# Schneier on Security

← Friday Squid Blogging: Squid Beard

2008 Cyberattack Against Turkish Oil Pipeline →

## Reacting to the Sony Hack

First we thought North Korea was behind the Sony cyberattacks. Then we thought it was a couple of hacker guys with an axe to grind. Now we think North Korea is behind it again, but the connection is still tenuous. There have been accusations of cyberterrorism, and even cyberwar. I've heard calls for us to strike back, with actual missiles and bombs. We're collectively pegging the hype meter, and the best thing we can do is calm down and take a deep breath.

First, this is not an act of terrorism. There has been no senseless violence. No innocents are coming home in body bags. Yes, a company is seriously embarrassed--and financially hurt--by all of its information leaking to the public. But posting unreleased movies online is not terrorism. It's not even close.

Nor is this an act of war. Stealing and publishing a company's proprietary information is not an act of war. We wouldn't be talking about going to war if someone snuck in and photocopied everything, and it makes equally little sense to talk about it when someone does it over the internet. The threshold of war is much, much higher, and we're not going to respond to this militarily. Over the years, North Korea has performed far more aggressive acts against US and South Korean soldiers. We didn't go to war then, and we're not going to war now.

Finally, we don't know these attacks were sanctioned by the North Korean government. The US government has made statements linking the attacks to North Korea, but hasn't officially blamed the government, nor have officials provided any evidence of the linkage. We've known about North Korea's cyberattack capabilities long before this attack, but it might not be the government at all. This wouldn't be the first time a nationalistic cyberattack was launched without government sanction. We have lots of examples of these sorts of attacks being conducted by regular hackers with nationalistic pride. Kids playing politics, I call them. This may be that, and it could also be a random hacker who just has it out for Sony.

Remember, the hackers didn't start talking about *The Interview* until the press did. Maybe the NSA has some secret information pinning this attack on the North Korean government, but unless the agency comes forward with the evidence, we should remain skeptical. We don't know who did this, and we may never find out. I personally think it is a disgruntled ex-employee, but I don't have any more evidence than anyone else does.

What we have is a very extreme case of hacking. By "extreme" I mean the quantity of the information stolen from Sony's networks, not the quality of the attack. The attackers seem to have been good, but no more than that. Sony made its situation worse by having substandard

security.

Sony's reaction has all the markings of a company without any sort of coherent plan. Near as I can tell, every Sony executive is in full panic mode. They're certainly facing dozens of lawsuits: from shareholders, from companies who invested in those movies, from employees who had their medical and financial data exposed, from everyone who was affected. They're probably facing government fines, for leaking financial and medical information, and possibly for colluding with other studios to attack Google.

If previous major hacks are any guide, there will be multiple senior executives fired over this; everyone at Sony is probably scared for their jobs. In this sort of situation, the interests of the corporation are not the same as the interests of the people running the corporation. This might go a long way to explain some of the reactions we've seen.

Pulling *The Interview* was exactly the wrong thing to do, as there was no credible threat and it just emboldens the hackers. But it's the kind of response you get when you don't have a plan.

Politically motivated hacking isn't new, and the Sony hack is not unprecedented. In 2011 the hacker group Anonymous did something similar to the internet-security company HBGary Federal, exposing corporate secrets and internal emails. This sort of thing has been possible for decades, although it's gotten increasingly damaging as more corporate information goes online. It will happen again; there's no doubt about that.

But it hasn't happened very often, and that's not likely to change. Most hackers are garden-variety criminals, less interested in internal emails and corporate secrets and more interested in personal information and credit card numbers that they can monetize. Their attacks are opportunistic, and very different from the targeted attack Sony fell victim to.

When a hacker releases personal data on an individual, it's called doxing. We don't have a name for it when it happens to a company, but it's what happened to Sony. Companies need to wake up to the possibility that a whistleblower, a civic-minded hacker, or just someone who is out to embarrass them will hack their networks and publish their proprietary data. They need to recognize that their chatty private emails and their internal memos might be front-page news.

In a world where *everything* happens online, including what we think of as ephemeral conversation, everything is potentially subject to public scrutiny. Companies need to make sure their computer and network security is up to snuff, and their incident response and crisis management plans can handle this sort of thing. But they should also remember how rare this sort of attack is, and not panic.

This essay previously appeared on Vice Motherboard.

EDITED TO ADD (12/25): Reddit thread.

Tags: cyberterrorism, cyberwar, hacking, North Korea, privacy, Sony

Posted on December 22, 2014 at 6:08 AM • 112 Comments

## Comments

**bitstrong** • **December 22, 2014 6:35 AM**

Didn't Mandiant and the FBI both say the level of sophistication of the attack was such that few networks could have withstood it? The CEO called it unprecedented .All the stuff that comes out after the fact - oh, there was some carelessness, is ultimately irrelevant. Corporations spend tens of billions of dollars on network security and employee education and on pentests and consultants. And even though it's been said countless times that defense has to be right ALL the time and an attacker only has to be right ONCE, you will continue to spew the same tired self-serving garbage, carefully back-treading when necessary to spin it anyway you want. And here come the dopey suck-ups....

---

**Jens** • **December 22, 2014 6:51 AM**

I'm sorry, I still can't believe the accusations towards north korea. We've seen that the nsa collects every bit of data possible, even from their "friends". One would assume that these surveillance is much bigger towards enemy states like north korea. Additional, there is not that much traffic from that country as technology advancement there isn't really the site it is in the us or europe. So I really can't imagine that a hacking operation of this size wouldn't triggered some kind of alarm.
I suspect the accusations to be some kind of covering operation which should hide the documents leaked after the hack, in which you can find information about massive corruption towards politics and state attorneys in the fight against piracy. This is serious enough for some people to start those accusations and war threats as distraction.

---

**David Penfold** • **December 22, 2014 8:09 AM**

And furthermore, if the US hacks foreign servers, it's for "legitimate governmental interests". American exceptionalism once more...

https://twitter.com/dellcam/status/546080068272132096

---

**Tualha** • **December 22, 2014 8:13 AM**

And now, Obama is saying the internet needs more regulation because of this. The really ironic part is where he says cybersecurity is an urgent issue, while under his orders, the NSA is doing their best to undermine everyone's cybersecurity. Yeah, we can really trust Obama to do the right thing with the internet.

---

**Myriam** • **December 22, 2014 8:23 AM**

I'm so glad you exist. Thank you! you're the voice of reason. (I mean it)

---

**steve • December 22, 2014 8:32 AM**

Sooner or later, companies will be dragged unwillingly into a legal or regulatory regime where they have to pay for their poor security when their negligence exposes other people's data. It may happen through legislation or through insurance. Then they will suddenly find ways to stop getting hacked through more preventible vectors like malicious PDFs, Flash, MS Office docs, USB drives and so forth. It may even mean (at last) a shift away from Microsoft products.

The corporate world will resist this reform as long as possible - why pay to avoid imposing costs on others, when you can get away with it? But with an inescapable mandate, at least it would no longer mean a competitive disadvantage, because all the competitors would have to do likewise.

---

**Cp • December 22, 2014 8:34 AM**

The government and press statements are giving me flashbacks to the WMD allegations in Iraq (which were given by false-flag informants)

---

**Ken • December 22, 2014 8:40 AM**

"I personally think it is a disgruntled ex-employee"

That gets my vote.

I also think the analysis that the FBI used to identify NK as the culprit probably came from an FBI employee who was hired before Obama became president, and does not like Obama or his policies. The only justification for labeling this as state sponsored is political, and it doesn't benefit Obama politically to do this if it is incorrect.

What also doesn't make sense is hackers thratening to attack movie theaters. You don't have to break into computers to do that. This is more evidence that whoever did this is just messing with Sony.

---

**SR • December 22, 2014 9:09 AM**

"I personally think it is a disgruntled ex-employee"

The SPE hacker exfiltrated terabytes of data, and wrote custom malware to own every Windows box at the corprorate headquarters. You really think a disgruntled ex-employee is capable of doing that?

The SPE hacker didn't just leak embarrassing corporate emails. They doxxed 15,232 current or former co-workers addresses, social security numbers, and banking details which are now selling on carding websites. You really think an ex-employee is so disgruntled that they're going to burn their friends and colleagues?

"Nationalistic cyberattack was launched without government sanction" seems plausible, but the "lone wolf" theory seems pretty implausible.

Disclosure: I am a former SPE employee doxxed by the leak.

---

**Bob S.** • **December 22, 2014 9:09 AM**

I think it's pretty funny myself. Maybe more funny than the dumb movie.

Let's not forget the very sordid Sony rootkit affair of 2005-7. And, that our own government feels free to root around every computer drive in the world, literally.

It's all legal you know, if you are exceptional.

---

**vas pup** • **December 22, 2014 9:16 AM**

@Bruce: “they're certainly facing dozens of lawsuits: from shareholders, from companies who invested in those movies, from employees who had their medical and financial data exposed, from everyone who was affected. They're probably facing government fines, for leaking financial and medical information, and possibly for colluding with other studios to attack Google.” They deserve those punitive measures! Now, unfortunately, money is the only powerful tool left to affect behavior in any direction (positive or negative).
Attack was not act of terror or war as Bruce noticed absolutely right (just want to add that regardless of absence human casualties target is not element civil/national infrastructure: power grid, health system, water supply, air traffic, etc. or military object – base, communication, command and control, etc.), In this case US gov. reaction was right, balanced and reasonable, and our ‘peace doves’ in Congress should chill out on that and not escalate on this particular case. On other hand, I guess lessons were learned out of this case for necessity of development/adjustment security plans/measures for such objects against similar attacks. Regarding exceptionalism: let say North Korea created movie with the similar plot to kill POTUS or leader of the other developed country (e.g.Japan, GB, etc.). Are we going to react emotionally in the same way if target of cyber attack is North Korean movie company (public I guess)?

---

**Anon** • **December 22, 2014 9:33 AM**

Thing I most want to see in the leaked emails : low-level IT staffer bringing up the lack of security and the potential damage a serious breach would bring, followed by a dismissive reply from a supervisor.

---

**Mr E** • **December 22, 2014 9:36 AM**

Perhaps just coincidence that Sony were working on a politically charged film at the time of the hack, given the rush of security companies to discover APT's and state sponsored 'cyberwar' doesn't this generate an atmosphere where the tendency is to jump to conclusions like they

have rather than face the fact that it may well have been a handful of spotty kids living in their moms basement that managed to penetrate this huge corporation.

