Schneier on Security

← Manipulating Juries with PowerPoint "Santa Claus and the Surveillance State" →

Did North Korea Really Attack Sony?

I am deeply skeptical of the FBI's announcement on Friday that North Korea was behind last month's Sony hack. The agency's evidence is tenuous, and I have a hard time believing it. But I also have trouble believing that the US government would make the accusation this formally if officials didn't believe it.

Clues in the hackers' attack code seem to point in all directions at once. The FBI points to reused code from previous attacks associated with North Korea, as well as similarities in the networks used to launch the attacks. Korean language in the code also suggests a Korean origin, though not necessarily a North Korean one, since North Koreans use a unique dialect. However you read it, this sort of evidence is circumstantial at best. It's easy to fake, and it's even easier to interpret it incorrectly. In general, it's a situation that rapidly devolves into storytelling, where analysts pick bits and pieces of the "evidence" to suit the narrative they already have worked out in their heads.

In reality, there are several possibilities to consider:

- This is an official North Korean military operation. We know that North Korea has extensive cyberattack capabilities.
- This is the work of independent North Korean nationals. Many politically motivated hacking incidents in the past have not been government-controlled. There's nothing special or sophisticated about this hack that would indicate a government operation. In fact, reusing old attack code is a sign of a more conventional hacker being behind this.
- This is the work of hackers who had no idea that there was a North Korean connection to Sony until they read about it in the media. Sony, after all, is a company that hackers have loved to hate for a decade. The most compelling evidence for this scenario is that the explicit North Korean connection -- threats about the movie *The Interview* -- were only made by the hackers *after* the media picked up on the possible links between the film release and the cyberattack. There is still the very real possibility that the hackers are in it just for the lulz, and that this international geopolitical angle simply makes the whole thing funnier.
- It could have been an insider -- Sony's Snowden -- who orchestrated the breach. I doubt this theory, because an insider wouldn't need all the hacker tools that were used. I've also seen speculation that the culprit was a disgruntled ex-employee. It's possible, but that employee or ex-employee would have also had to possess the requisite hacking skills, which seems unlikely.

- The initial attack was not a North Korean government operation, but was co-opted by the government. There's no reason to believe that the hackers who initially stole the information from Sony are the same ones who threatened the company over the movie. Maybe there are several attackers working independently. Maybe the independent North Korean hackers turned their work over to the government when the job got too big to handle. Maybe the North Koreans hacked the hackers.

I'm sure there are other possibilities that I haven't thought of, and it wouldn't surprise me if what's really going on isn't even on my list. North Korea's offer to help with the investigation doesn't clear matters up at all.

Tellingly, the FBI's press release says that the bureau's conclusion is only based "in part" on these clues. This leaves open the possibility that the government has classified evidence that North Korea is behind the attack. The NSA has been trying to eavesdrop on North Korea's government communications since the Korean War, and it's reasonable to assume that its analysts are in pretty deep. The agency might have intelligence on the planning process for the hack. It might, say, have phone calls discussing the project, weekly PowerPoint status reports, or even Kim Jong Un's sign-off on the plan.

On the other hand, maybe not. I could have written the same thing about Iraq's weapons of mass destruction program in the run-up to the 2003 invasion of that country, and we all know how wrong the government was about that.

Allan Friedman, a research scientist at George Washington University's Cyber Security Policy Research Institute, told me that, from a diplomatic perspective, it's a smart strategy for the US to be overconfident in assigning blame for the cyberattacks. Beyond the politics of this particular attack, the long-term US interest is to discourage other nations from engaging in similar behavior. If the North Korean government continues denying its involvement, no matter what the truth is, and the real attackers have gone underground, then the US decision to claim omnipotent powers of attribution serves as a warning to others that they will get caught if they try something like this.

Sony also has a vested interest in the hack being the work of North Korea. The company is going to be on the receiving end of a dozen or more lawsuits -- from employees, ex-employees, investors, partners, and so on. Harvard Law professor Jonathan Zittrain opined that having this attack characterized as an act of terrorism or war, or the work of a foreign power, might earn the company some degree of immunity from these lawsuits.

I worry that this case echoes the "we have evidence -- trust us" story that the Bush administration told in the run-up to the Iraq invasion. Identifying the origin of a cyberattack is very difficult, and when it *is* possible, the process of attributing responsibility can take months. While I am confident that there will be no US military retribution because of this, I think the best response is to calm down and be skeptical of tidy explanations until more is known.

This essay originally appeared on *The Atlantic*.

Lots more doubters. And Ed Felten has also written about the Sony breach.

EDITED TO ADD (12/24): Nicholas Weaver analyzes how the NSA could determine if North Korea was behind the Sony hack. And Jack Goldsmith discusses the US government's legal and policy confusion surrounding the attack.

EDITED TO ADD: Slashdot thread. Hacker News thread.

EDITED TO ADD (1/14): Interesting article by DEFCON's director of security operations.

Tags: FBI, hacking, intelligence, national security policy, North Korea, overreactions, rootkits, Sony

Posted on December 24, 2014 at 6:27 AM • 119 Comments

Comments

usgov • December 24, 2014 6:56 AM

Just think of who wins from this whole scenario?

It's simply the US and all of its funded 3-letter organisations. So the most plausible explanation is (just like 11th september) this is from the US itself to test and fund more cyberweapons.

Some guy • December 24, 2014 7:28 AM

Or was it all a hoax?

http://www.bostonglobe.com/opinion/2014/12/22/sony-hack-attack-stunt/PN9UiT2eHTJO669N37NqxJ/story.html

---

mb • December 24, 2014 7:39 AM

Hackers have been inside Sony for years. The crime scene is as corrupt as their executives. They've been negligent and now they've been turned into a pawn. This is typically where a 3-letter-agency steps in. They've got plausible deniability to serve whatever purpose they want. We'll never know the truth.

Daniel • December 24, 2014 8:01 AM

I agree there should be some skepticism, but I don't buy the "hackers only stole The Interview/NK spiel after the media started speculating about it". The name the group used from day 1 was "Guardians of Peace", which seems an obvious reference to "guarding international peace by forbidding the release of this film". They also followed up with various statements about preserving world peace by stopping the "terroristic" film.

What motive, either true or false, could someone claim to have for hacking Sony while claiming to protect peace? Hacktivists or a disgruntled employee would likely go a very different route.

The NK link was there from day 1. So, I think it's safe to narrow down the perpetrators to either North Korea pretending to be hacktivists, or hacktivists or some other threat group pretending to be North Korea.

Skeptical • **December 24, 2014 8:09 AM**

Allan Friedman, a research scientist at George Washington University's Cyber Security Policy Research Institute, told me that, from a diplomatic perspective, it's a smart strategy for the US to be overconfident in assigning blame for the cyberattacks. Beyond the politics of this particular attack, the long-term US interest is to discourage other nations from engaging in similar behavior. If the North Korean government continues denying its involvement, no matter what the truth is, and the real attackers have gone underground, then the US decision to claim omnipotent powers of attribution serves as a warning to others that they will get caught if they try something like this.

Let's play this out. Two scenarios: NK Responsible (NK-R); NK Not Responsible (NK-NR)

NK-NR:

US attributes blame to NK. US promises retaliation.

Possible follow-on sequences:

Best case.

Real culprit never identified. US succeeds in persuading others that it identified NK as real culprit.

Result:

Possible deterrent effect on other nations, but only if other nations assume that US capability to detect NK responsibility also applies to them. Without details as to how US identified NK as the culprit - which will not be possible to give - there is no way for other nations to presume that the US capability applies to them. Indeed, overconfidence bias predicts that other nations will tend to assume that the capability does NOT apply to them.

Risks:

(1) Nations with deep knowledge of NK cyber operations, which may well include the PRC, may know definitively that NK is NOT responsible. US attribution therefore may well diminish US cyber capabilities in the eyes of such nations.

(2) Even if no other nation is yet aware of the US bluff, the real culprit now potentially has something very valuable to sell to US adversaries: proof that the US wrongly attributed responsibility and wrongly retaliated.

(3) Finally, the real culprit may already have some connection to other US adversaries. Perhaps the real culprit is a Russian group contracted to undertake the operation, for example. This hands those adversaries damaging information to use against the US.

So, that's the best case.

What about the negative case, a state to which some of the risks just described exposes the US?

In the negative case, the real culprit (not NK) is identified. The US exposed as identifying the wrong culprit, and moreover undertaking - or promising to undertake - retaliation against an innocent actor.

Result: Damage to US credibility along several dimensions. Loss of deterrence power.

Conclusion:

Even the best case provides the US with very weak and uncertain benefits, while running the real risks that the PRC or other nations will be able to see through the bluff, that the bluff will be exposed, (not mentioned above) that retaliation against NK may result in an escalation of conflict.

Note that there is no reason to assume that the best case has better odds than the negative case under the NK-NR scenario.

Nor is there any reason for the US to rush to judgment and assume the risks of the NK-NR scenario. Maintaining favorable foreign perception of US detection capabilities does not depend on the US making a public attribution of responsibility mere weeks after a formal investigation was begun.

Therefore Friedman is incorrect - it would be highly foolish for the US to have attributed responsibility, and promised retaliation, if the US is uncertain. If the US is uncertain, it should simply note that it does not wish to comment on any ongoing investigations or operations, but it is highly confident that the perpetrator will be held accountable, whether publicly or covertly. This runs no risk of any weakness in US detection capability being exposed, and enhances uncertainty as to the extent of that capability - thereby preserving a deterrence effect. It also preserves the opportunity for the US to expose the real culprit if ever identified and to take retaliatory action if merited.

NK-R Scenario:

If the US *is* certain, then although the rapid attribution of responsibility to NK may have uncertain effects on other nations (for reasons already given), it would indicate to North Korea quite definitively that their attempts will be detected, attributed, and will draw retaliation.

This is of significant benefit to the US and its allies in East Asia, as North Korea has reportedly begun to heavily rely on cyber-capabilities as a means of leverage to be used against its

perceived adversaries.

Overall Conclusion:

I do think it's healthy to maintain some skepticism when officials make claims but indicate that the evidence justifying their claims is classified. It makes a direct analysis of the strength of those claims more difficult. But we should be wary of drawing analogies to very different sets of circumstances (Iraq WMD). Better analogies might be to detection of PRC cyber-espionage efforts, or detection of foreign bribery and commercial espionage. But such analogies aren't very helpful here.

I think instead we need to look at US interests as a guide to whether they think they're holding the cards to back their claims. An analysis of those interests, in my own view, suggests they do.

Then we'd need to look at US capabilities as a guide to whether they may be mistaken about the cards they hold. This is a much more difficult assessment to make, but given the actors involved here, it seems safe to rate those capabilities very highly.

Taken together, these considerations lead to the conclusion that the US probably has sufficient evidence to conclude properly that NK is the responsible party.

Michael • **December 24, 2014 8:50 AM**

I don't buy it. If the authorities cannot produce the evidence, they have almost no grounds to accuse North Korea's government. End of. Without that evidence, any act of 'retaliation' against North Korea or its government is little more than vigilantism, retribution without the burden of proof, and would make other malicious hacking justifiable.

Again, where is the evidence?

---

vas pup • **December 24, 2014 8:59 AM**

Bruce pointed in his book that real test of security is pen test, and actually it is very difficult to imitate cyber attack of real scale. Now, I guess concern who did it should be more of politicians, but for IT/security/Sony-gov that is invaluable opportunity to analyse weak links in security and prevent similar attacks in the future. That particular attack could be just a test just of vulnerabilities on the side of attackers to prove that penetration tools used are actually workable and to apply those tools in the future for similar attacks for more important objects than Sony Pic within US. Conclusion: focus for IT is prevention and mitigation versus politicians - retaliation.

Steven • **December 24, 2014 9:00 AM**

@Michael: To be fair, it's very likely they're withholding a fair bit of evidence. If the NSA has some intercepted comms from NK's central committee, or if they otherwise have privileged

access to their government or perhaps even the actor group itself, they obviously do not want to reveal that to the public.

---

anonymous • **December 24, 2014 9:20 AM**

Several people/groups broke into SPE. They had very low hanging fruit.

Michael • **December 24, 2014 9:36 AM**

@Steven - Very likely the NSA has *something*, but it's still as good as having no evidence if the authorities were to act on that. If North Korea's government was the cuprit, it should be held accountable, proven guilty beyond reasonable doubt and damned by the evidence.

@anonymous - That's what I consider the most likely scenario: An insider with a very personal grudge collaborated with an outside hacking group.

Cowbert • **December 24, 2014 9:40 AM**

My own personal hypothesis is that it's the last category (co-opted false flag), since spoofing source is relatively easy to do. I postulate the initial attack was conducted by either:

1. The US IC. This serves 2 purposes. Both as a practical cyberwarfare training/skills development exercise and to be hawkish in general (give an excuse to increase funding/authorizations to attack North Korea further) - remember we are still mired in the whole nuclear weapons issue and perhaps those US agencies are looking for a way to deploy something like Stuxnet or even special operations forces to degrade enrichment processing in DPRK.

