconsistent facts that are the hardest to explain by any theory, not to try to make everything consistent. Science works by eliminating models, not by confirming hypotheses (or overfitting the data with conspiracy theories).

Here are what I consider the hardest things to explain about all the leaks:

- why don't Assange and Snowden get on better? Assange never retweets Snowden, even though WikiLeaks often does. Assange only retweets Greenwald over Ecuador. Was the friction over the Manning publication permanent? Odd if they're all Russian patsies together.

- if Clinton is right and WikiLeaks almost single handedly tipped the election with help from the DNC leaker and Podesta phisher, why is Trump so keen on bringing Assange to justice?

- why do the Shadow Broker releases seem to be timed to American political events, and reference them, when the hacks themselves have no political content at all, but simply embarrass the NSA?

- why did the Shadow Brokers take the trouble, clearly, to tell Microsoft about three 0days that weren't yet patched, then wait a month until they do so. If the NSA is behind the shadow brokers (discussed above), why wait until just now, and if the NSA is not the shadow brokers, why isn't the conversation with Microsoft being investigated by our CI? Do we just give spies a free pass when they are nice and give warning of their attacks?

- why do the Shadow Brokers releases seem like a reaction to the WikiLeaks? If it is a single FIS harming the US, why do you need two sock puppets talking to each other?

Again, the key is not to find a way to make these hard to explain facts consistent with your theory, but to eliminate theories using them, or similar hard to explain facts.

---

fajensen • May 3, 2017 3:57 AM

@Fredric Rice

Apart for the TLA gang-bangers fighting over the same turf, maybe a powerful actor like SAIC has a commercial interest in proving that those government agencies in the security biz are really incompetent and If Only everything was outsourced to Them, or If Only they were using their tools ....

@Clive Robinson

I did read somewhere that Kennedy was killed by a negligent discharge from one of the guards driving along with his finger on the trigger of his rifle then slipping when Oswalds bullets caused panic and him losing balancve pulling the trigger. That sounded credible to me. It kinda a thing: Government agency fucks up badly, then the inept cover-up feeds all manner of conspiracy theories and stupidity, which then needs more cover-up - of the same quality as before ...

---

matteo • **May 3, 2017 4:16 AM**

"They [the US ally] monitored the [Russian] hackers as they maneuvered inside the U.S. systems... Countries don't often reveal intelligence capabilities...

maybe they invented this (=lie) because:
-if you have been hacked it's not nice you look like a noob
-if you let them in to spy them you look like a pro with a strategy

and after snowden, Hal Martin and shadow brokers to normal people seems like that anyone can get access to that secrets.

how can you promote backdoored encryption? if you can't keep safe your data how can you ask also data of other people?

Dirk Praet • **May 3, 2017 6:06 AM**

What happens when intelligence agencies go to war with each other and don't tell the rest of us?

Well, if the net result of their spilling each other's guts is that analysis of their tool kits leads to a better comprehension of what they're up to and to tech vendors being forced to patch the holes, then I really couldn't care less who's behind it and for what reasons.

However much this may be an important matter of national security within the US, public exposure of totally out-of-control criminal organisations like the NSA and the CIA is a good thing for the rest of the world. I just wish someone would hang out the washing of FSB, GRU and MSS too.

Tiri • **May 3, 2017 11:23 AM**

@Dirk

As far as stopping NSA and CIA crime, there is much going on that is auspicious. The EU is practically punching Theresa May in the face to remind her that she can't override the ECJ on surveillance. Brexit is likely to rip Northern Ireland loose because the ECHR underpins the Good Friday Agreement. Scotland's halfway out the door. So you have the most hardline US satellite disintegrating.

Meanwhile Merkel's got a friendship Drang nach Osten going now that DIHK is tired of the anti-Russia mass hysteria CIA stirred up. Merkel's got Austria, Spain, Greece, Cyprus, and half a dozen more with her on the imperative of friendly relations with Russia. More talking, less spying.

Sabrina de Souza is doing her community service, singing like a canary, safe in Portugal. Robert Lady lost his sumptuous Hannibal Lecter villa and he's quite disgruntled. He thinks CIA sacrificed the foreigners. This will be the easiest mafia rollup the Italian judiciary ever did. And CIA's international witch hunt for leakers raises the interesting prospect that they've lost control of BND - or they will, by alienating them with anti-transparency paranoia.

Sean • **May 3, 2017 1:02 PM**

"They [the US ally] monitored the [Russian] hackers as they maneuvered inside the U.S. systems...

That's surprisingly exactly what the Russian would have been capable to do with all these stolen weapons: once you got the weapons, the only things you need next are the methods. They would just have had to build a gigantic *in vivo* honeypot to study the US intelligence agencies attacking strategies against them.

Once these tools released by the Russian, the NSA couldn't have done differently than pretending the opposite, before any chance that the Russian reveal the true story : telling the totally opposite story, ie. they monitored the Russian attaching them... and it was epic.

That's one scenario among many others. If any producer passing by, please give me a call!

The Inquisition, What a Show! • **May 3, 2017 5:59 PM**

Wikileaks “crosses a line when it moves from being about trying to educate a public, and instead just becomes about intelligence porn,” Comey said. The organization just “pushes out information… without regard to the First Amendment values… and simply becomes a conduit for the Russian intelligence services… to damage the United States.”