---

**R. Pito Salas** • **December 22, 2014 9:37 AM**

@bitstrong "you will continue to spew the same tired self-serving garbage, carefully back-treading when necessary to spin it anyway you want. And here come the dopey suck-ups...."

This is not a dopey suck-up but an honest question about how this is self serving and/or how the author of the article has a conflict of interest? I guess I wasn't aware.

---

**Mr E** • **December 22, 2014 9:38 AM**

Furthermore given that Sony apparently consulted with the State department about the film and knew it would be provocative and likely to anger the NK govt they may well have been anticipating some kind of backlash, again leading them to jump to conclusions.

---

**ned_flanders** • **December 22, 2014 9:44 AM**

SR,

While it sucks that your information is in the wild, you can thank your former c-level leaders and Microsoft for it.

The only reason this has become national security theater is Hollywood's paid access to Congress and the Executive office.

---

**Mr E** • **December 22, 2014 9:50 AM**

Emails Reveal US State Department Influenced Sony's "The Interview" so as to Encourage Assassination and Regime Change in North Korea

"Sony Emails Say State Department Blessed Kim Jong-Un Assassination in 'The Interview.'" The emails also reveal that a RAND corporation senior defense analyst who consulted on the film went beyond "blessing" and outright influenced the end of the film, encouraging the CEO of Sony Entertainment to leave the assassination scene as it was (in spite of misgivings at Sony) for the sake of encouraging North Koreans to actually assassinate Kim Jong-Un and depose his regime when the movie eventually leaks into that country. According to the Sony CEO, a senior US State Department official emphatically and personally seconded that advice and reasoning in a separate correspondence. The emails also reveal that the U.S. special envoy for North Korean human-rights issues also consulted with Sony on the film.

---

**ned_flanders** • **December 22, 2014 9:54 AM**

Sony c-level is desperate to lay the blame outside their hallowed high school playground.

North Korea has everything you need in a scapegoat. They are an American political enemy, little is known so there is plenty for practically everyone in the U.S. to fear. The unreleased movie is **great** blame shifting.

Just don't talk about the amount of time required to move all the data stolen, don't talk about the c-level negligence and whatever you do, do not speak of Microsft's weak product.

---

**previousnext** • **December 22, 2014 10:05 AM**

> We wouldn't be talking about going to war if someone snuck in and photocopied everything, and it makes equally little sense to talk about it when someone does it over the internet.

Although I agree with your general thesis that this was not an act of war (and also with your oft-repeated stance that the word "war" is thrown around far too easily), the above sentence minimizes what happened here in order to support this thesis. A more accurate metaphor would be to say that someone snuck in, photocopied everything, made copies available to anyone who wanted it - *and* destroyed the originals, *and* seriously damaged the physical infrastructure.

And you leave something else out of your metaphor: One can argue about how seriously one should take the threat, but a threat to blow up movie theaters is, by definition, a terroristic threat.

---

**ɦɪɳʈɛɾlɑɳძʒɾ** • **December 22, 2014 10:16 AM**

I've always found Schneier's blog to be an amazingly grounding read, especially when the echo chamber of social media is at its worst. Thank you, Bruce!

---

**Ray Dillinger** • **December 22, 2014 10:18 AM**

Of course we have a word for it when it happens to a company! The word is dox. Exactly the same as when it happens to anyone. Sony got doxed.

Just because the victim is a corporation or an oligarch rather than a prole, doesn't make it into a different crime.

Any laws against what happened to Sony, need to protect everyone else as well. The crime is the same crime and everybody deserves the same protection under law.

---

**ned_flanders** • **December 22, 2014 10:39 AM**

@Ray Dillinger,

It is a different crime. This time it happened to one of the copyright cartel members who

generously fund politicians to protect their business from competition.

If it happened to you or I no one would be talking about it being an act of war. The President would not be having a press conference about it either.

@previousnext

What serious damage was done to their network? Did someone break in and smash stuff to bits? No. The serious damage was Sony c-level was finally trapped by their own negligence.

I too am waiting for the IT worker-level emailed warnings about their infrastructure and the dismissive replies from further up the chain.

---

**Clive Robinson** • **December 22, 2014 10:45 AM**

@ SR,

> The SPE hacker exfiltrated terabytes of data, and wrote custom malware to own every Windows box at the corprorate headquarters. You really think a disgruntled ex-employee is capable of doing that?

Short answer "yes".

Long answer, it's because of the very reasons you give that it is way more likely an insider or ex-insider was involved.

To get terabytes of information out of organisations like SPE you need a lot of inteligence or luck or both to avoid triping alarms or an "inside man". This is because the alarms should not be visable from either outside of or on the network. If they are then they have been set up in a rather stupid way, thus a true outsider would have to be lucky in some way, which to be blunt "Only happens in the movies", "whilst Jef Bloom smokes a cigar".

It is not even considered "best practice" but "required practice" these days for organisations of the size of SPE --and a lot smaller-- to fit exfiltration alarms, that cannot be seen on the network they are monitoring.

Now if they were not fitted that's negligence, if they were not setup to detect such abnormal network traffic that's negligence, if they were setup in such a way they were visable on the network in any way that's negligence, if documentation refering to the network security was available on the network that was negligence.

I could carry on but it's clear that if SPE were attacked by a pure outsider then it's negligence on their behalf and that's what the lawyers will argue and fairly easily prove when a class action starts on behalf of those harmed.

The only way it could not be negligence is if an insider or ex-insider arranged things such that getting a very exceptional chunk of data out on the network without raising alarms was

possible.

I'm sorry for you and others who have had their details and other PII etc revealed to the world, employers should know a lot better than this these days and they have no excuse, and it is their policy not a bad actor who is to blaim. The reason for this is a reasonable policy would have mitigated most of the harms a bad actor could perform. Knowledge of this mitigation requirment was made glaringly obvious by Ed Snowden and his exfiltration of data from the NSA.

I may sound like I'm being harsh about SPE managment, but unlike you I'm not the one who has been harmed by their lack of suitable policy when it comes to ICT security, their choice was not to make the required investment, now they are probably wondering how to avoid the law suits...

---

**vas pup** • **December 22, 2014 10:49 AM**

@Anon • December 22, 2014 9:33 AM. Greedy pays twice!
You may not have crystal ball, but your vision is looks like very true. By the way, President Of Sony Pictures claims on exclusive interview on CNN/GPS (as best as I recall) Company does have insurance against cyber attack. So, who is going to feel financial pain to generate Pavlovian reaction on bad security?

---

**Fred** • **December 22, 2014 10:59 AM**

Who's calling for war and missile strikes at DPRK ? I've never heard that from anyone I spoke to. We must live in a different world.

---

**anonymous** • **December 22, 2014 11:08 AM**

Just follow the trail...of bodies under the bus...

---

**Kurt** • **December 22, 2014 11:15 AM**

@ Bruce "I personally think it is a disgruntled ex-employee"

People have been saying this for weeks...

How hard is it to loc a disgruntled ex-employee with the h4x0r skills to pull this off?

Given our government's internet powers, not very hard to find this guy or girl, isn't it?

---

**Mr E** • **December 22, 2014 11:23 AM**

Makes a much more engrossing story than that torture report thing

---

**Greg Linden** • **December 22, 2014 12:21 PM**

Bruce, I'd very much enjoy hearing more about whether this big payoff means any change in the frequency of these attacks.

You suggest that we won't see any change, but I'd predict the opposite. This was a very cheap politically-motivated operation that yielded a massive payoff. I'd think that this big payday would motivate many more attempts to do something similar. And there have to be many other corporations and government organizations that have similarly weak security and would be equally easy targets.

Could you elaborate on your thoughts on this more? You don't think this example of a massive payoff will encourage more of these politically-motivated attacks?

---

**previousnext** • **December 22, 2014 12:29 PM**

No, @ned_flanders, no one broke in and smashed stuff to bits in a literal sense. Mr. Schneier used a physical-world metaphor to describe what happened. I gave what I thought was a more accurate physical-world metaphor. In my metaphor, paper copies are made (in the actual incident, digital copies are made). In my metaphor, the original papers are destroyed (in the actual incident, Sony's original digital files were destroyed). In my **metaphor**, the physical infrastructure is destroyed (in the actual incident, it is reported that Sony's software infrastructure is has been rendered unusable. Payroll can't be processed, etc.).

You are taking my metaphor and saying, That didn't literally happen! You're right - it didn't literally happen.

---

**Joe** • **December 22, 2014 12:38 PM**

Interesting how the media jumped on this, there are now breaches everyday and no action is done. The US is the weakest and most targeted link and no new security software will fix this as the problem can happen from different perspectives... no end in sight.

---

**ned_flanders** • **December 22, 2014 12:45 PM**

@previousnext,

Ok. Sorry for getting too literal. I hope they had more resources for DR than they did security!!!!

The trail of bodies thrown under the bus is a very good metaphor. It will be very interesting to see how much excrement is pushed downhill onto others.

---

**ned_flanders** • **December 22, 2014 12:57 PM**

@joe,

There are some meaningful improvements though. No one at c-level is interested in deploying them. There is no perfect solution. But a network can be made much more difficult to penetrate and easier to monitor for unauthorized activity.

The likely c-level response scenario is a Big-IT vendor gets a contract to provide monitoring of a windows domain, with kickbacks naturally. Maybe Sony goes all the way and outsources all of their business IT? Movie production IT would be a totally different story.

Waiting for more. I've already bought my popcorn.

---

**uh... don't remember** • **December 22, 2014 1:21 PM**

We should stop calling these acts "hacking"... I woud prefer "cracking" or, from now, "making a Sony".

I agree, the U.S. are overreacting. On the other hand, they are not the right actors to talk about illegal activities related to information operations and CNO/CNE.

---

**George Capehart** • **December 22, 2014 1:26 PM**

There are several aspects of the aftermath that cause me some concern . . . Firstly, there is no smoking gun . . . only circumstantial evidence with no apparent means of confirming. Secondly is the fact our government seems to be putting itself on (cyber) war footing in a purely reflective, Chicken Little fashion. @Bruce observed that Sony execs are running around with no plan . . . given the state of their (info)security, therefore their whole risk management process, that doesn't surprise me. They are clueless. Well, it seems Washington is, too . . .

I can't find the reference immediately, but somewhere I read that Obama had been coordinating with other countries to form an alliance against North Korea. Now, I've been around infosec for 20 years or so, and I know how bad most institutions' security is . . . including the DoD and the NSA. I don't think any of the "management types" in Washington are any more clueful about security than are the execs at Sony . . . Manning talked about it in his chats with Lamo - “Weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis . . . a perfect storm.” They didn't learn anything from that . . . Then Snowden comes along and leaves bread crumbs for them to find to help them figure out what happened and they completely missed them.