2. Another pro-Western Asian country (possibly South Korea or Japan). Again this could be a combination of driving factors:
A. Why it could be South Korea
a. The current President, Park Geun-hye is known to be hawkish. Her father, after all, was infamous for his leadership in the military coup of 1961 and authoritarian presidency from 1963-1979.
b. South Korea has significantly increased its economic ties to China over the past few years, prompting Western analysts to wonder about the stability of its pro-US military alliances. Perhaps the ROK believes that playing up a "common enmity" towards the DPRK that is shared by the US and PRC will increase stability between its two main rival allies. In addition, like the US-led scenario above, this would be a perfect training and development opportunity for ROK cyberwarfare units. Another possibility is that ROK is exploring a defense treaty with China, which would alienate the US. But if they got the US to attack DPRK, it would fulfill one of their longstanding strategic goals now, even if future US support diminished.

B. Why it could be Japan
The current Prime Minister, Shinzo Abe, is known to be hawkish. As a whole, his

administration is eager to loosen traditional constitutional interpretations against militarization (because among other things it would allow them to renegotiate US force levels in Japan). Japan also regards DPRK a strategic and tactical threat due to being in range of DPRK cruise missile capability (which is why Japan owns several Aegis BMD-capable/Arleigh Burke-derived destroyers and an islands-wide network of PAC-3 systems). Attacking a domestic target like Sony would have reduced the difficulty of the attack. Finally, like the US-or-ROK-led scenario above, this would have also been a perfect T&D opportunity for JSDF cyberwarfare units.

Evan • **December 24, 2014 9:50 AM**

Bruce, how long is your memory? You write,

> But I also have trouble believing that the US government would make the accusation this formally if officials didn't believe it.

What about the 2007 National Intelligence Estimates on Iran's capacity and intention to develop nuclear weapons? The preliminary draft that the public saw said the exact opposite of what the final draft said, and concurred with the earlier 2005 estimate. The factual basis of the 2005 NIE, the 2007 draft, and the final 2007 report were substantially the same, so why the opposing conclusions? It's hard not to conclude that at least one document prepared by the intelligence community in the period 2005 to 2007 for advising policymakers contained deliberately false, or at least wittingly unsubstantiated, conclusions about Iran's nuclear arms program. That makes it very difficult for me to trust the veracity of intelligence agency's public statements on these matters, since it's clear they allow themselves to be influenced by political instructions from higher up (whether the White House or agenda-pushing careerists in the Defense Department in unclear).

Frank Ch. Eigler • **December 24, 2014 10:02 AM**

(Plus Bruce's jab at "we all know how wrong the government was about" Iraq WMD's is also overdone, considering recently publicized contemporaneous discoveries of germ warfare stocks there, plus persistent stories about WMD evacuation on the eve of the invasion.)

Avi • **December 24, 2014 10:08 AM**

"no idea that there was a North Korean connection to Sony"

They had to compile their code in Korean before the media said a word, so that theory doesn't work.

AJ • **December 24, 2014 10:13 AM**

"Guardians of Peace" — Could be a group worried that NK might do something drastic to disturb world peace in the event that the movie gets released if it insults Kim Jong-un too badly. They don't have to be from NK to believe that.

ned_flanders • December 24, 2014 10:21 AM

...situation that rapidly devolves into storytelling....

C-Level tyrants and exec sycophants doing what they do to stay in power at Sony.

Sony execs as the 'victims' in some kind of geopolitical incident as a story is complete nonsense. It would make a good movie though.

What we know is the incident did not use special code, Sony's infrastructure was a joke, C-level execs behave as if they are still in high school, Microsoft's enterprise product is still a security mess. No boogeymen needed, unless you are trying to keep your management job at Sony.

Sony is an aggressive member of the copyright cartel with deep connections into Congress and the Executive branch. They are using the elected officials they bought to shift the blame away from them onto some poorly understood enemy of the State.

Spaceman Spiff • December 24, 2014 10:27 AM

Let's stop focusing on NK's involvement in this issue, and on Sony's abysmal network security practices. They have no one to blame but themselves, and they should be held 100% accountable for this debacle!

Anonymous 1 • December 24, 2014 10:39 AM

@Skeptical:

> Taken together, these considerations lead to the conclusion that the US probably has sufficient evidence to conclude properly that NK is the responsible party.

The US has blamed foreign powers for cyberattacks before that then turned out to be done by American teenagers and they've seemed about as confident then as they do now.

@Frank Ch. Eigler:
What WMDs were found were leftovers from before Desert Storm ended his first WMD programme for good, i.e. Saddam wasn't making the new ones the invasion was publicly justified on.

Saddam made the whole thing up to look strong to Iran and didn't expect the US to believe it strongly enough to invade.

Robert Thau • December 24, 2014 10:46 AM

As a counterpoint to the current situation, let's remember what was happening inside the

intelligence agencies which were tasked with assessing Iraqi WMD programs in the run-up to the 2003 invasion. The head of that office reportedly told his underlings "Let's face it, the president wants to go to war and it's our job to give him a reason to do so." (This is quoted from the memoir of ex-CIA agent Lindsay Moran.)

Similar incentives may be at play here, perhaps at lower levels; US Cybercommand has been all dressed up with nowhere to go for something like a decade now. One can easily imagine the guys down the hall, reporting to the same commanders in their dual roles, being under pressure to build the best possible case for some kind of mission. And that higher-ups who aren't in the mix would take that resulting case for more than it's worth.

---

mvario • December 24, 2014 11:13 AM

Remember, the announcement came from the same government that announced with certainty that Iraq had weapons of mass destruction. When an agenda is at stake they are not above lying.

David Keldsen • December 24, 2014 11:57 AM

Enough about WMD in Iraq. There were WMD there, hidden caches were encountered repeatedly in the field during US involvement. Yes, there were ALSO overstatements by the Bush administration, but to say they were never there was to buy in to another form of secrecy and misdirection.

http://www.nytimes.com/interactive/2014/10/14/world/middleeast/us-casualties-of-iraq-chemical-weapons.html

The 'truth' is often both subtle and complicated. And reasoning by analogy is a classic fallacy. Bruce, you know better than that.

---

dse • December 24, 2014 12:16 PM

NK threatened to retaliate if the film was out, but against whom? the first victims (maybe the only ones) would have been SK neighbors. Maybe hacktivists (initially from SK) decided to prevent that from happening (thus GOP name), but after they got the whole stash they found many lulz-worthy material, and meanwhile some individuals in the group remembered the old grudges against Sony.

Anonymous 1 • December 24, 2014 12:55 PM

@David Keldsen:
Except for the fact that they didn't repeatedly encounter them, in fact all they encountered was leftovers from more than a decade ago the first time Iraq agreed to destroy them.

It's a fact that the WMDs the Bush II administration used to justify the invasion were never

there. Had you read the article you linked to you would know that.

Anura • **December 24, 2014 1:09 PM**

I love this article:

http://www.reuters.com/article/2014/12/24/us-northkorea-cybersecurity-google-idUSKBN0K213K20141224

"Google weighed security, free speech in move to stream Sony film"

Google made their decision based on free speech and hackers? Umm... No. These hackers don't pose much of a threat to Google; while Google isn't perfect, they are dealing with attacks from state and private actors all the time and there is no reason to believe these guys are sophisticated enough to attack someone with Google's resources and experience. The hype combined with the fact that they already own the largest streaming video service in the world means that there are a lot of revenues to be made for little cost.

Gayn • **December 24, 2014 1:44 PM**

All of the “similarity arguments” to N. Korea are indeed circumstantial.

I doubt any argument that an independent North Korean group is responsible. How could such a group exist without the knowledge and probably the control of the government?

The FBI's announcement hints at classified information that is conclusive. If so, it comes from the NSA, and we'll never see it. The NSA, according to Snowden, has many more techniques than Weaver mentions. If we've penetrated North Korea, we wouldn't want to tip our hand as to how or where.

Sony may get some legal defense if the hackers were from N. Korea, but they could just as easily lose all their cyber insurance if that insurance has a terrorism disclaimer.

I too am dubious that the attack was due to an insider, but the argument of insider help seems plausible to me. For example, finding the file of passwords among 10's of Terabytes might be hard without inside help.

I don't see how blaming N. Korea deters an independent hacker group #GOP. It should embolden them. The downside of being proven incorrect, would be a credibility hit against the US.

JustReading • **December 24, 2014 1:51 PM**

>>But I also have trouble believing that the US government would make the accusation this formally if officials didn't believe it.

Why so? We already have a precedent: fabricated evidence of WMD in Iraq. There are more...

SR • December 24, 2014 1:53 PM

"I worry that this case echoes the "we have evidence -- trust us" story that the Bush administration told in the run-up to the Iraq invasion."

After 9/11 we identified Osama Bin Laden almost immediately, and remained confident even after he denied it. We had boots on the ground in Afghanistan in early October. It was only much later that neocons started trying to use 9/11 as a basis for war in Iraq. Colin Powell's UN presentation wasn't until February 2003 - 18 months later.

Daniel (the normal one) • December 24, 2014 2:03 PM

I agree with Skeptical that it really isn't in the US interests to bluff in this scenario. I question the geopolitical judgement of anyone who says otherwise. The Obama administration probably does believe that it has solid evidence that NK is behind the attack. The question is what is the burden of proof? They probably don't have proof beyond a reasonable doubt but they probably have a "more likely than not" proof.

To use a poker (Texas Hold-em) analogy: the stakes are too big to raise with king high after the flop. But the stakes are small enough that raising with a pair of aces makes sense. Maybe someone else does have a better hand but with a pair of aces you have to raise, if nothing else to shake out the easy money.

Wankety wank wank • December 24, 2014 2:05 PM

InfoSec Taylor Swift has more.
BREAKING: FBI releases evidence that North Korea has stolen the source code for Linux.

---

jim • December 24, 2014 2:11 PM

I have to say I really don't get why you would think the government would not claim north Korea did this without being convinced it was true. Historically we have a variety of examples of where false claims have knowingly been made - recently on Syria and before it Iraq. If it serves political agendas and they are confident they won't get challenged on it, they will do it. I forget how many times bush stated that Iraq would not allow inspectors into the country - but it was a lot. A bare faced lie clearly in contradiction to public record and not once challenged by the mainstream media.

Andrew • December 24, 2014 2:26 PM

I don't know what the truth is but Obama is not really an awesome liar (remember the yes/no/maybe/its classified answer?). I'd say the speech was pretty honest related to this question.

Waldo • December 24, 2014 2:45 PM

It's a stunt by the Obama admin and the DNC to cast Obama as protecting free speech and not being a dictator which he is. This is another "false flag" people. This is the only thing they have to shape out thinking. It's plain to see. Not very complicated at this point. Anybody feel the need for sopa and cispa?

Bauke Jan Douma • December 24, 2014 2:52 PM

Who is responsible is not the issue. Who is the biggest loudmouth, that is the issue. Drumproll, tensions mounts, Sony after all is a Japanese company, ... USA!!!

Winner again. Oh, guys and gals, with 'USA' I mean the thugs that (think they) are in control in that rogue state, most of them prob. situated in an around Washington D.C.

When o when is that bunch of degenerates going to be reigned in? Is there a heartbeat yet among libertarians and freethinkers in that neck of the woods? Are they doing any thing to get organized besides 'analyzing the situation' till death do us part?

Bruce Schneier • December 24, 2014 3:00 PM

"Or was it all a hoax?"

That seems so remote a possibility that it's not even worth considering. The damage to Sony is so extensive, thinking that it might be self-inflicted makes no sense. If it were a hoax, it would have been executed very differently.

Bruce Schneier • December 24, 2014 3:02 PM

"Several people/groups broke into SPE. They had very low hanging fruit."

That also seems unlikely: too much of a coincidence.

Bruce Schneier • December 24, 2014 3:03 PM

"It's a stunt by the Obama admin and the DNC to cast Obama as protecting free speech and not being a dictator which he is."

That makes no sense at all, and not worth considering.

Bruce Schneier • December 24, 2014 3:06 PM

"Bruce, how long is your memory? You write, "But I also have trouble believing that the US government would make the accusation this formally if officials didn't believe it."

Agreed. That's why I also wrote: "On the other hand, maybe not. I could have written the

same thing about Iraq's weapons of mass destruction program in the run-up to the 2003 invasion of that country, and we all know how wrong the government was about that."

---

steven • **December 24, 2014 3:08 PM**

Whether North Korea had any involvement, they won. Sony Pictures are financially hurt and embarrassed; other corporations likely budgeting for more security out of fear, which often comes with further expense to productivity. The American government has lost much credibility through their accusations. The hackers actually behind it are emboldened from success and others inspired to act similarly against other targets.