Comey may be the stupidest FBI head in history. He mouths all the trendy catchphrases, like 'crossing a line' - a line with two contemptibly vague snatches of poesy on either side. And 'porn' - trending now because he sells it like hotcakes on Playpen, re-victimizing all the victims. Then he pulls, not the First Amendment, which is words, but First Amendment Values out of his flabby flagellated Opus Dei ass. Because, as everyone knows, FBI's nonexistent legislative charter makes them the Values Police. And Russian intelligence - you know, the guys that made a fool of him to the point where he can't find any trace of them.

Does he have like special elite dumb Jesuits to write talking points that resonate with imbeciles? They don't even square with his secret-society fanaticism. Comey's a fake Catholic, otherwise he'd know that Article 19 is Vatican Doctrine. He's enough to make you nostalgic for the little beady-eyed invert that set up this Gestapo.

Milo M. • **May 3, 2017 6:46 PM**

@John Goodwin

"if Clinton is right and WikiLeaks almost single handedly tipped the election with help from the DNC leaker and Podesta phisher, why is Trump so keen on bringing Assange to justice?"

Randomness as policy.

The scientific term is *entrumpy*.

Coyne Tibbets • May 4, 2017 12:55 AM

I think this is inevitable, and the question of who is pure minutia.

The security agencies loved technology, barring encryption. Every moment of every life, everywhere. After all, they presume everyone is a potential attacker.

They wanted perfect surveillance, now they have it, and it was nothing but pride that they believed they would not be subjected to it.

"It's a poor atom blaster that won't point both ways." -Isaac Asimov, *Foundation*.

Adam • May 4, 2017 9:38 AM

When it comes to nation state intelligence "communities" Occam's Razor doesn't necessarily apply.

Clive Robinson • May 4, 2017 11:11 AM

@ Adam,

> When it comes to nation state intelligence "communities" Occam's Razor doesn't necessarily apply.

If you think about it Occam's Razor only realy applies when there is neither freedom of choice nor is there indeterminacy.

When it comes to nation state IC's the only things that are realy deterministic is the outstretched hand towards the public purse, and the lying to cover up incompetence at all levels.

---

ab praeceptis • May 4, 2017 11:43 AM

Clive Robinson

When it comes to nation state IC's the only things that are realy deterministic is the outstretched hand towards the public purse, and the lying to cover up incompetence at all levels.

Pretty much sums it up. Well spoken.

Clive Robinson • May 4, 2017 12:22 PM

@ ab praeceptis,

The question that arises is how do we stop their behaviour without splitting atoms over their heads...

ab praeceptis • **May 4, 2017 12:43 PM**

Clive Robinson

"how do we stop their behaviour without splitting atoms over their heads."

A reasonable first step seems to be to create means for confidential communications to allow for that discussion.

Desmond Brennan • **May 4, 2017 11:00 PM**

Putin has been angling for over 20 years now, building up an arsenal of (physical, information & social) weapons. He was always dark, but gave up the pretense c 6 years back

He miscalculated on the Trump Op ...he set chaotic Russian Roulette in progress, and since c last May, he has been "all in"

Trump turned out more lunatic than expected, and Putin was likely glad of gropegate. WeinerLaptopGate seems to have been more home grown, but the Russians were hedging their bets on an insurgency if Hillary won ...almost to the closing line

By December, Putin realized he had a CI nightmare on hand ...it has been hand to hand combat in the engine room of Earth since...with the peverse incentive of the engine room being on fire (There is no MAD type equilibrium with the DPRK ...and cyber...is same ballpark problem)

HumInt , Information Warfare and Hard Cyber are those in the battle.

Putin and his anarcho-fascist (oxymoron intended) Chekism 2.0 Crimintern Empire is fighting to avoid being destroyed. The stakes are higher for them.

Bruce's game analysis bears out ...just over 24 hours back ...there was a wave of nastiness from Russia, the bombers with fighter escorts, the threats against Viber, WhatsApp etc by their Internet Regulator ...with the WA outage being related . Other things happened that the press miss ...most press just print what famous people tell them.

The Russian Empire knows of Trump falls, the blowback will be cosmic ...but...they are not Madmen ...they are just trying to draw us into a game of Russian Roulette ...where at least they have some chance.

Ratio • **May 5, 2017 12:03 AM**

@Gerard,

> If you mean human suffering at large scale, that is caused by roughly three reasons.
> One is exploitation (with tyranny), second by military intervention and third by nature.
> The first two are caused by people who want to become rich at the expense of others.

So is, for example, the current situation in Venezuela the result of 1. exploitation, 2. military intervention, or 3. nature?

Or, since you are looking at the last hundred years, another example. How about the Soviet famine of 1932–33? A couple of million die because of 1. exploitation, 2. military intervention, or 3. nature?

Seems your classification needs a bit of work.

Ratio • **May 5, 2017 12:12 AM**

@Gerard,

Not "couple of million" in the literal sense, obviously. (Most estimates I've seen are between 6 and 8 million.)

Subscribe to comments on this entry

Leave a comment

Login

Name (required):

E-mail Address:

URL:

Remember personal info?

Fill in the blank: the name of this blog is Schneier on _____ (required):

Comments:

Allowed HTML: <a href="URL"> • <cite> <i> • <b> • <sub> <sup> •   • <blockquote> <pre>

Preview Submit

← Friday Squid Blogging: Live Squid Washes up on North Carolina Beach

Fitbit Evidence Used in Murder Investigation →