There are two things to consider here: one is that they still don't have a clue how many other Mannings and Snowdens are playing around on those networks, two is that if those networks are that wide open, think about the condition of the rest of .gov. Then consider how many defense and other type contractors have links to .gov. I'm thinking that now is not an especially good time to pick a fight with anyone with serious network penetration skills.

One last thought: Again, I apologize for not being able to locate the source right now, but someone made the point that the hackers siphoned off 100 terabytes of data and that there is only one ISP in North Korea. They would have to have some awful big pipes coming in to

accommodate that amount of data and serve the rest of the country. To this thought, I'll add the observation that, even as incompetent as the NSA is on securing their internal network, they have a pretty good idea of what goes where on the internet backbones. Now, 100 terabytes passing over an IPv4 network with an MTU of 2500 bytes ads up to lots of packets. Given that 1500 bytes is more prevalent, that adds up to lots more packets. Given that the NSA (apparently) looks at every packet that goes over the internet, one would think that after a while the pattern of a whole lot of packets originating from a couple of IP addresses in the US heading to a couple of IP addresses in North Korea would become obvious. (Now, I know that it's possible to run across VPNs and hopscotch all around, but that adds a lot of overhead and increases the risk of detection. It might be possible to avoid detection if the data were sent in bursts with random intervals in between, but now we're talking about increasing the amount of time it takes to get the data moved.

Finally, what would North Korea want with employees' health records and stuff like that? A state actor doesn't operate this way. They don't post data that they've scarfed on Pastebin . . . This just doesn't look or smell like a state-sponsored attack.

Of course, they really could have done it and did it this way as a red herring to make people think they couldn't be that stupid . . . :-)

---

**jdgalt • December 22, 2014 1:26 PM**

At least one tweet, apparently from North Korea, admitting responsibility has turned out to be a practical joke. Here is the jokester owning up to it.

Which doesn't prove they didn't do it anyway. But that tweet at least is debunked.

---

**AM • December 22, 2014 1:32 PM**

The probability of this being a disgruntled ex-employee is proportional to the security of Sony's network. The harder the security, the more insider knowledge they needed to break in. From all that I've heard, read, and seen, I have the distinct impression that Sony's security could not have kept out even the most technologically inept great-grandparent.

On the other hand, Sony has pissed off a rather amazing number of technologically competent individuals on nearly every continent. And not once, but repeatedly. Taking away what folks have already paid for and own through software updates. That rootkit of theirs did, and continues to do, an amazing amount of damage. I've seen machines bricked by it. Without backups, that's expensive! Even with backups it's no fun. So this break-in was not only foreseeable, but inevitable.

That said, I think this talk of SSNs and personal data being sold on darknet sites is oblivious to the more obvious money making opportunities. Surely someone who can pull a stunt like this is smart enough to invest in put options on ADR (Sony) stock. Or perhaps short sell on a margin account if they're willing to take a little risk. Then again, such profits may tip their hand to authorities.

Consider who stands to gain Sony's business as they lose face? There's a lot more money involved there than what folks will make off the stock market.

Perhaps we shouldn't be so quick to rule out future attacks motivated by stock price manipulation or business competition. That's where the real profits lie.

---

**NobodySpecial** • **December 22, 2014 2:04 PM**

North Korea was first linked to the attack on December 7th.
Which state-level actor would wish to attack a Japanese corporation on 7 December?

---

**Buck** • **December 22, 2014 2:16 PM**

I wonder if they'll consult VisionSpear. ^_^
Keep that revolving door spinning!

---

**Clive Robinson** • **December 22, 2014 2:19 PM**

@ ned_flanders,

There are some very easy low cost changes that can be made to most corporate networks to increase security.

You first have to ask the following two questions,

1, does this user machine / server require Internet access?
2, does this user machine / server reqyire isolation from the corporate network?

In the case of HR and pay role the answer was almost certainly no in the first case and yes in the second for fairly obvious reasons.

The problem of course will be the howls of withdrawal from the likes of Facebook, twitter, grinder, et al by the staff...

Whilst I have a modicum of sympathy for their addiction most of the staff in that division of Sony have just found what the price of such adictions can be...

---

**Scared** • **December 22, 2014 2:25 PM**

@Cp:I agree the Sony hack is a false flag operation to show that we need the NSA to be able to track everything on the internet.
I just listened to a bunch of "experts" on KPBS debating the "US retaliation" against North Korea's infrastructure. It was as if they all read from the same script. And they couldn't stop mentioning Snowden over and over again.

**Skeptical • December 22, 2014 2:53 PM**

While I agree that the public evidence is insufficient to establish with high confidence that DPRK is responsible, the persuasive element is that President Obama not only did state that DPRK is responsible, but promised a proportional response at a time, place, and in a manner of US choice.

Keep in mind that a finding that DPRK is responsible, if it were innocent, is not in US interests. It's much easier if the responsible party is some private party that can be arrested and tried. It's much harder if the responsible party is an isolated government that loves to play brinksmanship politics.

So I do not see the President making such a statement without having very high confidence that DPRK is responsible. Nor do I see the US government, and the private consultants who were involved, as being anything less than completely diligent, since an unwelcome finding that DPRK is the responsible party would be subject to lots of double-checking and second-guessing, if only because ultimately that's not an answer that most people want to hear.

On a probably unrelated note, there are now reports circulating that North Korea's internet access has been completely shut down as of earlier today, following "technical problems."

---

**Jennifer • December 22, 2014 3:21 PM**

Terrorism doesn't require dead bodies to be called terrorism. When you do something on a massive scale that makes people change their lives because they're scared to death to do otherwise, that's terrorism. Terrorism = controlling people through the use of terror. (And usually there's a political agenda of some kind involved, either real or imagined.) It just happens that killing people is an easy and effective way to terrorize people.

---

**Tim • December 22, 2014 3:36 PM**

terrorism does not require dead bodies. It requires that the terrorist make a threat and for the victim to respond by changing their behavior as the terrorist desires. Doxing is a form of online terrorism imo.

Think of it this way: if a robber put his hand in a paper bag and pointed it at a clerk and told him to give over all the money is it armed robbery?

---

**Sancho_P • December 22, 2014 4:13 PM**

What a humiliating government allegation without evidence, unprofessional, without any need. - Is this American?

No, we shouldn’t remain skeptical but SILENT about the origins unless anybody has real evidence.

An embarrassing blunder of western government and the President of the U.S.A.
Do you think it will distract from the torture report? Probably in America.

Even if it turns out to be NK, the timing was wrong - the ammunition exploded at home.
*"… promised a proportional response at a time, place, and in a manner of US choice."* was obviously recorded by the local's Kindergarden surveillance CCTV?
Sung be a Nobel Peace Prize laureate?

If insider attack:
There is no way today's technology could stop an admin to leak emails or data.
Let's face it: We are vulnerable, probably because of our own paranoia.
We desperately need this kind of attacks to improve.
(I do not agree with @Clive Robinson that "a reasonable policy would have mitigated most of the harms" but I don't know enough details to discuss it)

Again, **I'm missing the broad discussion about the value of that film**
- although it still seems unknown whether it was the real target or not.
Probably this could be a lesson for Sony (and Co) not to go for every American wet-dream.

They deserve punishment not only for the incident but for the film in the first place.

@ Skeptical

I guess they had more than very high confidence for the "impregnable cave fortress" of Tora Bora (sorry, "many of those") and WMD in Iraq before going to war?

@ Jennifer, Tim

So NSA & Co are terrorists? The paper bag robber is a terrorist?
I think I didn't get the point.

---

**vas pup** • **December 22, 2014 4:17 PM**

@Jennifer and @Tim. You made a good point. On the other hand, cyber terrorism not = cyber warfare. The latter is addressed (as best as my humble understanding) to the country-sponsored cyber attack with particular tangible casualties (dead or mutilated bodies) or/and have as target critical infrastructure or military objects.

---

**Mr E** • **December 22, 2014 4:44 PM**

at least sony now have some good material for their next film.

---

**Captain Ned** • **December 22, 2014 4:51 PM**

FFS, what was unreleased and presumably valuable Intellectual Property content doing on servers with access to the 'Net? If you can't get this part right who cares about server

hardening and all of the buzzwords. Bloody hubris caused this, regardless of who actually did it.

---

**Rene** • **December 22, 2014 5:21 PM**

I may be naive, but why is this anyone's problem other than Sony's? Sony is a publicly traded multi-national company. Sony was, sadly enough, a victim of its own making. Corporations have to learn that brand protection is as important as shareholder return. And no, it is not the business of the American government or any other government to enforce enhanced security or to do anything else except to prosecute guilty parties to the full extent of the law.

---

**Steve** • **December 22, 2014 5:35 PM**

My theory, based on the same information being used to pin this on the NORKs (i.e., not much at all), is that it's the CIA, trying to deflect public interest from the release of the Senate Torture Report.

Think about it... the CIA knows that the report is coming out so they trot over from Langley to Fort Meade and load up a thumb drive or two with some nice No Such Agency penetration software (or just go to the dark net and get what they need for themselves -- there's plenty of it out there), hack Sony, and, presto, SQUIRREL!

Do I believe this is what happened? No.

Would I be surprised if was somehow related to the truth? No.

---

**steven** • **December 22, 2014 5:56 PM**

Maybe what the US needs is a "Great Firewall" for the nation, built by the most competent agencies and trusted commercial partners, to protect against all manner of nasty things infiltrating its Internets from the outside. *sigh*

@Steve: "My theory, based on the same information being used to pin this on the NORKs (i.e., not much at all)..." -- similarly, NK could accuse the CIA for the Internet outage they're having this weekend, even if that too could be the work of some teenage hacktivist and/or some amount of incompetence. It's horrifying to watch primitive hacking escalate to a diplomatic stand-off between countries, and who knows what next.

---

**Wesley Parish** • **December 22, 2014 5:56 PM**

This brings to mind JG Ballard's *The Atrocity Exhibition*, which Nelson Doubleday in 1970, showing the sort of dedication to free speech which we have all come to expect from US executives, ordered shredded. Why, I don't know: "Why I Want To Fuck Ronald Reagan" is an undervalued classic! As is indeed "The Assassination of John Fitzgerald Kennedy Considered as a Downhill Motor Race" ...

I'm also reminded of a Soviet-era Russian political joke: an American is explaining free speech to a Russian friend. "I can stand in the middle of Times Square and shout, "God damn you, Richard Nixon!" and nobody minds." The Russian replies: "Ah then, I also have free speech. I can stand in the middle of Red Square and shout "God damn you, Richard Nixon," and nobody minds either!"