In the aftermath was what looked like a 'hacktivist' revenge attack on North Korea's public Internet infrastructure; Arbor Networks reported it as a reflection/amplification DDoS of UDP source ports 123 and 1900. Elsewhere in the world, someone's leased line must have been hijacked to transmit spoofed traffic for that attack, which some corporation is paying for, unaware. Then reflecting off broadband routers, to the cost of those broadband ISPs and maybe affecting many people's home Internet access. Also amplified by unpatched NTP servers, in offices and datacentres, increasing bandwidth costs for their owners and/or suppliers, and perhaps hurting performance or availability of people's business systems for the duration.

Losing Internet connectivity for a day or week, frankly doesn't matter to a society barely using it, and based on self-sufficiency - so who was really hurt most by that?

Simon • **December 24, 2014 3:10 PM**

While it is always good to consider alternative explanations don't you find "This is the work of independent North Korean nationals" a bit far fetched? Independent North Koreans? It would be good news if there were such people.

Waldo • **December 24, 2014 4:15 PM**

Bruce. Just know that Sony has much to gain with sopa and cispa an now they are releasing the movie. I think you need to reconsider this. It is a concerted stunt and as the actors involved continue ton playboys this hoax, it becomes more apparent. Time will tell.

---

jew • **December 24, 2014 7:34 PM**

Another US tale.....
common nk?

Us can torture, can spy on the entire world,
they can produce all kind off weapons, ...

They want to rule the world.

Sony just got what it deserved.

Am not a fan of North Korea, but this one it's a joke

Criminal organization? yes we all know nsa....
nsa have no credibility

Nice Christmas tale....

sry my english

Roland Dobbins • **December 24, 2014 7:43 PM**

Malicious insiders or ex-insiders could've easily found or collaborated with some l33t d00dz; the insiders or ex-insiders themselves needn't necessarily have anything more than run-of-the-mill technical skills.

Soni • **December 24, 2014 8:21 PM**

Maybe the movie was so crap that they had to invent all this mess just to promote it and save the budget.

Gweihir • **December 24, 2014 8:44 PM**

Excellent analysis. I particularly like the part about the US administration having a rather strong motive to lie or claim something they have no compelling evidence about (which is also lying....). The whole thing is just to tidy and neat with the bad guys being unable to credibly defend themselves, Sony having a strong motive for misdirection away from the face that they screwed up to an extreme degree (again), etc.

I still think this is some mediocre hackers like LulzSec stumbling in, taking everything they could get their hands on and then stumbling out again. And possibly they will get away with it even if the NSA could identify them, as the political capital made by the fiction that NC was it is just too valuable for the bad actors perpetrating it. Then again, there is a residual possibilility NC was behind it or that they were planning something like it but did not execute yet.

Nick P • **December 24, 2014 8:47 PM**

@ Bruce Schneier

I also like Nicholas Weaver's theory that the government is leveraging evidence from NSA secret capabilities. It was one of first things I thought. The problem (and reason I didn't post that option) is trust: I'd rather default on they're full of shit for claims based on secrets given all their deceit. I still think they *might* have something. Just waiting on more than that. In retrospect, I should've probably added the NSA option to be more fair to the government's side.

I think they should use third parties that each side trusts for these situations. Perhaps some of the professionals who are in a neutral ground. Even you maybe. They show them how they did it if it's based on capabilities that have already been leaked. Then, the third party tells us if the data is good or even an abstract version of it. People would still be suspicious but that's better than a total black box of a government.

Marko • **December 24, 2014 11:26 PM**

Doesn't anyone else see that this was clearly for the lulz? It's like straight out of /r/pyongyang

---

Wesley Parish • **December 24, 2014 11:40 PM**

@David Keldsen

You might like to recall some of the wording employed, verbal images of mushroom clouds over American cities, the like.

A shell disperising mustard gas doesn't make any more of a mushroom cloud than an HE shell, so the official using that image can't have been "concerned" about Iraq stocking mustard gas shells; nor for that matter can they have been too concerned about "magic mushroom" contamination of their food; perhaps it is a requirement for US Federal officials making unbelievable allegations to ingest magic mushrooms ...?

Wesley Parish • **December 25, 2014 12:05 AM**

@Everyone

With regard to the US govt's absolute standard of truthfullness in relation ot incidents and its high standard of required evidence, we might recall the USS Maine, sunk in Havana Harbour after the Spanish authorities apparently bribed the coal dust in the bunkers to explode ... secular people without regard to the high respect of US govt authorities to miraculous happenings, might doubt that, and believe that the US Navy was full of itself and full of nincompoops who couldn't be trusted to take elementary safety precautions with coal dust, but the True American Patriot(TM) refuses to believe such Doubting Thomases and believes firmly in the supernatural powers of the Spanish authorities ... the True American Patriot(TM) is much loved overseas, because anyone anywhere can sell the True American Patriot(TM) anything anywhere at any price ... I'm hoping to sell our own @Skeptical a Moscow Harbour Bridge, and a simultaneous naval invasion of both Bolivia and Outer Mongolia: I've discovered that some of my very distant Pacifica relatives a few decades (and a century) ago, successfully sold to palagi more of Samoa than actually existed, and I'm keen to pass that record ...

---

general read • **December 25, 2014 12:48 AM**

routine discuss framework: motive, method and opportunity

0.) are the methods really unique or is there plenty of open source to look at?

2.) so, maybe methods are not quite important in the age of the internet. next to opportunity

4.) much of the value is in intangibles. there is suspicion of the steel transaction on the phone - so the
'steel' heavy metal does not deliver it and it is hard to hide big steel beams maybe?

5.) and the 3rd could be motive. so
we go to history on this NO HISTORY day of december 25. Oh
happy holiday and JOYOUS CHRISTMAS.

a person (hybrid?),
entity claims to be
god with the big G.
meaning that THE CAUSE of the ROMAN EMPIRE FALLING was not
lead in the water but the pardigm shift of philsophy - religion, the discussions in the temple of a jewish poor man.

PS. allegedly if historical j had no MIT background in crypto, and was the son of a poverty carpenter, yet spent most of his time in the complex arguments on schneier on security in the temple of security. He as others - fellow ATHEISTS and agnostics seek the truth of TRUTH or even 'security.'

Does history show a lot of pretexts, even planning? maybe but perhaps SONY was the South KOREANS hoping to point the finger or
FRAME N. KOrea or subsitute any other theory. Assisted of course by insiders -
what better way in the fasion of MADOFF to 'cover the tracks.'

---

emk • **December 25, 2014 1:51 AM**

What is astonishing is that intelligent people will actually believe anything the US government says regarding an official enemy like North Korea. How much lying does the US government have to do before it loses any credibility with American cyberprofessionals. Apparently that number is asymptotic to infinity. By now the US government should have zero, repeat zero, credibility!

What does North Korea (NK) have to gain from hacking Sony? It may be hard for many American's, but suspend disbelief for a while and assume NK rationality. Would it not be better for NK to have the film released and then use the fact to paint the US as an aggressor? Why hack a private company? The potential for this to backfire and drive support and viewership for the film is immense. The NK are not stupid. It is far more likely that the US govt is piggybacking on this to threaten, attack and harass NK, than that NK did the hack.

Clive Robinson • **December 25, 2014 2:38 AM**

@ Nick P,

Whilst I understand Nicholas Weaver's theory that the government is everaging evidence from NSA secret capabilities, I have my doubts about it's reliability. Partly because it's got a large number of technical flaws, but also it's a "have my cake and eat it argument" when viewed overall.

Simplisticaly the argument is the Internet is like a masive collection of plumbing, if you squirt a lump of data in at one point it has to squirt out at a other point, much like the simple circuit theory about "the sum of the currents..." that is as a first order aproximation the argument assumes that the Internet has no storage capabilities.

We know that at untill fairly recently at a fundemental level the internet is used to "store, copy and forward" that is it has by default "storage" which means the "first order aproximation" is usually incorrect as there is a significant "time" aspect. Further there is the issue of "copy" where data in effect multiplies many many times beyond it's original size, which further complicates the first order aproximation.

Thus any attacker with state level experiance would know this, and further know that for the first order aproximation to be of any use the observer (NSA) must have a reliable "tag" on the data to tell when it has been "time shifted" by storage, or "multiplied" by copying. With "plain text" data "tagging" is possible, with link layer encryption it's not as the cipher text changes at each node, which is one of the reasons that since the British invented Traffic Analysis in WWII military communications has used link layer encryption to stop data being tagged and followed through the communications network.

Thus every state level player has known for well over a year (post Snowden revelations) and realisticaly since the 1960's that the US uses significant traffic analysis. Thus as a state level attacker you would take steps to either hide the traffic in the noise with crypto or in some otherway make the destination of data indeterminate.

The fact this has not been done, suggests this attack was not by a state level actor.

I could go on digging down to much deeper layers and showing how the uncertainty of not having reliable tagging makes any thing more than one or two hops distant so unreliable as to be nothing more than "gut feeling", but it's Xmas Day and I have significant KP duties to perform "to keep them home troops happy".

---

japan watcher 66 • December 25, 2014 2:44 AM

your grade is only 83 and happy holidays. Why??

HOW TO PREDICT THE CAUSES of World WAR III?

1.) the ultimate pretext is hacking, the internet and 'technology.'

2.)"Nukes of Hazard" schlosser book. Korea DID IT. In similar

fashion to the flock of geese on the radar that caused M.A.D.
all missile launch. (M.A.D. == mutual assured destruction)

3.) so, any 'roague agent', accidental Morris worm triggers
'the blame game.' See HISTORY and 1984. Russians are
our friends against the Nazis. our enemies. our friends.
our enemies for now.

4.) So, the cause is bad security >> internet >> cybercrime >>
maybe cyberwar? >> justification >> physical war >>
It's about the 'evil empire of North Korea.'

5.) Or is it Japan and China. starting with Japan leaders -
much easier and an inconvenient truth: hitttler part of democracy,
popular, etc.

6.) Japan. Abe. strong family since this is 'THE CULTURE.'
grand-FATHER was not a WAR CRIMINAL, since he was un-indicted.

7.) is this significant? Position title was Minister of Armaments,
a key important position and in Manchura. Manchuria, part of the
Greater Co-Prosperity Asia Sphere where the bio-warfare experiments
Unit 731 and crimes against humanity.

8.) so, perhaps the US and others just forgot about this or what was
the 'real agreement'?

9.) Japan seems to have good security research and even crypto, so...

10.) thiis is the FLAW of the traditional police technique:
method, motive and opportunity.

11.) method - say Kaspersky analysis of the Stuxnet et al??
Very nice. Russian actually understand assembly and detail.
but, I argue hy hypothesis - almost everyone has similar methods
and even metasploit.

12.) opportunity. awwww. common. this is LA and this is 'hollywood'
numerous USA presidents appear to have dated movie stars starlets/
actors, etc. so, likely not opportunity.

here's proof about Home Depot. while seeking a job, filled out
an application at HOME DEPOT retailer. this was an OLD windows
XP machine, with easily reachable usb ports. LOL. no secret to
just about even the public customer.

14.) motive. there are so many motives and even one person has

shifts in their motivation -----

15.) lot harder to change character. from a theoretic gaming perspective - no references are supplied. your grade is 84, so do the diligent, hard work - thanks -

from a theoretic gaming perspective, the futherance of the stalin-like or man of titaniium or cult of the leader or the 'father of the nation and relgion' - by the way Merry Christmas, december 25. - is key to the character, IMHO. I have no psychology course, so this could be complete bs.

from a theoretic gaming perspective, much better for following fictional scenario

1.) smuggled movies of the interview is truth.
2.) confirmation Afghanistan, other kiillings throughout history with USA involvement of heads of state, etc. - check
3.) plenty of carnage, but cleverly staged so the 'leader seems wounded with catsup saunce.'
4.) rebirth of a 'christ' or g-dlike figure. which shows the power and longevity of the 'caesar-like leader.'

footnotes:
1.) bible - caesar or kaiser or tsar, etc means -near god in the roman empire panetheon
2.) playing dead to reappear alive as in Chinese book 36 strategms
3.) narratives or 'mystery miracles' of religion
4.) the 3rd and 4th book of the 're-surrection' of Sherlock Holmes.

5.) please, I am a christian (for now) it is NOT about relgion, but about thought and Gilead and David vs. Goliath and the war-games of the bible, etc. and 'the search for security.'