I think we could all agree that David Cronenberg is the ideal director for a comedy about the assassination of the US President. He after all did the definitive interpretation of *Crash* ... which I had thought was unfilmable.

---

**Martin Merck** • **December 22, 2014 6:47 PM**

Rene, I would agree with you that Sony should be responsible for themselves, not the US Govt. This was an attack on Sony, not the US govt. But you know how things go. Govt is to stay out of business, unless business wants them in it.

Privatize the profits, Socialize the Loss.

---

**jdgalt** • **December 22, 2014 7:08 PM**

@NobodySpecial: *Which state-level actor would wish to attack a Japanese corporation on 7 December?*

Anyone that wanted to do a false-flag against the US.

---

**MrC** • **December 22, 2014 7:49 PM**

I'm still not sure about Skeptical, but Jennifer/Time is an obvious failure of persona management.

---

**Blah** • **December 22, 2014 8:18 PM**

"You really think an ex-employee is so disgruntled that they're going to burn their friends and colleagues?"

Considering how many workplace shootings we have in this country every year, I'd say being disgruntled is the easy part.

---

**Cory** • **December 22, 2014 8:27 PM**

@ Sancho_P:;If insider attack:
There is no way today's technology could stop an admin to leak emails or data.
Let's face it: We are vulnerable, probably because of our own paranoia.;

This is the nail that hurts. An over-powered surveillance state complaining about over-powered

insider admins. When technology and expertise become another revolving door, a grey area casts over everything black and white.

There are no clear-cut villains when the villain is among us. This is like a hollywood trilogy movie with a twist.

---

**Carlos** • **December 22, 2014 8:56 PM**

Yeah, I'm on the side of disgruntled employee too.

Someone said, but hey, would anyone attack their fellow empolyees? Why, yes, yes they would. You know, there's even an expression for it, "going postal".

Also, getting terabytes of data off a network using the Internet? Even if you had a very fast connection that would take a very long time -- literally days. And the huge spike in outgoing data would surely be noticed, unless, you know, someone was looking the other way.

On the other hand, you can easily fit an HDD with a few terabytes in your pocket. Or, if you have the time, and are afraid of getting caught with a HDD in your pocket, take a few 128GB MicroSD cards every day. These babies are tiny, and very easy to hide. They're also small enough that they likely aren't detected by metal detectors.

And if it indeed was someone working in IT, they'd obviously plant a lot of fake evidence to point the finger at someone else, and avoid being caught.

Oh, and a lot, if not all, of the sofware used in the hacking can be bought. And in case you're wondering where a lowly IT employee would afford that, remember that there are people in the world that make a living by selling pirated movies, selling personal information that can be used for various nefarious purposes.

---

**Cory** • **December 22, 2014 9:27 PM**

@ Carlos;

Where do we see this 100's of terabytes of data?

No evidence means non-existent. If it is not possible to pull that off the network, then perhaps they weren't stolen at all.

---

**Rob** • **December 22, 2014 9:30 PM**

I applaud you for the even keel reaction after some contemplation. I think that comes from more experience dealing with these sort of things over the years. kind of like decades of more data for a control system.. i think the bulk of the stolen info left sony not over the wire...

---

**Adrian** • **December 22, 2014 10:05 PM**

Inside job. Too much data to leech by means of internet. Like another person said.... the volume of data and wording selected for communication points towards inside job. However, there is more to this story. Our friendly govt cybersec experts know that already. A company on the fence the fence on giving in to blackmail or sinking is more probable.

---

**65535 • December 22, 2014 10:09 PM**

“Short answer "yes". Long answer, it's because of the very reasons you give that it is way more likely an insider or ex-insider was involved. To get terabytes of information out of organisations like SPE you need a lot of inteligence... avoid triping alarms or an "inside man". This is because the alarms should not be visable from either outside of or on the network.” –Clive

I agree.

“I apologize for not being able to locate the source right now, but someone made the point that the hackers siphoned off 100 terabytes of data and that there is only one ISP in North Korea. They would have to have some awful big pipes coming in to accommodate that amount of data and serve the rest of the country… 100 terabytes passing over an IPv4 network with an MTU of 2500 bytes ads up to lots of packets. Given that 1500 bytes is more prevalent, that adds up to lots more packets. Given that the NSA (apparently) looks at every packet that goes over the internet, one would think that after a while the pattern of a whole lot of packets originating from a couple of IP addresses in the US heading to a couple of IP addresses in North Korea would become obvious.” -George Capehart

I basically concur. 100 Terabytes is a lot of data to go unnoticed [even if the TCP segments were longer than the MTU].

I suspect the “Terabytes of data” could have come from various backups – ether copied or stolen and carried out on multiple Terabyte HDDs.

Next, the canceling of the movie – which some say "sucked" [and could have produced huge financial losses].

Thus, any excuse such a “terrorism at movie theaters” would be a viable reason to cancel the move and avoid further loses.

'…according to CNN there is a "sad irony" in the fact that "one of the great tests of America's freedom of speech should involve a movie that, according to some reviewers, utterly sucks".' - The Week

http://www.theweek.co.uk/world-news/61845/the-interview-was-sony-wrong-to-cancel-the-release

[negative film review]

“…the makings here of a buffoonish espionage farce in the tradition of Woody Allen’s “Bananas” or Elaine May’s underrated “Ishtar,” but just when “The Interview” should be revving

its comic engines, it seems to hit the brakes. By far the movie's funniest, most outre scene is its first: a phalanx of patriotic North Korean schoolchildren singing… It's a strategy that deprives "The Interview" of one of its richest comic possibilities: seeing these two characters at play in the world's most isolated, information-deprived "republic." … Rogen and Goldberg never get a sustained comic rhythm going, and they bungle even some of their better gags. The slow-acting poison with which the characters are meant to contaminate Kim, concealed on a small adhesive strip, practically begs to be passed around like a hot potato, or perhaps lost in a Band-Aid factory, but all we get is a rather lame bit about Aaron having to conceal the poison (and its large conical container) inside his rectum… The hype around "The Interview" suggests a take-no-prisoners dirty bomb of a movie, but the reality is more like a deflated whoopee cushion. It goes splat." –Variety

http://variety.com/2014/film/reviews/film-review-the-interview-1201376293/

If the movie was perceived to be a money loser this adds more suspicion to the fact that Sony had a monetary reason to cancel it – and did – while taking advantage of an internally generated IT faux pas.

---

**Jeffrey Radice • December 22, 2014 11:14 PM**

@Clive Robinson:

All signs point to negligence, if even pieces of this article at fusion.net are provable:

http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/

Start with the organizational structure of Sony Pictures Entertainment cyber security team. How much more do you need than their org chart (can't corroborate that) and the public comments that Jason Spaltro has made about risk (can be corroborated). If Spaltro's comments are to be taken at face value, the company was deliberately not spending enough to stay ahead of the problems they were facing.

I count 3 individual contributors (analysts) reported up to 8 Pointy Headed Bosses (3 Mgrs, 3 Directors, Ex Dir & EVP). To compound the understaffing, the organization is optimized for a lot of meetings and no real work getting done. Remove 2 Mgrs, 1 Dir & Ex Dir and replace them with 4 talented hands-on types and you already have a better structure to defend against advanced persistent threats at less cost. What were all those managers and directors doing? Seriously?

I don't buy the theory that it was North Korea. I also don't buy the theory it was an insider. Whoever it was, it was a dedicated team of individuals working over months if not years . . . to infiltrate and explore and escalate privileges. That type of infiltration didn't happen overnight. That doesn't mean it wasn't preventable by the company. They could have made it a lot more difficult than they did. It's negligence and they brought in Mandiant for damage control. Nothing Mandiant, nor the FBi nor Obama says should be considered trustworthy. They have their own

agendas, which are sometimes at odds with the truth.

If you start thinking about exfiltration along month-yrear timeframes, in a company where video streams and packages are being pushed around. How difficult would it be to pull out any data you want through an rtp pipe that shows up as normal to the systems? Even if SPE spent ducats on the best exfiltration alarm tools money could buy, no signs suggest they spent enough on staff to configure and monitor the output of said tools . . . at least from the evidence presented to me thus far.

---

**Paul Harper** • **December 22, 2014 11:29 PM**

@bitstrong Mandiant is a great company with some of the best people in Information Security. However Mandiant's marketing element is hardly going to say that Sony needs to be hit repeatedly with a lart due to their complete lack of clue regarding security. Look at how clueless their $300,000 a year Director of Information Security Jason Spaltro is regarding basic password security. http://www.dwheeler.com/essays/sony-lax.html

Hacking into Sony would NOT take much sophistication. What was sophisticated was how they behaved once they were inside. As John Robb points out they were patient in mapping the entire Sony network and in how the slowly released document. http://globalguerrillas.typepad.com/globalguerrillas/2014/12/sony-and-how-corporations-go-to-war.html

It was the same as the doxing of HBGary only on a larger network.

I still see this as more likely to be a Lulsec/Anonymous type group rather than a Nation State for the reasons that Bruce Schneier lists below. The lack of reference to the movie for several weeks before the press mentioned it seems like a massive hole in the North Korea hacked Sony narrative. http://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/

Actually the most difficult thing in the Sony Hack may have been trying not to trip over the rootkits from all the other hackers who must have been inside that network.

---

**Jeffrey Radice** • **December 22, 2014 11:55 PM**

Encrypted Steganography over RTP exfiltration very do-able and likely undetectable. How do you defend against a trickle of that over weeks to months, within an organization that doesn't take security seriously enough from the top down? You don't.

http://druid.caughq.org/presentations/Real-time-Steganography-with-RTP.pdf

http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-de_lancaster_technical_report.pdf

@Paul Harper, Mandiant has an agenda that is orthoganal to the truth. The company serves

Sony, not the public interest, regardless of the quality and individual honesty of people inside the company.

---

**A most conservative liberal • December 23, 2014 12:08 AM**

Bruce, you are a pacifist.

If the NOK invaded your electronic life, you'd feel differently.

Meantime, it is attitudes like yours that allows for the bad buys to run amok.

I say, nuke the NOK Internet connectivity permanently.

Seriously.

---

**Nick P • December 23, 2014 12:42 AM**

@ a most conservative liberal

Being famous in INFOSEC, he's probably had dozens of organizations and their malware try to infiltrate his life. Understanding INFOSEC and related issues, it doesn't change his opinion of situations like this as reality is reality regardless of how much something scares you or can damage you.

Bad guys run amok because of human nature, how our systems work, and our liberties. The price of democracy and an innocent until proven guilty by due process system is that some criminals might go free to protect innocent people from prison. Founding Fathers thought that was a good tradeoff and so do I. Yet, Congress, Executive Branch, FBI, spy agencies.... all have been involved in all sorts of corruption for decades straight. They aren't trustworthy. FBI is contributing to terror plots to arrest said terrorists, NSA is weakening security across the board, and CIA does whatever the hell it wants. All with criminal immunity. No wonder the situation is so bad wherever these have influence.

Relative to nuking North Korean Internet they might have done it: they're experiencing a bunch of problems coincidentally. That's not wise, though. The better position for regime change is to do what Tor, etc are doing and give North Koreans *more* Internet. Let people see the outside world, the truth. The more that do and the easier/stealthier they do it the more will be on our side. Cutting the Internet off is utterly stupid as their leaders can just claim U.S. is attacking them for no reason because we're evil and North Koreans should put more effort into fighting America. And so on.

So, you're full of crap. Strange enough, the kind of crap that benefits both the NSA and North Korea's government simultaneously. You should get an award for that.

---

**Thoth • December 23, 2014 12:43 AM**

@A most conservative liberal
It is too hasty to nuke someone's Internet off the Earth's orbit. There are possibilities of someone borrowing another person's hand to beat up other people and that's very possible. There are no really hard evidences of Nork responsible but also no way to possibly deny Nork involvement. We are just basing decisions based on somewhat murky guesswork and same goes on the Washington side.

Even if US were to not service Nork network, what makes you think other countries would do likewise to similarly block Nork IP addresses ?

The main thing that needs to be done after the mess is to do post-disaster remedial actions. Fix the holes, analyse the impact, remediate impact, learn the lessons, formulate post-diaster actions and rinse and repeat. About time big companies sit down and think the worth of their data security and start to do something really meaningful about it. Those normal Cisco firewalls, routers, switches and F5 stuff are not going to be adequate. Something as rich as Sony should be able to afford higher assurance methodologies and practices and should have already implemented them.

---

**Thoth • December 23, 2014 2:09 AM**

@Jeffrey Radice
Steganography via RTP is kind of close to Kleptography. Interesting concept and current in the rise, where data are hidden or encrypted and sent over a hidden channel in some form usually that is close to unnoticeable. Only defense is air gap with data separation (data diodes).

---

**Christopher • December 23, 2014 2:54 AM**

@Jeffrey Raddice, "I don't buy the theory that it was North Korea. I also don't buy the theory it was an insider. Whoever it was, it was a dedicated team of individuals working over months if not years . . . to infiltrate and explore and escalate privileges. That type of infiltration didn't happen overnight. That doesn't mean it wasn't preventable by the company. They could have made it a lot more difficult than they did. It's negligence and they brought in Mandiant for damage control."

If that is true then what is the motive?

NOK has the strongest motive.

---

**Gerard van Vooren • December 23, 2014 3:12 AM**

@ Mr E - December 22, 2014 9:50 AM

"Emails Reveal US State Department Influenced Sony’s “The Interview” so as to Encourage Assassination and Regime Change in North Korea"

Do you have any links?

**Mr E • December 23, 2014 3:30 AM**

@Christopher "NOK has the strongest motive"

Sorry but corporations the size of Sony with vast infrastructure are faced with attacks from a multitude of threat actors every day and it is far too simplistic to suggest NK 'has the strongest motive' simply because Sony happened to be working on a film poking fun at the country when they suffered this breach.

Yes that kind of infiltration and data exfiltration doesn't happen overnight. But sprawling corporate and institutional networks can incubate small compromises that go unnoticed for months or years and there may well have been multiple, entirely distinct bad guys who had gained access to parts of the network independently with a variety of motives. Even opportunistic hackers can have a very high level of sophistication in their attacks and frankly I see more security theater in the public discourse on incidents like this than rational informed analysis.

While talk of 'cyberwarfare' and so on generate headlines and fuel peoples imaginations, the reality of computer security is often quite mundane.

---

**Mr E • December 23, 2014 3:31 AM**

@Gerard Van Vooren

http://antiwar.com/blog/2014/12/18/state-dept-the-interview/

http://www.thedailybeast.com/articles/2014/12/17/exclusive-sony-emails-allege-u-s-govt-official-ok-d-controversial-ending-to-the-interview.html

---

**JestInCase • December 23, 2014 4:01 AM**

Everyone gets to have an opinion. Here’s mine:

I think it is likely that there are at least two actors involved in the Sony hack. There seems to be at least some likelihood that there are three. Note that only the first is assumed to be a single individual.
• The enabler: A current or former IT employee, say a SysAdmin or Network Manager. He has the keys to the castle and knows where the treasure is stored. This person had the time to exfiltrate the data and the knowledge of the entire network. Must have pretty good OPSEC skills since we haven’t seen his head on a pike. Yet. Motive: Revenge.
• The profiteer: Could be a straight ‘for profit’ motive. Could be a rival wanting the inside scoop on a narrow segment of the business. Could be the usual actors looking for identity theft items. Motive: Profit.
• The joker: Actor one or two passed the data that didn’t fit with their plans off to the joker to act as a smoke screen covering the original theft by obfuscation. Motive: For the lulz, man. For the

lulz.

As far as the (in)security of Sony, I submit that it is very likely that the majority of publicly held corporations have similar situations. See this:
http://www.cio.com/article/2439324/risk-management/your-guide-to-good-enough-compliance.html
QUOTE
“The dirty little secret here is that everybody tries to figure out how much risk they can assume without being embarrassed or caught,” says David Taylor, a former Gartner security analyst and now vice president for data security strategies for Protegrity, a security and privacy consultancy. “The people I regularly talk to are trying to figure out if [their security] fails, what’s the smallest amount they need to do to stay out of trouble and how they can blame someone else.”
/QUOTE

---

**Gerard van Vooren • December 23, 2014 4:12 AM**

@ Mr E

"The claim that the State Department played an active role in the decision to include the film’s gruesome death scene is likely to cause fury in Pyongyang. Emails between the Sony Entertainment CEO and a security consultant even appear to suggest the U.S. government may support the notion that The Interview would be useful propaganda against the North Korean regime."

Now match that comment with this:

"The Government of North Korea has a long history of denying responsibility for destructive and provocative actions," NSC spokesman Mark Stroh said.[1]

They are both clearly playing games. It also reminds me again of the hypocrites the White House officials are. Because if I replace NK with US in that sentence I can come up with a long list in no time.

[1] http://www.reuters.com/article/2014/12/20/sony-cybersecurity-usa-idUSL1N0U40IN20141220

---

**Clive Robinson • December 23, 2014 5:56 AM**

@ jestincase,

The problem with the later points in your theory is they fit some of the known points rather to well but others not at all... so is likely to be wrong in part (but that's true for most of the "full theories" put here). Let's see if it's possible to fill the gaps a bit ;-)

As has been noted the subject of the film did not come up in the earlier threats and demands. In fact it did not come up untill after the critics had said the film was the sort of turkey you don't want spoiling what otherwise might be a good time... Thus Sony have a couple of problems a 100million USD turkey that is going to be a box office fail and major hole in the finances -- which means reduced C-level bonuses-- and an extortion attack which is going to let all their extreamly dirty laundry be seen in public which is likely to not only totaly kill C-level bonuses but quite a few of there cushy jobs and reputations leading to a "poor life in the wilderness of Walmarts returns dept".

One the maxim "all news is publicity which is good" lets see if we can cover this with an aditional point,

Thus it's ementy possible some bright spark in Sony notices that if the movie gets pulled due to terorist threat etc, a good chunk is claimable on their insurance...

OK that plugs the bonus hole in the finances, but how to make that work... well talk about how it must be NK that's thrown the toys out the pram. The problem is how to make it work without being totaly obvious and thus not get the insurance pay out.

It's probably not lost on the Sony C-execs that the US admin are pro parts of the film that the execs back in Japan are having fits of the vapours about and have said should be cut. These bits are not just anti NK premier but also from what has been said quite distasteful, and most people don't want to see turkey guts spoiling their festivities.

Well... the C-levels have sufficient circumstantial evidence to make it look like the US Gov is pulling the directors strings to make the film not "free speach" but out and out propaganda, something the US Gov is not supposed to get caught doing, that's going to be embarrassing for the US Administration not something they need immediately after that 6000 page "what the CIA did last summer" report...

Knowing this and the fact that the Sony Execs know quite a few senior US politico's are either on the payrole or extreamly sympathetic then, you have the idea position for a "you scratch my back..." deal.

But it gets better, the US war hawks have been ratteling NKs cage for the past half century, trying to push them into a premptive attack, which NK would claim as "self defence" but the US "war crimes".

It's known that many of the supposed NK Cyber attacks on SK are not supportable, and some suspect SK right wing groups aligned with US views. Something Mandient knows but sits on because it does not fit the "US and it's allies are under attack from RED APT" agender which is currently so profitable for it and the current US Gov foreign policy.

As an aside it's a now a wildly held belief/joke in parts of the industry that Mandints investigations are carred out through "red spectacles, no tint about it", and some of the regular blog readers here have called them out over their "China APT" claims. Thus perhaps unsuprisingly some would say that Mandient would be an ideal pick to push an "NK is to blaim"

agenda (despite the evidence probs).

I could add that such a "NK is to blaim" attitude suits US Gov policy and that "Anonymous" who many suspect are now "owned by the FBI" have anounced an unspecified retaliation and low and behold some such has just happened... Although supportable facts in their own right, there is not any publicaly available evidence to link these facts together...

---

**Mr E • December 23, 2014 6:00 AM**

*IF* it wasn't north korea - Wouldn't it be farcical and tragic if the real perpetrators escape justice because political posturing caused the FBI and US govt to paint themselves into a corner in insisting NK was to blame?

---

**vas pup • December 23, 2014 8:27 AM**

@Martin Merck • December 22, 2014 6:47 PM: “This was an attack on Sony, not the US govt. But you know how things go. Govt is to stay out of business, unless business wants them in it.” In this case I agree with you absolutely, but taking into consideration that not all businesses created equal (importance for the life and functionality of the whole country - e.g. Sony versus Boeing, McDonald's versus major electricity generators/providers, etc.- I hope my point taken). In US almost all elements of critical infrastructure are private, i.e. businesses. When critical infrastructure is targeted, that is gov concern for sure regardless of as you stated 'unless business wants them in it'. But, even in those cases, gov should help business, not be 'primary care' agent. Gov regulation for cyber security (minimum standard/measures) should be mandatory for businesses involved in critical infrastructure. For me it similar to gov regulation on financial/banking sector after latest crisis even causes of that crisis were pure insider job (see documentary with the same title "Insider Job") not terrorism.