Conclusion: let's say the N. Koreans have some smarts above IQ of 124.55. Sure, they are hungry and cold, but that does not affect IQ. Much better to let the movie "THE INTERVIEW" play. later accompained by the usual 'stalin story' of internal purges, etc.

crude threats to stop the showing of a movie ON CHRISTMAS DAY seem ...

counterfactual: switching fields to martial arts
footnote: read Bruce Lee thesis on Jeet Kune Do
the N. Korea martial art of hapkido seems to emphasize breaking stones/bones and kicking hard. this is not a soft

art like Japanese akido or judo.
maybe crude actions work?

argumentation code in haskell is OMIT for brevity. :)

Wael • **December 25, 2014 4:11 AM**

@Clive Robinson, @Nick P,

> **Simplisticaly** the argument is the Internet is like a masive collection of plumbing, if you squirt a lump of data in at one point it has to squirt out at a other point, much like the simple circuit theory about "the sum of the currents..."

Good thing you said "simplistically"! If you squirt in data at one point, it may squirt out at many more points, not just one. And it may not squirt out anywhere sometimes. As for the analogy with circuit theory (the first order approximation,) I don't think it applies for the simple fact that the sum is not zero. If data packets were to represent current in circuits, then one could not apply something like kirchhoff's law to the Internet in general; it may apply in special cases, though...

Wael • **December 25, 2014 4:21 AM**

I like conspiracies like the next guy, but I think this is an insider attack by a disgruntled group -- not a disgruntled individual. It's also possible a competitor is behind it. Governments work at a much larger scale, and usually don't attack "movies", although history records show that filming some movies were used as a disguise for military covert operations...

Deus Ex Machina • **December 25, 2014 5:10 AM**

The broken English looks deliberately bad and doesn’t exhibit any of the classic comprehension mistakes you actually expect to see in “Konglish”. i.e it reads to me like an

English speaker pretending to be bad at writing English. Also person is media savy concerning American social media and corporate culture.

The fact that the code was written on a PC with Korean locale & language actually makes it less likely to be North Korea. Not least because they don’t speak traditional “Korean” in North Korea, they speak their own dialect and traditional Korean is forbidden.

The web message left by “Whois ” was written by someone who speaks (and spells) good English his first language! The Sony message was written by someone who speaks English as a second language. And lastly this sentence - Thanks a lot to God - no North Korean would use that phrase.

It’s clear from the hard-coded paths and passwords in the malware that whoever wrote it had extensive knowledge of Sony’s internal architecture and access to key passwords.

Occam’s razor suggests the simpler explanation of an insider. It also fits with the pure revenge tact that this started out as.

Why was the State Department advising Sony?

Initial emails did not mention anything to do with the move but only after the press mentioned it.

Someone copied the released 200GB of data over 5-6 hours on the night of November 21st. Transfer rate equate usb 2.0 based on timestamp the very night that the very same day that Sony Pictures’ head of corporate communications,executive, publicly resigned from a $600,000 job wiith previous connections with NewsCorp

God’s Apstls relates more to Japanese Anime ‘The Drops of God’ than to the DPRK

Spoofed gmail account–frank1973.david@gmail.com could reference Jerome D. Frank (the second edition of whose seminal work Persuasion and Healing was published in 1973) was a critic of nuclear weapons.

The compile language and timestamps are so damn easy to set manually when you compile the code. Eldos RawDisk driver files are commercially available. Nnew version of the Destover malware that was used in the recent SPE hack, the sample is signed by a legitimate certificate stolen from Sony. The new, signed version of Destover appears to have been compiled in July and was signed on Dec. 5. In all three cases: Shamoon, DarkSeoul and Destover, the groups claiming credit for their destructive impact across entire large networks had no history or real identity of their own

Someone really knew the the network really well or they took a long time learning it.

If this indeed what SPE declared a week ago, so why then the sudden reversal by SPE on the release of the movies against the explicit directions of the hackers knowing that the worst is still to come? Does that make sense?

http://fabiusmaximus.com/2014/12/20/rebuttal-holes-fbi-north-korea-sony-attack-74873/
http://marcrogers.org/2014/12/21/why-i-still-dont-think-its-likely-that-north-korea-hacked-sony/

Virmaline • December 25, 2014 6:47 AM

"But I also have trouble believing that the US government would make the accusation this formally if officials didn't believe it."

-- Disappointing statement, but somewhat clarified in the comments. I can't think of one thing the US government has told us in the past 10+ years that hasn't been complete and utter bs, and I'm trying! US federal govt = bearer of false witness.

"North Korea's offer to help with the investigation doesn't clear matters up at all."

-- Blanket statement which leaves out the most important part: *why not?* N. Korea has asked for a joint, out-in-the-open investigation. If the US refuses, the US becomes suspect #1. It either did the attack itself or is using it as a convenient reason to bear false witness against N. Korea.

NSA could have even orchestrated the entire attack (with or without Sony's cooperation). It could have decided to teach all corporations a lesson: "*This* is what could happen to you if you cross us, irritate us too much (e.g. don't build in back doors, etc.)" That would be an example of an involuntary attack on Sony. NSA could have also elicited Sony's cooperation and might be compensating and/or otherwise rewarding it for playing the "victim" in the scheme, but the former scenario is more likely than the latter considering the amount of damage to Sony.

Clive Robinson • **December 25, 2014 7:44 AM**

@ Wael,

Yes that's the point, the method Nicholas Weaver describes works on the idea that the first order aproximation is valid for following the data from Sony to NK, it's not except on certain kinds of network, of which the internet is not one, hence the results of such a method are suspect to put it mildly (or "not bl**dy believable" to put it enginering vocab ;-)

The only way the "NSA knows it's NK" conclusion could be valid is if the perps never encrypted the data and the NSA had perfect knowledge of the contents of every datagram. The first issue is a "scrpit kiddy" level mistake which a state level adversary would not make unless they are running a False/Red Flag operation, and the second issue requires a level of "perfect omnipitance" that the NSA might desire and pretend for politicaly reasons, but is very unlikely in reality.

Thus I have my doubts about the argument, even before I look into it any further.

For example let's assume you are setting up a false flag operation, you have illicit access to the Sony servers and likewise illicit access to one of the NK servers, both of which is quite likely. You also have legitimate access to one or more servers on the internet.

You set up a stream head in the Sony server, and a stream tail to dev null on a NK server with the stream going via a server "U" you have legitimate physical access to.

From a network only view point there are two network segments the NSA see, the Sony-U and U-NK if they see the same data packets on both networks they might falsely come to the conclusion that your server U has been illicitly used as a "router" by NK to cover their tracks whilst the steal the data.

However you are using your server U not as just a "router" node but a "store-n-forward" node and all the data gets dumped onto detachable hard drives you have legitimately attached to server U. Because you have illegitimate access to the NK server you know that the data you are forwarding to it is actually ending up in that great big bit bucket in the sky not in any other

NK computer.

Thus you have a copy of the exfiltrated Sony data on the drives the NSA cannot see, NK are probably not even aware that you have forwarded the data onto their server and it's just dev nulled and importantly the NSA think that NK have the data...

It's just like "Magic 101 - Audience Misdirection" where you end up with the --data-- card up your sleeve and the intended audience think the selected stooge has it in their pocket.

This sort of misdirection is very easily carried out and thus False/Red Flag missions fairly easily accomplished by even moderatly profficient individuals with a little for thought.

Lulz^10^10^10 • December 25, 2014 9:35 AM

From the experts at No Shit Sherlock Security:

http://www.geopolitica.ru/en/news/security-firm-says-sony-hack-might-have-been-inside-job

Lena! She made fools of more people than Madoff. She made a fool of the President of the United States.

Lena I will marry you and wait for you to get out of prison.

Virmaline • December 25, 2014 11:16 AM

Interesting article re the Sony hack from the director of security operations for DEF CON:

http://www.thedailybeast.com/articles/2014/12/24/no-north-korea-didn-t-hack-sony.html

---

Johnny • December 25, 2014 12:09 PM

This has been the best movie this holiday season. Hopefully, the movie itself is even better, fingers cautiously crossed.

I doubt we'll see the parallel construction until real culprits are arrested or put to justice, be it a nation or individuals.

Our president could have simply given the executive greenlight, but he's so convinced that he went public with the finger pointing. Remember, he is also a politician, and politicians don't like to be associated with losers. That means he saw some really classified evidence.

Nicholas Weaver • December 25, 2014 3:32 PM

The reason why I'd believe the NSA is that the attackers have to be near perfect to evade the dragnet. Its not a case of

> "The only way the "NSA knows it's NK" conclusion could be valid is if the perps

> never encrypted the data and the NSA had perfect knowledge of the contents of every datagram."

but rather the opposite: If the hackers mess up *once* in a way visible to the ?hundreds? of NSA Internet wiretaps, the NSA finds them. This is very much bread-and-butter SIGINT which the systems are designed to do.

Also, as important, the NSA has the personnel for this, or at least one such person. Whoever wrote the "I Hunt Sysadmins" and "Tor Stinks" documents would probably start SIGINT dumpster diving for the Sony hackers if only for the lulz: after all, it would be really cool howto in ?his?her? motivational series.

There are also a couple of analyses here from Brian Krebs and Steve Bellovin.

TheyDoItWithMirror • December 25, 2014 3:45 PM

Fantastic analysis. Agreed, highly doubtful that DPNK or insiders are behind the latest Sony hack based on the information released by the FBI.

Frankly, the press release from the FBI reads as a propaganda operation that was run to quickly satisfy an somewhat plausible notion. Those responsible for the investigation were likely instructed to wrap this up quickly, as the U.S. doesn't want to appear inept to the rest of the world. It was easy to pin the blame on DPNK because they knew evidentiary data to prove their innocence would not be provided. The ask of China for assistance is perfunctory at best given the known state of affairs between China and the U.S. on cyber warfare.

As for the insider theory, it is well-known inside of Sony Pictures that passwords are passed around on spreadsheets. Why? Despite being a technology company, enough of the managers are not tech savvy enough and would rather not be bothered by security controls. They did not have a security awareness program either which is concerning considering they hired a CISO who formerly held leadership positions with Microsoft Trustworthy Computing and the Department of Homeland Security. He left early this past year and formed his own consulting practice. I would opine that given the known politically hazardous environments he previously navigated successfully, his seemingly abrupt departure is a career saving move as his efforts to fix security issues were blocked by politics.

Some people wonder how could so much information be removed. Well it was well-known amongst employees that malware was on their network since at least Feb 2014 and nothing was done to remove it. We know that means, along with no awareness program, they had no decent incident response capabilities, hence the call to Mandiant. So the malware was there, the hackers took their time escalating privileges, bypassing poorly configured controls and taking advantage of the clear absence of a security program.

Overall Sony Pictures is glossy on the outside and tarnished on the inside. Their priorities are not about security but rather how to fix the bleeding Sony Pictures venture. Yes of course Sony Pictures is on its way somewhere and that is not up, otherwise they wouldn't be hemorrhaging

employees.

Weritas • **December 25, 2014 5:03 PM**

Sony may have done it themselves to both forstall an attack from NK and because the film is such a POS they wanted to guarantee an audience of pissed off Americans. I certainly would not put it past them. That movie by the South Park Guys was really offensive about NK leaders and there was no cyber attack then.

Sancho_P • **December 25, 2014 6:15 PM**

For the “evidence”:

It does not matter whether NK or not.

True or not, (in)officially to point at NK was an **epic fail**.

Let’s assume the FBI / CIA had credible insider information regarding NK’s involvement, clearly these sources must remain protected.
So it’s all classified, confidential, top secret - whatever. No speak No, nada.

¿ Would it be a bright idea to cry:

> *“We know it was NK but can’t tell why we know it”*

???

No, absolutely not. But plausible for USG.

For sure it will cost some lives in NK.

The USG already has a respectable history of uncovering their heroes for political “bonus” points.

Sancho_P • **December 25, 2014 6:22 PM**

For the “evidence”:

First it would be very important to discuss the concept of “evidence” in the IT compared to the “law of evidence” used in conventional litigation / court.
It would turn out that there is no such “evidence” when IT is involved,
because our common understanding of the term is incompatible to the use of computers and Internet.

One point is we can neither trust our machines nor our software, let alone an conglomerate of machines, software and “expert” handling (of “evidence”) in complex systems.
Evidence must be provable by an other entity, that’s not the case in the IT, especially with the

Internet. The timeline, completeness and integrity of data can’t be evaluated in retrospect by approved, certified experts or the trier of fact.

But the biggest issue is software in general:

(1) Software is deemed faulty and incomplete per se (law), not generally trusted.

(2) We can evaluate certain known / expected functions of a given software, but we can’t prove that there isn’t any other unknown or unexpected function.

As a consequence, whatever “evidence” would be provided e.g. in “The Sony Hack”, no one could evaluate it, we would have to trust - or not **[1]**.

To use the term “evidence” in context with IT is a bluff.

[1]
Sony was hacked for years. Who could today sort the bytes to individual hacks?

Harry • **December 25, 2014 6:30 PM**

"This is the work of independent North Korean nationals."

Is this a serious suggestion?

What are these "independent North Korean nationals" of which you speak? There aren't many such. Further, they'd have to have computer skills, computer and internet access, and be willing to do something - nay anything - without official sanction. There aren't any such persons within North Korea, and there's no evidence of NK refugees outside of NK who are pro-NK.