---

**Sancho_P • December 23, 2014 9:36 AM**

@ Nick P

> *“... and give North Koreans *more* Internet. Let people see the outside world, the truth.”*

Hillarious.
Yes, let’s show them the western democracy, the leading nation, America.
I bet they’d cut their Internet themselves.

@ Thoth

Sorry but what needs to be done isn’t in the technical domain but in benevolence.
I agree dearly with “analyze and learn the lessons”, but technically it’s an arms race no one can win but all will lose.
Technics can only solve technical problems.
Real life means goodness and solidarity, values robots won’t never have.

@ Christopher

A motive doesn’t make a murder.
BTW which motives did you compare to find the strongest? What do you know?

@ Clive Robinson

Your story is so unbelievable and schizophrenic that I take it for true, granted.
Thank you, we can close the books now.

---

**Sancho_P** • **December 23, 2014 9:40 AM**

ah, sorry, "...robots won't _ever have"

---

**Henry** • **December 23, 2014 10:50 AM**

@ liberal said, "A most conservative liberal • December 23, 2014 12:08 AM Bruce, you are a pacifist. If the NOK invaded your electronic life, you'd feel differently."

Bruce is the one to ask because I doubt he has much privacy. HSAs look at him as an asset, haxors look at him as a trophy, blog readers scrutinize his every word, etc.

so.. yeah let's blow NK out of the internet map so they can get on with their real lives.

---

**Skeptical** • **December 23, 2014 11:00 AM**

Am I reading the Hollywood Movie Plot thread or the Sony thread? Some of the theories in here belong to the former.

@Clive: *But it gets better, the US war hawks have been ratteling NKs cage for the past half century, trying to push them into a premptive attack, which NK would claim as "self defence" but the US "war crimes".*

Note that if the US wanted war with North Korea, they would have found ample cause in dozens of incidents over the last few decades, which include the sinking of South Korean naval vessels, artillery bombardments, and multiple kidnappings. So the idea that - after all those things - the US decided finally to resort to a hack on Sony as a means of igniting a war is ludicrous.

For obvious reasons, the US does not want a war with North Korea. If you have evidence to the contrary, please explain it.

Regarding the US State Department:

The stolen emails make clear that Sony contacted the State Department *after* North Korea

made threats concerning the film. Quite obviously the State Department played no role in the creation of the movie.

Bottom line:

The bottom line is that there is no reason for the US to deliberately point to North Korea unless the US were completely convinced that North Korea is in fact guilty.

The repeated references I see to Iraq WMDs are a bit silly. The stakes here are not remotely similar (no one is contemplating an invasion of North Korea), and there is no desire to find North Korea to be the culprit (it's actually very inconvenient for the US). Few of the factors that drove the mistaken finding regarding Iraqi WMDs in 2003 are present here. Argument by analogy to that mistake is weak.

A rational weighting of the evidence, including US claims, tilts the scales towards North Korea. If you want to believe in some incredibly complicated plot whereby a disgruntled insider plants sufficient evidence to mislead the FBI, NSA, and the various other agencies and private consultants that would have assisted, and gets away with it, go for it. If you want to think that those agencies would not have crawled over every inch of any disgruntled insiders or former employees before ruling them out, go for it. And be sure to leave some cookies out for Santa. :)

---

**dalgoda** • **December 23, 2014 2:00 PM**

As far as cashflow goes...pulling the movie was the smartest thing Sony could do. Just think that through for a minute.

This film is NOT a work of art. This is NOT Citizen Kane we are talking about here.

This film is probably a stinker, truth be told.

Sony has now created SOOOOO much buzz about this film, whether it is good or not, it will be a bonafide hit and people will go see it just out of some kind of Patriotism or something.

And the fact that it will be released to only a few theaters to begin with.....

Well..just something to ponder.

---

**Mr E** • **December 23, 2014 2:40 PM**

Now about that torture report.....

---

**Sancho_P** • **December 23, 2014 4:04 PM**

@ Skeptical

Again you try to weasel around the points:

1) It's **not** about the timing.
When they learned about the movie and the NK complaints,
what did the State Department say:

a) "Go ahead, let him explode and burn in supercolor, we appreciate that"
or
b) "Stop it, you can't do that, that's not funny, forget it" ?

2) Regarding "Bottom line:"
The silly references are not regarding invasion but to fabricated "evidence" from professional liars, deniars and not-commenters.

*"Sorry, but we, the superiors, do not explain us to the plebs"* is their only comment,
e.g. see:

> *"We aren't going to discuss, you know, publicly operational details about the possible response options," adding that "as we implement our responses, some will be seen, some may not be seen."*
> (Marie Harf, cited by the NYT )

Those are the authorities **expecting trust and respect.** ¡Felicidades!

3) [cough] *"rational weighting of the evidence"* - which "evidence" are you talking about?
We do not even have their fabricated / *"mistaken"* (???) evidence as from Iraq.
Evidence would be provable fact, not hearsay.
I'm afraid there won't be any such cookie from Santa! (BTW Los Reyes Magos here)

Only @Clive Robinson gave us a plausible narrative, that's all we have.

@ Mr E
Seconded.

---

**Daniel • December 23, 2014 4:09 PM**

You're making the same error that multiple security experts have been making on this crisis- assuming that plausibility and possibility are one and the same thing. The experts that are skeptical are exclusively IT experts. Where are the North Korea experts who are skeptical? That exposes the flaw in your thinking. After the attacks, North Korea released a statement of support for the attacks. Yet while your article fails to mention this, you state that the US government statement isn't credible. This says something about the limits of your expertise. Please read the North Korean statement of support for the attack and read the work of BR Myers for some background information on North Korea.

---

**Steve • December 23, 2014 4:33 PM**

steven (no relation) makes a good point: "Maybe what the US needs is a "Great Firewall" for

the nation, built by the most competent agencies and trusted commercial partners, to protect against all manner of nasty things infiltrating its Internets from the outside."

This is probably the most dangerous notion to emerge from this whole mishegas. It gives our digital overlords one more excuse to pry and poke into anything and everything, all on the premise of "keeping us safe."

BTW, I have it on good authority from an acquaintance who works in Hollywood that the film is "the biggest turkey since the first Thanksgiving." At first, he was suspicious that Sony might've hacked themselves for the publicity.

---

**Steve** • **December 23, 2014 4:37 PM**

@Daniel: Just because all the "experts" are pointed in one direction doesn't mean that they're right. There are hundreds of thousands of dead Iraqis who can attest to the falsity of that line of thinking.

---

**JestInCase** • **December 23, 2014 4:58 PM**

@ Clive Robinson
I like the way your mind works. ‘Follow the money’ is always a good starting place. Just for the record, I don’t believe that the NK government is behind the Sony attack. The most telling objection, for me, is that NK reminds me of the schoolyard bully; always blustering, antagonistic, and full of braggadocio. If the NK government were responsible, they would be crowing to the clouds. Instead, they are claiming innocence. There is, however, another group of NK citizens who could very well be involved. Call them NK-NGOs, working from a base on the mainland. Shrug. Perhaps we’ll know someday.

Which leads me to: @Mr E
“*IF* it wasn't north korea - Wouldn't it be farcical and tragic if the real perpetrators escape justice because political posturing caused the FBI and US govt to paint themselves into a corner in insisting NK was to blame?”
If I were to wager on the eventual outcome of this mess, I would bet that what you suggest in your question would be the result.

@Skeptical
Your last paragraph troubles me. You used the word ‘evidence’ in successive sentences. If you have evidence, I would very much like to see it. Writing it here would be sufficient.

All of the supposed evidence that I have read about is circumstantial at best and wishful dreaming at worst. Widely available black hat tools, that can be bought for ~300 USD, which are easy to administer, does not constitute ‘evidence’ in my books. I stand ready to be convinced. Please do so.

---

**C Gomez** • **December 23, 2014 5:08 PM**

So the line of thinking is that if you are skeptical then you are a conspiracy theorist?

That doesn't fly in this case. The evidence presented so far is easy to falsify and routinely falsified in any attack. If the FBI, NSA, or anyone else would like to present more evidence, they may. When a true terrorist plot has been foiled, the US govt falls all over itself to present the evidence because they finally got a small win in exchange for the wasted false positive scans on every passenger who walks into every airport in the US every day.

They would be falling all over themselves to lay it out here.

As Schneier pointed out, the timeline suggests the hackers wagged the dog. The various nightly news broadcasts began speculating about The Interview, so they did the equivalent of phoning in a bomb threat.

Most bomb threats (maybe none?) are phoned in. Timothy McVeigh didn't phone anyone.

I do dispute the idea that Sony pulled the movie or gave in. I thought that at first, too, but there is ample evidence that the exhibitors decided to listen to their tort lawyers. At some point, if the large chains won't show a movie that is relying on being on as many screens as possible, there's no point. Even this limited release being planned now will still leave open a massive direct-to-video release.

It's not the first time we've been asked to believe that a film of some kind incited violence or threats. It seems like those in the Administration (the political hacks who advise the President) are desperate to look like they are on top of things... "on the case" as it were. And you know... it's okay to tell the truth and say "we don't know", but the media would tear them apart and tell the people that the Administration is operating without a clue... when in reality governance at that level is all about making moves in a cavernous fog of unknowns.

---

**CJ** • **December 23, 2014 5:38 PM**

This Sony doxing is unimportant to me. However...

I'm amazed at how much coverage this is getting. This is really astonishing considering what an ordinary every day break in this is. The emails and movies are stolen now, so that horse is out of the barn. Yet, the Sony guys (are marketing professionals after all and) are able to keep the publicity machine flowing at full throttle with after burners.

---

**Wesley Parish** • **December 23, 2014 5:52 PM**

Good grief, @Skeptical! Good grief. I'm sure that no one's argued that the US _wants_ war with North Korea. On the other hand - or "foot" do it please ya - everybody believes that the US wants to intimidate North Korea. And likewise, since the PRC is the last remaining official sponsor of the North Korean govt, intimidating the North Koreans is intended to warn the PRC to keep its head pulled in.

It would not surprise me to learn after a few years, that this was part of the US "pivot" to the Asia-Pacific region that went disasterously wrong. With all the faffing about confusing the issue, intended to present the US govt as a pack of bunglers who couldn't possibly have set into motion such a disaster, with Sony set to take the rap, because, face it, they play Keystone Kops so well.

---

**Sancho_P** • **December 23, 2014 6:28 PM**

@ Steve

Sorry, I did not understand whether you meant “good point” sarcastic or not.
Regarding the “U.S. firewall”:
Yes, the U.S. could ask other totalitarian states to help them building that firewall.
That is similar to the sentiment that it’s fine to spy on foreigners but not on Americans, because Americans are always the good ones, and foreigners are the enemy.
Simply put: White man shoots, red / black / yellow man is dead.

Isn’t there the slightest possibility that the enemy is already two blocks away from your home?
OMG, probably working inside your company?

White, **tie**, **no beard**, American citizen? (named “Dick”?)

They do not need any more excuse, look at Bruce’ mugshot (no tie, beard) and you know why they have to dig deeper and deeper (sorry, Bruce, couldn’t resist ;-).

---

**Sancho_P** • **December 23, 2014 6:33 PM**

@ CJ

The incident is interesting for several aspects:
- Business (Sony got it right for publicity but that may not save their ass)
- American government reacting at all and unprofessional
- American open aggression (sorry to say, just a feeling from outside)
- The cover for the true disaster (torture report + **not reaction**, CIA hacking incident)
- The real danger from hacks / insider attacks for both business and society
- The need for secure communication from sender to recipient w/o prying eyes

to name the first that come to my mind.
I guess it won’t go away soon.

---

**Dirk Praet** • **December 23, 2014 7:03 PM**

@ Skeptical

*The bottom line is that there is no reason for the US to deliberately point to North Korea unless the US were completely convinced that North Korea is in fact guilty.*

If the USG is so completely convinced the DPRK is behind the Sony attack, the UN is the right place to present the evidence. From where I'm sitting, I still haven't seen any smoking gun, just circumstantial evidence primarily based on similarities with past operations like the Dark Seoul incidents against South Korea. And statements like "We haven't seen the skeptics produce any evidence that it wasn't North Korea" from folks like CrowdStrike's Dmitri Alperovitch are really beautiful examples of seriously twisted logic.

---

**Hubert** • **December 23, 2014 7:12 PM**

@Clive Robinson writes, "But it gets better, the US war hawks have been ratteling NKs cage for the past half century, trying to push them into a premptive attack, which NK would claim as "self defence" but the US "war crimes"."

In order to bring war back to Korean peninsula, both US and China must concur. So far the two doesn't tango.

@Skeptical writes,s "Note that if the US wanted war with North Korea, they would have found ample cause in dozens of incidents over the last few decades, which include the sinking of South Korean naval vessels, artillery bombardments, and multiple kidnappings. "

Not in the terms of conventional warfare, cyber warfare is what Pres. Obama implied. Logically, US must flex its cybercomm muscle periodically, so as to put the folks to work. Otherwise, good people may get bored and leave.

"If you want to think that those agencies would not have crawled over every inch of any disgruntled insiders or former employees before ruling them out, go for it. And be sure to leave some cookies out for Santa. :)"

Oh you're too kind. That guy in van would appreciate it. Make sure you turn the light on, it's a dangerous track down the snow covered slippery slope.(or not)

@dalgoda writes, "Sony has now created SOOOOO much buzz about this film, whether it is good or not, it will be a bonafide hit and people will go see it just out of some kind of Patriotism or something."

Creating a buzz for a bad film may not be the best idea. Once people realize they were duped, you must create a bigger buzz for them to show up for your next bottom line buster.

@Mr E writes, "Now about that torture report....."

sorry that's boring... and repulsive.

@JestInCase writes, "All of the supposed evidence that I have read about is circumstantial at best and wishful dreaming at worst. Widely available black hat tools, that can be bought for ~300 USD, which are easy to administer, does not constitute 'evidence' in my books. I stand

ready to be convinced. Please do so."

The patriotic side of me wants to believe in our president, blame NK, send drones in, and smartbomb the hackers over there.... but the truth is I seriously doubt NK's cyber capabilities were developed for this type of childish purpose of hackathon. You know the hack, the twits, the pastebins, the tauntings, this is more like anti-sec behavior.

the NK top brass are smart in the sense that they are the last standing true communistic dictatorship, after so many have fallen. that much I give them credit for with due respect. NK's, despite how crazy they appear in movies, know that as a highly sanctioned nation, whose technology were largely supplied by the chinese which probably includes cyber capabilities, know that they must exfiltrate knowledge and technology from the free world by unconventional means, hacking is one of those means of survivalship. wasting that capability on a movie, most people werent planning to watch, is not a logical behavior from NK. they'd much prefer exfiltrating terabytes of data, quietly, from our top pharma or military tech corps.

---

**Nick P** • **December 23, 2014 8:03 PM**

@ Daniel

" The experts that are skeptical are exclusively IT experts."

Not at all. The blog has all kinds of readers. Clive and I have studies INFOSEC and espionage plus been operators ourselves in various ways. A number of people blogging on the issue have experience with or studied hacking, the underground, and Anonymous type attacks. There's others that have dealt with company breaches. Quite a diverse crowd and more meaningful than the phrase "IT experts."

Now, what about the other side? The other side is the FBI and the White House. The White House has been pushing a cyberwar threat with control of Internet, cyberwarriors, mass surveillance, and so on as the supposed solution. This is utter nonsense not supported by evidence and yet they push it. The FBI is an organization that's so good at attribution that they've gone after printers for copyright infringement based on IP. They push a similar agenda as the White House and work with the NSA doing messed up stuff.

So, all we have is their word and whatever evidence in the public domain. They've lied and even screwed up things related to cyber war so much they can't be trusted by default. We need proof. So, we look at the evidence and we find stuff leading us in another direction. We go by that evidence-based theory until we get and review FBI's evidence it was North Korea. (Or someone more trustworthy does.) I'd do that whether knowing IT or not. They *might* have it and are certainly capable of producing it. They certainly haven't provided any, though.

We must be careful to avoid a digital version of Iraq. As one commenter said, NK has serious military and hacking capabilities. Whatever U.S. government does to them might have serious consequences for someone here. I'd like more assurance than a group of known liars saying take our word for it.

**Clive Robinson • December 23, 2014 8:09 PM**

@ Wesle Parish,

Technicaly the Korean war of the 1950's never ended, a temporary truce started and is technicaly still in place.

One of the problems that resulted from this is a bunch of islands that wouldr technicaly be in NK teritorial waters are claimed by SK. The previous SK premier was a bit of a nutter and towards the end was acting as though he wanted to attack NK. The US were involved in "war games" involving the disputed territory and acted in a way contrary to the original cease fire. The result was the NKs shot back with a number of artillery shells that remaind within what would bet their teritorial water. It is known that again contrary to the original terms of the cease fire agrement that SK/US vessels have regularly made incursions in NK teritorial waters. To most that have looked at it outside of the direct sphere of US influance the US and SK have in effect been the agressors trying to provoke a response from NK that could be claimed as a breach of the original cease fire agreement.

The history behind the Korean war is a bit complex, in effect it was started as a super power "proxie war" between Russia and the US. However the Russians decided not to get bogged down with it and droped it into the lap of the Chinese. China like Russia wanted a protective space between them and the US and thus Korea, Vietnam and Tibet have been regarded by China as "buffer nations" in the same way that Russia used many eastern european nations. The US only regards one country as a direct buffer nation (Canada) and regards the atlantic and pacific as their "ponds" thus you have the likes of the NATO countries acting as remote "buffer nations" that are to be used in effect as "forward staging points" for rapid reaction.

China has wanted to be shot of the NK issue for quite a few years now, which is why it's interesting that Vlad Putin is all of a sudden courting the NK leader.

The primary reason appears to be to run a gas pipeline down to SK. However if that happens there will need to be greater unity between NK and SK. Most SKs see the advantage of reunification as the North has the manpower and resources the South does not have abd the South has the finances and technology the North does not.

Also from an SK perspective China's recent agression in what it regards as it's "pond" means that SK is dangerously reliant on China's good graces. If the NK-SK boarder is opened up and a path opened to Russia, then this gives SK a land bridge out of China's influance, it would also act favourably for both SK and Russia.

From China's point of view Korean reunification would be problematical for it's home technology development. In effect a reunified Korea would have a manufacturing capability greater than Japan and Taiwan combined, also SK is technologicaly and research wise on par with Europe and America and thus some way ahead of China. However as a number of "technology stealing nations" have found --Israel in particular-- SK treats industrial espionage of any form as seriously as Super Powers treat "high treason" and have been known to lock

"agents" up for a lengthy period of time even when they are foreign nationals.

US corporates are also quite scared of what would happen if Korea reunified, and have been pushing via secret trade treaties to nullify any any potential benifit a reunified Korea would have.

It is there for more than likely that the US regards Korean reunification as a serious National Security issue, and thus would regards any "rocking of the reunification boat" as a highly desirable objective.

However it's not just US corporates that are running wary / scared of NK and any potential reunification with the south. Do you remember the cold war CIA "weapons gap" issue when senior US politicos and military were told that Russia had ten times the soldiers five times the tanks three times the nuclear delivery systems etc?

Well the same may be happening with NK, we know they have rocket technology capable of putting sizeable payloads into space, and it is believed thay now have uranium based nuclear weapons capability. What is not realy talked about is that nobody has anything aproaching a "missile shield" system for nukes launched from a space platform where the reliable warning time would be less than an anti missile missile system could be deployed in. Thus realisticaly you would have to have an anti satellite system, which is extreamly problematic technicaly let alone politicaly. Put simply, to disable a satellite effectivly you have to disrupt it using very high energy kinetic weapons, the result would be "space debris" the majority of which is unlikely to "drop to earth and burn up" before getting into the orbits of other satellites. The amount of "space debris" already up there causes more than a few headaches for those launching new satellites as they need debris clear launch windows that are currently getting smaller and making launches exponentialy more risky (there are now a number of international meets / conferences specificaly about how to deal with space debris with the more interesting suggestions being qube-sat related).

It will thus be very interesting to see how the US-NK issue plays out, currently the US is not realy doing themselves any favours. And whilst China may not be standing up for NK in the UN security council, it may be very likely that Russia will start doing so, if it feels that it needs to gift "good faith" NKs way to get the gas pipe line and the "land bridge" to SK. Russia might also do it to rub the US up the wrong way, as it already has done over Syria.

@ ALL,

Remember when talking about NK internet, you need to remember that there is the official State network which has significantly restricted access for all but a privileged few, and those getting connectivity from other countries via mobile phone etc connectivity. Whilst we know the latter happens we don't know to what extent, or what sort of restrictions the get from these networks. We do know that there have been what look like crude attempts to jam the signals at times. But it has also been suggested that this over the border connectivity is how some "cyber attacks" have been carried out on SK...