Closest case is that the right hand of the NK government didn't know what the left hand was doing, but I wouldn't characterize that as "independent North Korean nationals."

Charles • **December 25, 2014 7:45 PM**

Nicholas Weaver • "The reason why I'd believe the NSA is that the attackers have to be near perfect to evade the dragnet."

The fact that we 'officially' accuse NORK could mean the dragnet has either failed to identify or it is unsure.[1] The dragnet is not useless because it eliminated other possibilities.

[1]-Assuming by dragnet you meant internet surveillance, then our undisputable intel on the attackers must have been provided by methods otherwise.

ASmith • **December 25, 2014 9:42 PM**

Most know that Former Pirate Bay operator Fredrik Neij is currently jailed in Sweden after

being captured in Thailand last month. What many do not know is the direct involvement by Sony and their Maafa legion of Hollywood studios were directly behind locating that man with his young family and seizing their home and bank accounts where he had fled after being sentenced in Sweden for a mere 10 months in a Sweden Jail (health-spa).

This was exposed by the Sony Hackers release of Sony executives emails which outlined the plot, who was involved and how deeply Sony was involved in Fredrik's capture and extradition back to Sweden.

This angered a great many followers of the Pirate Bay torrent site and it is entirely likely the attack on Sony in Japan was the direct result of vengeance against Sony's involvement in the capture, arrest and extradition of Fredrik Neij.

Meanwhile Sony and their Maafa are ginning up a Re-Sopa legislation to slam thru the USA Congress, Senate knowing the Zionist corrupted Obama White House is certainly going to sign that into law if it reaches his desk further stripping USA and Western Internet rights, freedoms and liberty's while increasing website takedowns, censorship and attacks on anonymous networks as well as encryption use in the present and future.

North Korea is largely a convenient Western Patsy to blame what would be ILLEGAL for any Hollywood writer and script to portray of any living Western leader, namely plotting and carrying out their assassination. Such a trashy plot and 4 rotten tomato movie was doomed to fail and I'm pleased that Seth Rogans directorial debut was such a failure along with Sony losing $100 Million in the process. Even the idea for 'The Interview' script shouldn't have gotten out of the bong pipe it was born in.

David • **December 26, 2014 12:08 AM**

I'm amazed at the fact that the average american person is so annoyed at north korea's "propaganda" when they're being fed the same. It's an astonoshing psychological case of study. On the other hand, I'm really glad blogs like this exist. Greetings.

John • **December 26, 2014 12:12 AM**

Hollywood movies are plain BS, is a faithful representation of American culture -as seen in the outside. America is no different from North Korea: full of propaganda. Funny how you can be outraged at another nation's government yet your own is the same. They simply don't see it.

Dirk Praet • **December 26, 2014 6:37 AM**

@ TheyDoItWithMirror

Frankly, the press release from the FBI reads as a propaganda operation that was run to quickly satisfy an somewhat plausible notion.

About a year ago, the FBI released a 16-page report warning that US companies were facing

potentially crippling data destruction malware attacks. It includes details on previous malware attacks on South Korea banking and media companies. Given a number of similarities in the Sony attack, it was obvious they would immediately point the finger at the DPRK.

FBI warned Year Ago of impending Malware Attacks—But Didn't Share Info with Sony - The Intercept

---

Clive Robinson • December 26, 2014 9:23 AM

@ Nicholas Weaver,

> If the hackers mess up once in a way visible to the ?hundreds? of NSA Internet wiretaps, the NSA finds them. This is very much bread-and-butter SIGINT which the systems are designed to do.

Yes but as I've already indicated it proves nothing mearly raises a vague possibility, sigint always requires verification before it even remotely becomes actionable, I would think that most real military --as opposed to political-- commanders are acutely aware of the possability they are seeing misdirection quite deliberatly designed to mislead them.

Thus it's very interesting to note that those who have a pro attitude towards the guilt of NK have several things in common.

The first is the "super natural belief in the NSAs abilities" and the second that what the NSA has passed up the command tree is "golden" and that Pres BO is thus party to some Oh so confidential secret that "he dare not speak it's name"...

Thus science and reason gets thrown out the window to be replaced with what looks to others like "cult mysticism" espoused by kow-towing zelots who insit that everybody "believes" as they do, with out proof just "faith". Hardly a good place to be, let alone start a rational argument from.

Rational behaviour requires testable facts with hypothesiss that are founded on acceptable axioms that can be shown to be consistant with the testability of any relevent hypothesis that is provable within the system in use.

The law relies on a "tribunal of law" (the judge) a tribunal of truth (the jury) and the "burden of truth" (evidence) presented by the opposing parties. There are two acceptable measures used depending on the type of law "balance of probability" and the much stricter "beyond reasonable doubt". Cults and faith based belief don't measure up to these standards by way way more than a country mile.

There is a third commanality with the "NK must have done it" adherants, which is they don't appear to understand what the difference of levels of evidence are, that are required for an "Intelligence suspicion" and a "Diplomatic condemnation" given publicaly. The former requires no evidence, just coincidence, the latter requires evidence sufficient to go to war honestly and thus commit thousands to their deaths such that they should not be needless.

There has been nothing presented in the way of evidence that comes close let alone meets the "balance of probability" test and even when lumped together under the most favorable light it fails to make it as creditable "circumstantial evidence".

The evidence so far presented in the main even fails the "coincidence test" and that which does, is feeble at best, such as "uses a skull", "uses green and red writing", "uses readily available malware"...

The claims that the above coincidences matches other NK attacks is a rather stupid circular argument, the previous attacks also have no "balance of probability" supporting evidence just "espoused hot air" from "the usuall suspects" that might be at best poor supposition the attacks were carried out by NK.

Further all those currently known to have been involved with "looking for evidence" have either a very clear bias or incentive at finding NK guilty, thus have shown "confirmation bias. By ignoring fairly simple and believable "follow the money" arguments which can be made to show why various principle actors would want NK blaimed they fail to be credible. Thus as in a kangaroo court self interested parties are standing as police, judge and juries, and would I suspect also like to be executioner as well to see NK "hung, drawn and quartered".

Further it can also easily be shown why very many others would also have not just motive but oportunity to do what initaly happened to SPE, thus you have to clearly demonstrate either it was not them or that they were provably in collusion with NK, which has clearly not happened with the so called evidence so far presented.

I've also given a simple and quite easily done senario of how another party could have not just carried out the attack but laid down a false evidence trail to NKs door to cover their tracks in a way that would "blind side" the NSA "network taps" argument.

Thus the burden of proof so far is not just totaly insufficient it can easily be shown to have not just been "no evidence at all" but easily faked by others of which there are a large number...

It's time for people to stop the "cult beliefs" and add a little rationality to their lives, if they want to be seen as credible to the rest of the world.

When creating a Diplomatic incident, by accusing another nation you have to present credible evidence to support the accusation, which may necesitate revealing some clasified capabilities. Even Ronnie "Ray Gun" understood this point a third of a century ago.

---

z • **December 26, 2014 9:42 AM**

Whether it was North Korea or not, it only makes sense for the US to blame them.

My guess is that nobody in the government has any clue who did it, but they are smart enough to know when to jump on the situation for a political edge. Blaming North Korea justifies the

NSA and FBI roles in surveillance to the public, sends a warning to other nations (including North Korea) not to try this kind of thing, and makes the government look like the good guys for once. Sony has no problem going along with it because it's less embarrassing to be pwned by a nation-state rather than some bored teenagers, and the media likes it because it's a bigger story.

Skeptical • **December 26, 2014 10:13 AM**

I'm not sure why anyone is assuming that the US must persuade anyone other than itself that North Korea is responsible. They are under no obligation to convince skeptical journalists, security researchers, or skeptics in general as to the veracity of their conclusions. It would be inordinately foolish for the US to reveal sources and methods simply for the sake of persuading anyone else that North Korea is responsible. So if the crucial evidence involves classified information that would reveal sources and methods, particularly about how it is able to attribute responsibility for cyber-operations, I would not expect it to be released.

Outside of that information, all we can do is speculate based upon what is known about the US, North Korea, and the attack. I have to say that I find skepticism that assumes the US must simply be stupid, e.g. the US failed to consider that another actor was simply concealing their identity behind a North Korean mask, or the FBI isn't aware that some malware can be recycled, or similarity in code may not imply identity in authorship, to be completely unpersuasive. Deception is a standard component of military operations, and the notion that the NSA, FBI, or other agencies would fail to consider it is ridiculous, as are the notions that they'd somehow be unaware of the truly obvious caveats regarding similarity in code or tools that I've read by various skeptics.

There remains the possibility that the US is mistaken, and that it thinks it knows something that it really does not. One must weigh that logical possibility against everything we have learned about the resources that the US has poured into cyber-operations. One must weigh that logical possibility against the fact that since North Korea has engaged in high-profile cyber-operations in the past, North Korea's cyber capabilities and units are likely a focus of some components of the USG, and that those components have probably developed a high level of expertise and knowledge.

We should certainly keep an open mind about all of this. But we also shouldn't be naive about the level of US capability in this area.

Nick P • **December 26, 2014 11:58 AM**

@ Dirk Praet

To be fair, the report and it's recommendations are pretty good. At least they were doing something positive for INFOSEC. I kept a copy of the report that I intend to pass onto local businesses in addition to what I would normally give them.

Jon Pollard's talking hemorrhoid • December 26, 2014 1:45 PM

Skep still thinks the clowns who let 9/11 happen under their nose, who let Brittany Gordon get blown to pink mist, who didn't notice when Kim Jong Il kicked the bucket, who never knew what hit them when India blew off their bomb (now THAT was funny as shit,) they must know what they're talking about.

You can't fix stupid, can you?

Q • December 26, 2014 2:06 PM

Thank you, Bruce Schneier, for finally adding SANITY CHECKING as a necessity for analyzing security breaches.

These script kiddies leveraging 4gl tools without any awareness of what's going on behind the scenes is enough to drive a man insane!

Phill Hallam-Baker • December 26, 2014 3:18 PM

I am getting rather fed up of posts saying with great certitude that the government is lying about the source of the attack. The fact that the Bush administration lied about the pretext for their invasion of Iraq does not mean that we should automatically assume the opposite of what the government claims.

From what we know now, the evidence of attribution to North Korea is as good as it ever gets. The bigger problem is what Bruce points out above: We can't distinguish an actual attack by North Korea with an attack someone intends to look like it has been performed by North Korea.

And that is why the macho posturing from the would-be 'cyberwarriors' is futile: Cyberweapons are not a very effective means of achieving a goal. If the exercise was a false flag operation intended to provoke the US into responding with 'kinetic' force (the cure euphemism military folk have for killing people, it is a failure. If the North Koreans intended to protect the honor of their 'dear despot', well that failed as well.

The legacy of Stuxnet is a lot less impressive in retrospect. Stuxnet did not prevent Iran getting a nuclear bomb as claimed. Four years after Stuxnet was discovered, Iran still has not built the bomb it was six months away from completing. All Stuxnet did was provide politicians with a lower cost political option than telling Netanyahu that US allies don't decide when to start wars.

Cyber is very much like terrorism: it just isn't very effective at all. There is no point in terrorism unless people know why the attacks are taking place. Covert action becomes terrorism the minute someone finds out about it. Rather than running round in circles scaring ourselves with the use of a desperation tactic we should be asking how to downsize our militaries to respond to what is a modest threat compared to the USSR.

I have been saying of the drones that US policy will stop supporting them as soon as other

countries start to 'drone up'. The same will be true of cyber.

The people who run the US intercept/cyber warfare capability are the same folk who were out in public defending the Bush administration torture program. We should reject both as ineffective and morally repugnant.

Phill Hallam-Baker • **December 26, 2014 3:32 PM**

One other point, given what we now know about the scope of NSA surveillance, I really wouldn't discount the possibility that the NSA has a pretty good notion of where the attack came from.

But so what?

It is very clear that a well financed cyber attacker can do a lot of damage to the US economy with plausible deniability. It is also clear that the US and its NATO allies are far more vulnerable to this mode of attack than any plausible adversary.

It is now clear that we have exactly the wrong type of cyber-command. Rather than investing in building a capability to attack other countries we should invest 100% of our efforts in building defenses, including helping potential adversaries such as China to build defenses.

The US understands that there can never be sufficient confidence in cyber-attribution to respond to a cyber attack with conventional 'kinetic' force (don't you love the cute euphemisms people have for killing people). It has taken a great deal of effort to get the US policy makers to that point and as Bruce will confirm, that understanding cannot be taken for granted, there are many people pushing to reverse it.

We cannot be confident that other countries will respond with the same measured approach. This administration has used the attack as an opportunity to roll out a doctrine that says this type of attack is not warfare and does not justify a military response. What if someone creates an attack on China designed to look like it comes from Russia? Can we be confident that it won't lead to escalation to 'kinetic' war?