**Nick P • December 23, 2014 8:09 PM**

EDIT: Wait, that was RIAA that sued a printer. FBI's failures were often in connecting the dots or thinking IP ranges meant the attackers were physically there. They've gotten better over time but amateur mistakes don't improve trust.

---

**Clive Robinson • December 23, 2014 8:37 PM**

@ Hubert,

> In order to bring war back to Korean peninsula, both US and China must concur.
> So far the two doesn't tango.

Err no not realy, it just takes NK or SK to cross over the agreed demarc with forces under flag, or any other nation to send in forces under flag to either NK or SK teritory without permission then by defacto a state of war exists (as well as a war crime).

It's just like me entering your home without your permission, if I don't break in or carry the tools to do so then it's at the very least tresspass which you can persue me through the civil courts for damages etc. Hovever if I have broken in or carry the tools to do so then I have committed a criminal act and arrested by the police and sent to trial in the criminal courts.

---

**Daniel (the normal one) • December 23, 2014 10:11 PM**

@Nick P

That was some other Daniel and not the person who normally posts as Daniel. I agree with you 100% about not making the mistake of a Cyber Iraq.

---

**Skeptical • December 23, 2014 10:42 PM**

@Dirk: *If the USG is so completely convinced the DPRK is behind the Sony attack, the UN is the right place to present the evidence. From where I'm sitting, I still haven't seen any smoking gun, just circumstantial evidence primarily based on similarities with past operations like the Dark Seoul incidents against South Korea. And statements like "We haven't seen the skeptics produce any evidence that it wasn't North Korea" from folks like CrowdStrike's Dmitri Alperovitch are really beautiful examples of seriously twisted logic.*

Disagree on the UN. If the US evidence derives from sources or methods that it prefers to keep classified, the UN is obviously a poor forum. Besides, that kind of public forum is exactly what North Korea would want.

Look, here's the thing that almost no one in this thread seems to able to come to terms with:

(1) The US President stated that North Korea is to blame, and that the US will respond in a manner, at a time, and in a place of their choosing.

(2) You do not allow the US President to make such a statement unless you have what you believe to be ironclad proof.

(3) There is no reason for the US to have made gross errors here. They have access to the best experts, and the answer they found (North Korea) is the answer they were least motivated to find. As I said, this is not a preferable result for the US.

So these other commenters can spin their wheels on phantoms of disgruntled employees they know nothing about, and believe that the US allowed its President to promise retaliation without doing full due diligence (or, even more dubiously, that the US is somehow framing North Korea because... ? I frankly have no idea).

But none of that is reality.

In reality, an event like this brings down a huge amount of heat. You have agencies looking at every nook and cranny, and everyone wants to play a part. The NSA probably dusted off SIGINT that a live analyst hadn't looked at in weeks. These men and women are highly motivated, and they will absolutely bring a prey to ground.

That means interviewing disgruntled ex employees with the skill to do something like this, tracing out their movements, their presence, dumping their phones, their computers, their call records, their ISP records, their financial records, and fitting that with what's known about the Sony operation timeline.

That means reviewing all the intelligence on NK's cyber capabilities - and I'd venture that there would be a fair amount, given the attention it has received over the last few years - and tracing out their movements.

It means taking a hard forensic look at what's left behind, and looking for tells that the NKs may not even know exist - indeed, tells that someone else may have put into their tools in advance.

And after all of that is done, and the answer comes up NK, about eight different high-ranking individuals are going to say "are you absolutely sure about this? there are no competitive hypotheses?" And the analysts will need to show the alternatives they considered, they might even need to show a red team exercise if the evidence pointing to NK were not strong enough, and the discussion will continue.

And after all of that, if there is consensus, the President points the finger, and promises retaliation.

Don't misunderstand me: it's possible that this process resulted in a mistake. It's happened before on much more complicated and murky issues. The odds of it happening here are rather slim.

So, we may not see the evidence. But the above is enough to persuade me that the probability that NK is the guilty party is greater than 90%.

---

**Thoth • December 24, 2014 12:26 AM**

@Skeptical
It would be nice if they can release more evidences of trails of Nork involvement. Unaltered edition not to blind the citizens but solid proofs as well.

National issues should be debated and decided by the citizenry instead of allowing a handful of people who decide the lives of so many Americans. The people should be the one voting to approve war or not instead of some handful of guys who decide to press the button and expect submission of the population to those handful of top job people.

First off, no substantial and publicly verifiable evidence from US Govt ... no credibility.

I believe many of us here are scientists and domain experts who only trust properly published proof instead of just following the crowds. Hard proofs and data points are needed. Things like Sony's server logs, ISP logs and such being redacted by a bunch of public experts and put into public domain is the only way for truth to be known.

---

**Anony Mouse • December 24, 2014 1:07 AM**

Bureau 121's internet servers went quiet to our cyber scouts because they went to sleep. They got 9 hours of rest because "The Interview" was a cyber tactic by Sony to bring the new script for James Bond 007 into theaters. So if the interview was taken out of theaters and put into the global theater then the script to James Bond is probably the making of Sony's Christmas gift. It's someone's facebook.

---

**pretty in punk • December 24, 2014 1:13 AM**

"You do not allow the US President to make such a statement unless you have what you believe to be ironclad proof."

Monica, is that you?

---

**Thoth • December 24, 2014 2:56 AM**

I wonder what would be the US warhawks reaction if one day the "Axis Countries" of North Korea, Russia, China, Eastern EU, Germany, South America (including Venezuela, Peru, Castro Fidel's and Che's strongholds), Cuba, Middle East, Southeast Asian countries ...etc... which anyone of them were to portray negative intentions towards the US/UK warhawks, would they immediately use "proportionate force" to level them to the ground ?

Just a food for thought.

Such disregard towards the feelings towards the International community on flexing their strength and sabotaging other's development and industries are the hallmarks of these warhawks.

**Mr E • December 24, 2014 3:29 AM**

Western governments don't feel the need to produce evidence for anything before making public pronouncements like this because they act with impunity on the world stage, and in the absence of a functioning critical press can define and push their own narratives to fit their myriad behind the scenes geopolitical agendas.

These vagues threats of 'proportional response' is just the kind of aloof thuggish posturing those who hold the balance of power can use to bully and intimidate other nations. It may be 'soft power' in action but frankly, when there are people in the security community who talk enthusiastically about 'kinetic strikes' in response to scenarios involving attacks on digital infrastructure, attribution of culpability starts to become a matter of life and death, not just debate among bloggers.

@hubert

>>@Mr E writes, "Now about that torture report....."

>sorry that's boring... and repulsive.

Yes, it is repulsive. This is a government that lacks the moral integrity to prosecute itself for torture.

---

**Dirk Praet • December 24, 2014 5:20 AM**

@ Skeptical

*You do not allow the US President to make such a statement unless you have what you believe to be ironclad proof.*

Presidents and their administrations don't lie ? They will actually tell anything as long as it suits their agenda.

- Franklin Roosevelt in 1940: "Your boys are not going to be sent into any foreign wars."
- John F. Kennedy in 1961: "I have previously stated, and I repeat now, that the United States plans no military intervention in Cuba."
- Ronald Reagan in 1986: "We did not, I repeat, did not trade weapons or anything else [to Iran] for hostages, nor will we"
- Bill Clinton: "I did not have sexual relations with that woman".
- A 2008 study by two nonprofit journalism groups shows George Bush made 232 false statements about Iraq and former leader Saddam Hussein's possessing weapons of mass destruction, and 28 false statements about Iraq's links to al Qaeda.

But more to the point in this particular context:

- President James Polk lied to Congress in 1846 claiming Mexico had invaded the United States because he was determined to take the Southwest from Mexico. That lie led to the

Mexican-American War.

- President William McKinley lied to the American public in 1898 when he insisted that Spain had blown up the USS Maine warship in Havana Harbor, Cuba, although he had no evidence. That lie led to the Spanish-American war.

I'm afraid you've got history against you ...

---

**Peter** • **December 24, 2014 6:18 AM**

@ Skeptical *"And after all of that, if there is consensus, the President points the finger, and promises retaliation."*

I agree with Skep for the most part. Although most of the evidence may be classified, they are no doubt documented and presented to our president in a clear, conclusive manner before he could make this decision.

---

**Peter** • **December 24, 2014 6:24 AM**

@ Clive Robinson *"US corporates are also quite scared of what would happen if Korea reunified, and have been pushing via secret trade treaties to nullify any any potential benifit a reunified Korea would have."*

Sorry I don't follow this logic. Why would US be scared of a unified Korea?

---

**BJP** • **December 24, 2014 8:35 AM**

@Skeptical

"But the above is enough to persuade me that the probability that NK is the guilty party is greater than 90%."

Respect for admitting the possibility. My money is on "they're simply incorrect" or "this is a ruse to draw the DPRK out in support of other US interests". Not a conspiracy to pass new laws, not a conspiracy to (unnecessarily further) ostracize the DPRK.

---

**Skeptical** • **December 24, 2014 10:33 AM**

@Dirk: Of course governments sometimes lie. The question is ascertaining when it would be in their interests to lie, and when it would not be. You quote a letter from Kennedy to Khrushchev on the eve of the Bay of Pigs operation. If you read it carefully, it's rather clear that Kennedy is stating that there will be no overt US military invasion of Cuba, but that the US will covertly support Cuban resistance groups - which is precisely what the US was doing. Besides, obviously in such circumstances Kennedy *did* have reason to dissemble.

You quote FDR from a speech during the 1940 presidential campaign. He promised that he would not be sending US troops into a "foreign war" while in the same speech discussing at length the dramatic US arms build-up to defend against possible aggression. Quite clearly FDR did not imply that the US would not fight even if attacked. After December 7th, these were no longer "foreign wars."

Now, I can give real examples of deliberate deception by the government. FDR attempted to use a German submarine attack on a US destroyer which was escorting a British ship - when it was quite clear to him that the Germans could not possibly have known they were firing on an American ship - as a pretext for war, for example, and purposefully adopted naval tactics intended to be provocative to the Germans. There is the infamous Gulf of Tonkin affair.

But in those cases we can discern the interest of the government in lying - or at the very least shading the truth.

There is no such interest applicable here. Instead a mistake about DPRK's responsibility would involve the US in a pointless confrontation which it had no interest or desire in seeking. So you'd want to be very careful before doing so - and you'd want to be especially careful about having the President make a direct statement on the subject.

---

UNKNOWN_TYPE

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

Preview Submit