The US needs to get right out of the cyber-sabotage business. Shut down the cyber-command and build a cyber-protection center out of the NIST campus instead.

Sancho_P • **December 26, 2014 5:54 PM**

@ Skeptical

Unfortunately it is pretty obvious that *“the US must be simply stupid”* [1] :

There is absolutely no benefit for pointing at NK - **especially if that is the truth.**

On the contrary, it was extraordinary damaging to point at the NK regime for two reasons:

(1) The inability to punish them makes the US looking bad and vulnerable. [2] [3]

(2) Because of the nature of “secret” evidence nearly everybody (outside USG) starts thinking about some possible US moles within the NK regime.
And the NK regime will go further than just thinking.
OK, I guess the moles are (were) not US citizens so no problem for the “brave and free”.
But they’ve lost them and in all likelihood discouraged others.
That’s a loss for the US and a win for the NK regime.

[1] I didn’t write that but it would be the least damaging possibility if we can call it the “**G**rand **N**on **D**iplomatic **D**isease” of the US.

[2] They would have to topple and destroy the entire regime within days - better hours - to “bring them everlasting peace and democracy”.
Like it was done to Iraq, Afghanistan, Libya, ...

[3] More sanctions, seriously? Mind you, sanctions are counterproductive as history should have shown the USG.
You must convince the people, not hurt them.

Sancho_P • **December 26, 2014 5:59 PM**

@ Phill Hallam-Baker

I guess you’re barking up the wrong tree.
There is no great certitude, only great fear that some dimwits got it wrong again.
Probably all want it to be true because the consequences would be extremely bad otherwise.
But see my comment above @ Skeptical.

I concur with your other good points, thanks.

… Um, only *”There is no point in terrorism unless people know why the attacks are taking place.”* isn’t true, terrorism has no point even when ‘the reason’ is known:
Terrorized people simply ignore ‘the reason’ because terrorising is deemed “unfair” in the first place,
- see the “Sony Hack”.

Ughhhh • **December 26, 2014 7:58 PM**

It was North Korea.

Anyone who doesn't believe it are completley ignorant of the history of North Korea.

1. Bombing a airliner because they were jealous of the 1988 Olympics held in South Korea

2. Starting a naval battle because South Korea was co-hosting the World Cup with Japan in 2002.

3. Sinking the South Korea military ship the Cheonan because they were mad they lost a earlier naval battle.

Those are only some of the incidents but see the pattern? They react when they're jealous, they react when they're humiliated. The Interview was a humiliation for them, a provacative act by the US. Of course they're going to strike back somehow.

Ughhhh • **December 26, 2014 8:10 PM**

@John

"America is no different from North Korea: full of propaganda. Funny how you can be outraged at another nation's government yet your own is the same. They simply don't see it."

Wow shut up. I try to avoid namecalling but its impossible when someone meets a person of your ignorance. The ole' "America has done bad things too" equivalency fallacy.

@emk

"What is astonishing is that intelligent people will actually believe anything the US government says regarding an official enemy like North Korea. How much lying does the US government have to do before it loses any credibility with American cyberprofessionals."

Just because they lie a lot doesn't mean they lie about everything.

"What does North Korea (NK) have to gain from hacking Sony?"

Are you kidding? It just amazes me people who have zero understanding of recent contemporary history of North Korea speak so confidently on it.

They were insulted, they struck back. That's basically their m.o since the 60's. You're thinking as a perfect rational actor which North Korea is not. Go google "North Korea axe murder incident". Why would North Korea kill America GIs with axes which might trigger a war they would lose? I don't know but they did.

It may be hard for many American's, but suspend disbelief for a while and assume NK rationality.

Do you even know anything about North Korea? Or is everything you write based on simply your distrust of the US government? Just because the US government is bad doesn't inversely make the North Koreans good or innocent of accusations.

"Would it not be better for NK to have the film released and then use the fact to paint the US as an aggressor? Why hack a private company?"

Most countries in the world don't view a screwball Seth Rogen comedy as a grave interntional

incident. Why hack a private company? Oh gee lets see they were willing to bomb a airliner basically because they were jealous that their neighbor South Korea was hosting the 1988 Olympics, you really think they'd give two shits about hacking Sony?

"The potential for this to backfire and drive support and viewership for the film is immense. The NK are not stupid."

They're not stupid but revenge isn't based on rationality. There was no well thought masterplan, they saw a movie that pissed them off and they reacted angrily.

"It is far more likely that the US govt is piggybacking on this to threaten, attack and harass NK, than that NK did the hack.""

There is literally zero reason for the US to engage in a stupid game to attack or harass North Korea.

Again, if you knew anything about North Korean history you would know there's been tons of opportunities for the US to attack North Korea (such as 1999 when North Koreans were on the cusp of activiating their first nuclear reactor, or the more recent artillery attack on a South Korean island).

Please actually learn something about this topic before speaking on it.

Ughhhh • **December 26, 2014 8:24 PM**

@Cowbert

I don't even know where to start. This is right up there with "Israel did 9/11"

"My own personal hypothesis is that it's the last category (co-opted false flag), since spoofing source is relatively easy to do. I postulate the initial attack was conducted by either:

2. Another pro-Western Asian country (possibly South Korea or Japan). Again this could be a combination of driving factors:
A. Why it could be South Korea
a. The current President, Park Geun-hye is known to be hawkish. Her father, after all, was infamous for his leadership in the military coup of 1961 and authoritarian presidency from 1963-1979."

bashes head against wall

If you're going to come up with a half-assed theory like this shouldn't you add the most juicy motivation of all, that Park Geun-hye's mother was killed by a North Korean agent?

https://en.wikipedia.org/wiki/Park_Geun-hye#Early_life_and_education

"b. South Korea has significantly increased its economic ties to China over the past few years, prompting Western analysts to wonder about the stability of its pro-US military alliances. Perhaps the ROK believes that playing up a "common enmity" towards the DPRK that is shared by the US and PRC will increase stability between its two main rival allies. In addition, like the US-led scenario above, this would be a perfect training and development opportunity for ROK cyberwarfare units. Another possibility is that ROK is exploring a defense treaty with China, which would alienate the US. But if they got the US to attack DPRK, it would fulfill one of their longstanding strategic goals now, even if future US support diminished."

Again this is right up there with "Israel did 9/11".

Think of the risk/reward, South Korea according to you is going to frame NK for hacking Sony in the hopes that China and the US see NK as a common enemy? China has always been a stalwart ally of North Korea, the US accusing North Korea of something would just drive a wedge between China and the US like its had for about 10 years.

"Another possibility is that ROK is exploring a defense treaty with China, which would alienate the US. But if they got the US to attack DPRK,"

Should I just stop right here?

The phrase "only a fool takes up a fools argument" comes to mind. Sorry I don't want to call you a fool but you're talking so much nonsense right now its hurting me. Literally hurting me.

"Another possibility is that ROK is exploring a defense treaty with China, which would alienate the US. But if they got the US to attack DPRK,"

South Korea is framing North Korea so the US attacks North Korea.

I wish there was a group of North Korea policy buffs to laugh at this.

Do you just not know that North Korea has atomic bombs in addition to conventional artillery thisclose to Seoul the megapolis capitol of South Korea? If the US attacks North Korea that would trigger a all-out war where the North Koreans first target would be Seoul. Even without nuclear weapons they would turn Seoul into another Hiroshima.

"B. Why it could be Japan
The current Prime Minister, Shinzo Abe, is known to be hawkish. As a whole, his administration is eager to loosen traditional constitutional interpretations against militarization (because among other things it would allow them to renegotiate US force levels in Japan). Japan also regards DPRK a strategic and tactical threat due to being in range of DPRK cruise missile capability (which is why Japan owns several Aegis BMD-capable/Arleigh Burke-derived destroyers and an islands-wide network of PAC-3 systems). Attacking a domestic target like Sony would have reduced the difficulty of the attack. Finally, like the US-or-ROK-led scenario above, this would have also been a perfect T&D opportunity for JSDF cyberwarfare units."

You're writing a horrible Tom Clancy novel at this point.

Ughhhh • December 26, 2014 8:34 PM

Written by Bruce Schneier

1. "This is the work of independent North Korean nationals."

Most of the country doesn't even have internet access. I believe there are some expatriates in Japan I doubt they have the capacity or the boldness.

2. "There is still the very real possibility that the hackers are in it just for the lulz, and that this international geopolitical angle simply makes the whole thing funnier."

Possible but too much of a coincidence. You have North Korea one of the most prideful and petty countries in the world, you have a movie that clearly pushes their buttons, and you have one of the worst cyberattacks of all time. You're telling me that's a coincidence?

If you look at the pattern of North Korean behavior, saying they haven't reacted at all besides diplomatic protests and angry denouncements without some kind of retaliation would be an outlier.

3. "On the other hand, maybe not. I could have written the same thing about Iraq's weapons of mass destruction program in the run-up to the 2003 invasion of that country, and we all know how wrong the government was about that."

I'm far from a fan of the US government. Its true they could be wrong about North Korea being responsible, not a deliberate lie, but they have extremely flimsy evidence and they're only happy to say it was North Korea.

However what you and few others seem to be considering is the pattern of behavior by North Korea.

The hacking of Sony matches up perfectly with expected North Korean behavior when they're humiliated.

Ughhhh • December 26, 2014 8:48 PM

To be honest it just pisses me off that people have this weird apathy when it comes to North Korea.

Here is one of the most evil regimes in human history, a country that not only physically starves their people but spiritually starves, them, the closest thing we have to Orwell's 1984 and instead of anger it generates either apathy, a shrug of the shoulders, or better yet some giggles over the absurdity of it all.

And worse still unlike with Israelis and Palestenians, the South Koreans also share this or

better yet think the North Koreans are some kind of wayward brothers they have to bring into the flock.

And then what really makes me mad, then someone writes a book or documentary or movie telling me how bad the Holocaust is with the sloagan "Never Again".

Now I understand human nature, there is no spokesperson that's put a human face on the suffering inflicted on the North Korean PEOPLE, by the North Korean GOVERNMENT. No Anne Frank, no Malala, nobody. To make things worse the whole populace suffers from stockholm syndrome where they have to love their rapists, the Kims and their Orwellian government.

Look, I don't expect people to share my level of hatred against North Korea, but lets all recognize how bad they are. And dont shrug it off because Steve Spielberg hasn't made a movie on it in the lines of Schindlers List or you dont have a guy like Al Sharpton barking about it 24/7.

Many people jump to conclusions when a rich white athlete is accused of raping a poor black female, many people jump to conclusions when they hear a white person shot a unarmed black person, many people jump to conclusions when they hear a teacher has been accused of pedophilia, but the one time you ask me to not jump to conclusions is when one of the most evil governments in the world, in all of human history is accused of something?

If I'm too passionate in my hatred for North Korea, then I think you are a little too clearheaded and neutral.

And if you want some hard facts, go google "axe murders North Korea", "North Korea airliner", "North Korea kidnappings", "North Korea shoots tourist", "North Korea Cheonan".

Why are you all willing to give a country like this the benefit of the doubt?

Ughhhh • **December 26, 2014 9:00 PM**

Sorry, I know I've written a lot, dont want to give the impression I'm trying to flood the comments.

But a question for everyone here.

After reading about all these past incidents

http://en.wikipedia.org/wiki/Axe_murder_incident

http://en.wikipedia.org/wiki/Korean_Air_Flight_858

http://www.reuters.com/article/2008/07/11/us-korea-north-shooting-idUSSEO14908720080711

http://en.wikipedia.org/wiki/Blue_House_Raid

http://en.wikipedia.org/wiki/ROKS_Cheonan_sinking

http://en.wikipedia.org/wiki/Rangoon_bombing

http://en.wikipedia.org/wiki/USS_Pueblo_%28AGER-2%29

http://www.nytimes.com/2002/06/29/world/four-killed-as-north-and-south-korean-navy-vessels-trade-fire.html

http://en.wikipedia.org/wiki/Bombardment_of_Yeonpyeong

http://www.telegraph.co.uk/news/worldnews/asia/northkorea/8053617/Highest-ranking-North-Korean-defector-dies-aged-87.html

You dont think its perfectly within pattern of past behavior that North Korea was involved in the hacking of Sony?

Pattern: North Korea gets mad, then they get even in someway.

South Korea hosts Olympics = North Korea bombs airliner, North Korea denies involvement

North Korea loses naval battle = Sinking of the Cheonan, North Korea denies involvement

North Korea captures USS Pueblo, they say it violated their waters, US says it was in neutral waters.

At what point do you have to say where there's smoke there's fire?

Nick P • **December 26, 2014 11:32 PM**

@ Ughhh

"You have North Korea one of the most prideful and petty countries in the world, you have a movie that clearly pushes their buttons, and you have one of the worst cyberattacks of all time. You're telling me that's a coincidence?"

You're consistently applying one set of standards to the North Korea theory and another to every other theory. I could likewise say we have Sony pissing off hackers with CD malware, removing PS3 other OS option, and lure of total insecurity revealed during PSN hack [which hackers will mentally associate with Sony in general]. Then, they have their CISO publicly brag about getting compliance people to accept his insecure controls, treat their IT workers as disposable, treat their INFOSEC workers like they don't matter (5 bosses for 3 ignored techies), and add layoffs to layoffs.

And then they get hit as if someone knew all about their inside operations, had spent plenty of time in the network, and hated their guts. Classic revenge hacking absent any other information. See how easy it was to apply your method to lead to Bruce and I's theory of the Sony hack? And we have many more motives and potential attackers than one film pissing off

one attacker. And they would know it would be easy having been there and seeing Sony's mismanagement.

re doubts of U.S. govt

Regarding U.S. government, they bullshit by default on cyber threats to push an agenda to get [offensive] power and profit. Let's look at some things in this one subject area:

1. NSA said they are trying to increase the security of American products. We know they won't let TEMPEST tech in most products, they deliberately weakened standards, and promoted tech that is insecure by their own standards for critical infrastructure. They did the latter even when they could offer a secure GOTS alternative for free or at cost. That says a lot.

2. NSA said they were only collecting metadata, not data, on Americans. Snowden leaks showed they were collecting about everything they could. And they had changed definition of "collect" to mean an analyst looking at it rather than intercepting it. Clever deception.

3. NSA and FBI said they were trying to help businesses improve system development processes and organizational security to make their products/services more secure. Leaks showed that they were paying or "compelling" via FBI businesses to "SIGINT enable" their systems. For deniability, they often left in or inserted ordinary software vulnerabilities to make it look like an accident. Same kind Chinese and Russian hackers find with some being hit in the field. Talk about aiding the enemy while lying that they're helping.

4. FBI said they were catching and stopping all kinds of terror plots. Turned out they were entrapping people with undercovers: encouraging them and giving them ideas before arresting them. The FBI creating terrorism to say they were stopping it. Glad they didn't slip up and one bomb something with their new skills.

5. NSA vastly overstated the importance of its collection programs in stopping terror plots. We later found they had almost no effect. They're still pushing fiction about its effectiveness to keep it going for... whatever reason.

6. NSA, FBI, and other government groups pushed the notion that we need to worry about a subversion risk from other countries. We could trust their evaluated products to not be subverted. Leaks showed they had subverted more than about anyone and a nearly guaranteed way to get backdoored/hacked is using something they promoted.

7. NSA and FBI push for over a decade that they need backdoored access, err surveillance capabilities, in all systems and communications to stop cyber attacks. Everyone with any experience in INFOSEC knows that increasing the security of systems and organizations using them is only way to stop cyber attacks or reduce their effect. Adding deliberate vulnerabilities or backdoors while encouraging commercial and government procurement of such systems only reduced security.

I'm seeing a consistent pattern of lying over anything related to cyber attacks, cyber defense, information security, surveillance, and so on. That's on top of past examples of lies for political

posturing or imperialist activities. That's also not including incompetence other commenters mentioned where they misidentified attackers in major, hilarious (and sometimes quite sad) ways. Collectively, this justifies a Distrust Until Verified approach to NSA/FBI if the claims are related to a category where they have consistently deceived Americans for selfish gain. This event ties into several of those simultaneously and so I'd like at least a third party verification of these claims.

North Korea certainly could've done it. Just looks much more like Internet hacker culture + insiders than the typical brute style of North Korea. Your examples combined with how the Sony hackers acted post-hack is actually more evidence against North Korea angle than I've provided so far. Bruce and I's agree on an alternative theory as it fits better. If FBI/NSA provide evidence of theirs, I might change my mind. Regardless, though, the solution is to apply highly assured INFOSEC techniques to anything critical and reduce risk across the organization.

FBI and NSA surely won't help them do that. They'll do selective risk minimization like in their report at best. Leaving open all the methods they, foreign nation states, and sophisticated black hats use to get in. And then talking about how we need to worry about North Korea because Sony's security and management sucked. And trust that they're honest and working in our interests this time. ;)

Phillip • **December 26, 2014 11:32 PM**

@ Ughhhh

Calm down. Excellent posts; thanks. I have trouble discerning which is the bigger strawman; is it pyongyang with its history of impulsives or; mighty eagle with the history of lies? if we dove into history of geopolitiosociological hate, we saw root in the sk's people\of all three stakeholders. what's your take on that? I apologize for the bad typing.

Clive Robinson • **December 27, 2014 7:37 AM**

@ Ughhhh,

I've been keeping an eye on both Koreas for a little over a quarter of a century for business reasons, and happen to live in an area with one of the largest Korean communities outside of S.K.

And whilst I am very aware of what goes on in N.K. and I'm far from turning a blind eye about it I am however quite aware of how other Koreans see the situation.

For instance many S.K.s are quite anti US due to the way the US and others provoke the N.K. leadership, because they realise that the only way forward to help those in the north is by dialogue and business activities that open up the North to the South. What you frequently see them upset about is every time the US pokes it's nose in with faux initiatives is that it will go wrong when the US political wind shifts a fraction and fail but also take all the other dialogue work with it thus setting things back months or years.

When looking at what you claim NK has done you leave out an incredible amount of other information abou why the lash out. If you examin the behaviour of animals, children and many adults they all lash out when provoked, why would you realisticaly expect a nation to behave any differently? After all what about the US response to 9/11 that lashing out is still going on well over a decade, which suits US politico's well and thus will probably continue for another few decades one way or another.

You make comment about bombing planes but forget to mention that many nations including the US hijacked and bombed planes directly or indirectly for political reasons.

You don't mention that Russia shot down a Korean passenger jet and have in times past caused diplomatic incidents with NK when relations between Russia and China soured. You also don't mention that it was Russia -v- USA that started the Korean war and that Russia then dumped it in the laps of the Chinese. Nor do you mention the fifty years of US provications towards NK directly and indirectly through SK which in part are proxie attacks on China.

It just so happens that SK frightens both the US and China as both see SK as a significant economic threat. Thus neither want to see the reunification of the two Koreas due to what would happen economically.

You also forget to mention that Koreans hate the Japanese and it is this hatred that spured on their meteoric economic development that has only slowed due to limited population and resources, something the North is not limited in. I'm sure there are quite a few SKs who would chearfully kick the wind out of a large Japanese companies sails just for the fun of it, and dropping it in NKs lap would be even funnier for some of the more right wing groups.

Further you don't mention what China is currently upto with regards the China seas which is causing rather more than the US military to get nervous.

Nor do you mention what Putin is upto with regards both the North and the South.

It would be nice if all of these issues were not relevant to who might have had cause to hack SPE and where they come from and their motivation. But they exist and are very relevant.

Getting hung up on any of these issues is virtualy a guarantee that those who hacked SPE will walk away from it unharmed, and that is dangerous because it will embolden them to do similar again.

That's why we have to view the evidence and potential suspects fairly dispassionately, otherwise things will get a lot lot worse.

Whilst I'm aware of the NK leadership and it's continuing effects on the NK citizens, you need to also consider what will happen to those citizens when any backlash from the leadership happens because of these US Pres BO accusations... Especialy those who might illegaly access the internet via mobile phones connecting to service providers in adjacent countries...

We owe it to these people to make sure the SPE hackers who ever they are identified correctly

and dealt with. Which means we have to examine things in a detached way and consider all possabilities, to provide an honest outcome.

That said, as many SKs will tell you the way to make the lot of the NK citizens better is to first get the NK leadership to open the door a fraction and alow them to feel the benifits of opening the door further. As Koreans will also point out they were enslaved by the Japanese for over half a century, and it was WWII that gave them freedom from that, thus they can see it takes major wars to get rid of unwanted enslavers... They are thus both patient and pragmatic people in their outlook, they know change will take time.

Dirk Praet • **December 27, 2014 10:34 AM**

@ Ughhhh

Look, I don't expect people to share my level of hatred against North Korea

May I be so bold as to enquire where this hatred comes from ? Most regular visitors on this blog are familiar with one or more of the usual suspects invariably posting pro-USG comments, most of the time even in a very intelligent and articulate manner, but yours read entirely different, almost as if this is some kind of personal matter. Please don't fall into the trap of letting personal emotions cloud your judgement.

---

kittengloves • **December 27, 2014 10:38 AM**

Lot's of companies get hacked on school holidays. Many servers have gone down lately. BOOM all EA's servers just went down a while ago. It's fairly easy to take down servers with a little no how and preperation and pretty easy to prentend to be someone somewhere else.
I knew a 13 year old kid with 100,000 strong botnet who may some pretty good coin just DDOSing folks for other folks.

Darren • **December 27, 2014 9:26 PM**

@ Phill Hallam-Baker: "I have been saying of the drones that US policy will stop supporting them as soon as other countries start to 'drone up'. The same will be true of cyber."

Swapping banners or names does very little when the underlying agenda is firmly aligned. One can argue that "Ministry of War" must change its name and function to Defense Ministry in order to protect its legitimacy, but that does very little to transform its structure. Offense and defense must complement each other, regardless of banner. I'm not sure how you use the word cyber in your context. Years back it was action of two initimate adults over some type of comm., namely internet. Further back, it was a research called Cybernetics. In the war context, I'm sure you can alternate names like cyberwarrior and cyberdefender without anybody complaining about it.

Phill Hallam-Baker • **December 28, 2014 3:43 PM**

@Sancho_P

Oh I was not responding to Bruce specifically there but the comments on this blog and statements by our colleagues. Bruce sets out several plausible alternative scenarios besides the government one and I think they deserve serious attention.

I think the last one in which NK only comes in after someone else made the hack is very plausible. I have seen that done before. If the North Korean regime was like the Russian or Chinese regime with lots of loyal patriots inside the country with access to the net we would have to consider the possibility the extortion came from an irregular hactivist group. But NK is a really weird case in that it does not have any external friends at all. Even China is openly contemptuous of their 'ally'. They like having a buffer state but they detest the Kim regime.

What I object to is the statements made by folk with great certainty that the government is lying. We don't know what happened for certain and likely never will until the NK regime collapses.

I do however understand precisely where the skeptics are coming from. Anyone who hangs round this part of the industry is aware that there are many ex-US generals who are trying to turn cyber into a fourth domain for warfare with a budget to match land sea and air. And not by cutting any existing pentagon boondoggles either. They aren't working to make America safe, they are trying to divert government cash into yet another feed trough for wealthy parasites like themselves.

What the incident does illustrate though is the potential for cyberattacks like this to result in international incidents and possibly wars if the parties that are attacked don't think through the implications in advance.

We need to make cyberspace secure. That has nothing to do with developing ways to attack other countries or keeping them in a state of vulnerability.

Nick P • **December 28, 2014 6:18 PM**

@ Phill

"What the incident does illustrate though is the potential for cyberattacks like this to result in international incidents and possibly wars if the parties that are attacked don't think through the implications in advance"

Good point.

Clive Robinson • **December 28, 2014 10:41 PM**

@ Phill,

> "What the incident does illustrate though is the potential for cyberattacks like this to result in international incidents...

And the reason for that is, as I said above,

> *... they don't appear to understand what the difference of levels of evidence are, that are required for an"Intelligence suspicion" and a "Diplomatic condemnation" given publicaly. The former requires no evidence, just coincidence, the latter requires evidence sufficient to go to war honestly and thus commit thousands to their deaths such that they should not be needless.*

Even though we are not --yet-- trading shots with NK over the statment made by US Pres BO, it is almost certain that many people will die over it in the next few weeks, months and years.

As many of us who have posted here think there is way to little visable evidence of NK leadership involvment, the fact US Pres BO made the statment publicaly means that the NK leadership will assume there is some form of hard evidence the US has, and without it being made public the NK leadership will try to find it, as would any other nation.

If as we suspect the NK leadership were not involved, this will precipitate a "Witch Hunt" by the NK leadership. In turn, this will almost certainly mean that any assets / agents the US or other nations have in NK will be put at risk or compromised and end up being "fed to the dogs".

But it won't stop there, it's known that there are NK citizens that have "Smart Phone" access to the internet via service providers in adjacent countries. There will thus be a renewed vigor to find these people and they likewise will be hurt or killed as examples to others.

Such harms will not forment an uprising in NK, it will in fact undermine and destroy work done by others to get the NK leadership to be more open and thus moderate such oppressive behaviour.

Thus the door will be closed further and even more NK citizens will starve and die from the resulting economic down turn.

Then there is "future actions" to be considered, NK is fairly adept at making reprisals without going "to far", they have after all been doing it for over sixty years. However people who are not NK citizens get hurt or die in such reprisals.

All of this is well known, so you have to ask why US Pres BO wants to precipitate such harms and what the US and rest of the world gets out of it...

Even at the best of times and done responsibly diplomacy is a dirty game, where the dirt is the blood of innocents. Done irresponsibly it goes from a few perhaps justifiable deaths to out right needless carnage. Personally I think US Pres BO has behaved irresponsibly not just over NK but over the use of drones and many other things, I wonder if those that recommended him for his Nobel prize are now regretting their actions.

Dirk Praet • **December 29, 2014 7:42 AM**

"Researchers from the security firm Norse allege that their investigation of the hack of Sony

has uncovered evidence that leads, decisively, away from North Korea as the source of the attack. Instead, the company alleges that a group of six individuals is behind the hack, at least one a former Sony Pictures Entertainment employee who worked in a technical role and had extensive knowledge of the company's network and operations."

https://securityledger.com/2014/12/new-clues-in-sony-hack-point-to-insiders-away-from-dprk/

Nick P • December 29, 2014 1:56 PM

Darnit, Dirk, you beat me to it. Bruce and I's side of the debate just got a lot more cred. :)

Dirk Praet • December 29, 2014 6:23 PM

@ Nick P.

It gets even better.

A person identifying himself as a Lizard Squad administrator said the group provided a number of Sony employee logins to Guardians of Peace, the organization that allegedly broke into Sony's network and prompted the film studio to initially withdraw "The Interview" from theaters.

A Q&A with the hackers who say they helped break into Sony's network (Source: Washington Post).

Then again, we should probably still not entirely preclude the theory that this is a very clever DPRK psy-op setting up as patsies some European juveniles who just happened to get doxed by @BrianKrebs .

Nick P • December 29, 2014 7:22 PM

@ Dirk

Wow. That was some interview. Hope they're full of crap. Otherwise, they reiterate how vulnerable Tor users might be while making the NSA's problems with it confusing to me. Further, they show that DDOS attacks are up to around 2+Tbps. Nobody's pipe is going to handle that. I can't say if there is a solution past proxying through an anti-DDOS vendor as I haven't studied modern DDOS too much and doubt most companies can even afford the pipes. I think a very large amount of public funding should be put into finding economical solutions to the problem at the company, ISP, and backbone levels. It's worth it given how much damage it can do vs what little it costs.

I liked the pauses though. Always good to see cocky, fast-talking people pause. That tells you you're getting in their head a bit or they're screwing with yours with intentional pauses. Then, it's a process of narrowing it down. The author didn't do that, unfortunately. The next one should.

---

grammar police • December 30, 2014 9:45 AM

@Nick P

You write "and I's" often as in "Bruce and I's side of the debate". Should it not be "Bruce and my side of the debate"?

---

grammar police • December 30, 2014 9:46 AM

@ Nick P

Correction: "Bruce's and my side of the debate".

BJP • December 30, 2014 10:16 AM

@grammar police

Those textual quirks are useful for attribution.

Nick P • December 30, 2014 10:48 AM

@ grammar police

Maybe it was just bait intended to lure a grammar nazi in front of my scope. BANG! :P

@ BJP

Good point. Someone brought that up about Clive a long time ago. The size of the post was usually the identifier. Yet, if it was small, the quirks of his writing style gave it away before you saw the name.

Clive Robinson • December 30, 2014 12:52 PM

@ Nick P,

It should not be "Bruce and I" but "Bruce, others and myself"...

The simple fact is the evidence presented of only external hackers like NK, ment they had to somehow get extraordinarily lucky or be omnipotent, neither of which was as likely as an unhappy insider or ex-insider, then there was the speed the download happened at, to be at that rate across an external network SPE should have noticed it, but they apparently did not, so either they were incompetent or an insider did the equivalent of a backup to fast storage...

So untill a legaly valid explanation of these that directly points to NK turns up then US Pres BO "should not be casting stones".

But as I've said there are a whole lot of other issues that could spike the case if the US decided to "go to court" as it started with some Chinese military officers...

It's interesting to note that BO and advisors are not saying anything even though they are rapidly loosing credability over it...

It's going to be interesting to see if this ends with a "big bang" or a "damp squid" ;-)

Clive Robinson • December 30, 2014 12:58 PM

@ Moderator,

Speaking of quirks in style the comment above from Zach Anderson reads like link spam.

Sancho_P • December 30, 2014 5:04 PM

- It's still possible (IMO unlikely) that NK was behind, let's hope (for the sake of the USG).
- For the President it was clumsy to point at anybody.
- For the President it was extremely dumb to point at NK, regardless if true or not.

My condolences to all those involved in the reaction of the NK regime.

Embarrassing.
Seems to be right, this puppet is only there to cast bad light on the black in general.
(Remember what @Skeptical wrote , it hurt me:
*"(2) **You do not allow** the US President to make such a statement unless **you** have what **you** believe to be ironclad proof."* [emphasis added])

Until torture is back in the news they won't say anything again about Sony / NK.

For the download speed - sorry, I didn't get that point.
Using a 56k modem, being thousand miles away, I could dump terabytes from my company's server. Speed only depends on sender and receiver?

Wael • December 30, 2014 6:05 PM

@grammar police,

> You write "and I's"

I gave up on that a while back. Nick P is a stubborn dude ;) I assure you that your words will fall on deaf ears :)

Wael • December 30, 2014 6:41 PM

@Clive Robinson, @Nick P, @grammar police,

Re: Me, Myself, or I?

Perhaps a visit to Dr. Grammar may help ;) Mind you, his prescription may differ from the British ones...

In the old days when people studied traditional grammar, we could simply say, "The first person singular pronoun is I when it's a subject and me when it's an object,' but now few people know what that means. [. . .] The misuse of I and myself for me is caused by nervousness about me. [. . .] But the notion that there is something wrong with me leads people to overcorrect and avoid it where it is perfectly appropriate. People will say, 'The document had to be signed by both Susan and I' when the correct statement would be, 'The document had to be signed by both Susan and me.'

Trying even harder to avoid the lowly me, many people will substitute myself as in 'The suspect uttered epithets at Officer O'Leary and myself.' Myself is no better than I as an object. Myself is not a sort of all-purpose intensive form of me or I . Use myself only when you have used I earlier in the same sentence: 'I am not particularly fond of goat cheese myself'" (Brians, Common Errors in English Usage).

I am afraid to report Nick P's use of "I's" to the grammar doctor, he probably wouldn't believe me. Besides, if history is of any use, then there is no known remedy for this ailment. Lol @grammar police, Tell you what: Just arrest him, he's been cautioned before :)

Nick P • December 30, 2014 7:09 PM

@ Wael

(sighs long and audibly) (hand on forehead)

@ all three of you

It's called innovation. Maybe I just flex my language like I flex my mind. ;)

The alternative is a rigid and superficial approach where people focus on semantics more than the message itself. A time-wasting concept whose anti-social flare rivals my own approach to "discussing" COTS security. My standard says the use of language was successful if the message got across. That simple. Such a standard requires less work on grammar, saves bandwidth, and reduces editing time.

So, I'll continue in my crusade to promote conversational liberty in the face of against grammatical tyranny. Me, myself, and I's crusade. :P

Wael • December 30, 2014 7:33 PM

@Nick P, @All,

Digressing a little from the subject matter of the thread -- seems inevitable after a thread has been in discussion for a protracted period of time...

Speaking of languages, I recently (as in two days ago) started playing with Swift. Didn't have the time before, but since I am off for a few days... Anyway, was pretty impressed with its simplicity, power, and elegance. I recommend taking a look at it:

https://developer.apple.com/swift/
There is a book you can download for free (I read it in a couple of days.) towards the bottom of the link. Now I can think seriously about continuing the project I wanted to work on for years because the only thing that stopped me was Objective C, which has never appealed to me.

Wael • December 30, 2014 7:51 PM

Re Swift...
http://www.apple.com/swift/
Book is here: https://itunes.apple.com/us/book-series/swift-programming-series/id888896989?mt=11

Nick P • December 30, 2014 7:53 PM

@ Wael

It's a definite improvement over Objective-C. It kept me out of Apple development, as well. The one I'm seeing the most praise for is Rust. All of them say that it's a bit harder to get your app past the compiler. Yet, once you do, it pretty much just works. First major systems language I've heard that said of since Ada. I'll have to check both of them out.

Or build another BASIC/4GL/LISP that autogenerates to all of them. Might use a Wirth language instead of BASIC this time. Maybe Python instead of LISP, although Racket Scheme is incredibly powerful these days. Maybe a functional language for executable specifications & 3GL code generation instead of 4GL and CASE tools. Sounds much more fun than going mainstream. Plus, one of my old integration schemes lets me use libraries in arbitrary programming languages albeit with performance penalties. One tool to rule them all. (Villainous laughter)

Skeptical • December 31, 2014 8:02 AM

Before I respond to some specific comments, I have to say that I am amazed at the credulity shown by some in their reading of the private-sector "alternative theories" being reported by the media (who love controversy, as it sells, even when there really isn't any controversy).

"We talked with some people who said they were part of Lizard Squad, and they said they were in on it." Sure, Lizard Squad, a juvenile little group that grabs every bit of attention it can for causing problems for Sony. Very credible.

"We don't think that North Koreans would have made the same grammatical mistakes in English." Right, and I wonder what the confidence level on that conclusion is.

Then there are the theories that are quite literally speculation based on facts of which the speaker is completely ignorant. "Sony could not have missed the exfiltration of X amount of data." That's a fairly bold assumption for anyone who knows nothing about Sony's network,

data transfer needs, or how and what precisely was compromised.

I hesitate to even speak of any of these as alternative theories. They're faintly sketched possibilities, at best. They carry little weight against an analysis of US interest in avoiding a mistaken accusation and of displayed US capability in the cyber domain.

@Clive: *For instance many S.K.s are quite anti US due to the way the US and others provoke the N.K. leadership, because they realise that the only way forward to help those in the north is by dialogue and business activities that open up the North to the South.*

Er, that's why SK asked the US to postpone relinquishing command and control of SK military forces last year.

The US and SK both favor reunification. The NK regime, and the PRC, do not.

What you frequently see them upset about is every time the US pokes it's nose in with faux initiatives is that it will go wrong when the US political wind shifts a fraction and fail but also take all the other dialogue work with it thus setting things back months or years.

Believe it or not, South Koreans have much stronger opinions about how to handle North Korea than the US does, and changes of government in South Korea have far more significant effects than do political changes in the US. Indeed, just to give an indication of the depth of feeling about the matter, a former high-ranking intelligence official in South Korea was recently convicted on corruption charges relating to claims that he ordered a campaign to link certain political parties to "soft" views on North Korea as a means of discrediting those parties.

By contrast, US policy on the Korean Peninsula has been steady for decades.

When looking at what you claim NK has done you leave out an incredible amount of other information abou why the lash out. If you examin the behaviour of animals, children and many adults they all lash out when provoked,

You're comparing NK's actions, ranging from kidnapping Japanese citizens to use to train foreign intelligence operatives to sinking SK naval vessels to bombarding inhabited SK islands, to a child lashing out?

You also don't mention that it was Russia -v- USA that started the Korean war and that Russia then dumped it in the laps of the Chinese. Nor do you mention the fifty years of US provications towards NK directly and indirectly through SK which in part are proxie attacks on China.

The US certainly did not start the Korean War. The Korean War neither foreseen as part of US national strategy at the time, nor was the US military prepared to fight it. It is true however that Stalin pushed hard for it, believing that the US would not intervene.

And following the Korean War, the US strategy has simply been to help secure South Korea,

until North Korea eventually collapses under its own internal contradictions and weaknesses and a reunification occurs.

It just so happens that SK frightens both the US and China as both see SK as a significant economic threat. Thus neither want to see the reunification of the two Koreas due to what would happen economically.

North Korea would be a significant burden on South Korea, and the US signed a free trade agreement with South Korea in 2007. You're flat wrong about US views on South Korea.

Wael • **January 1, 2015 8:24 PM**

Just finished watching the movie. Pretty bad! What a waste of time! Not worth all the fuss...

ImAwake • **January 1, 2015 8:33 PM**

Just another excuse to send military and conker one more country.

Clive Robinson • **January 1, 2015 9:49 PM**

@ Wael,

OK, the film appears to be the "turkey not fit to serve on any day" that the critics said or the POS that members of the film viewing public have said...

So a question arises, "Why, knowing it was very probably a waste of time and money did you go and pay to watch it?"

With a second perhaps more pertainent question of "Without all this fuss in the papers and online over the SPE hack, would you have paid money and gone and seen it?".

I need to say at this point I've no intention of wasting either my life or money on this film as I've made that mistake before with a "Colon Brothers" film.

Wael • **January 1, 2015 10:15 PM**

@Clive Robinson,

I'll answer all your questions with this paragraph:
I only watched it because of the noise people made of it. I did not "go" to watch it, it came to me via Amazon for $5.99, which I regret spending on it, and I am not frugal by any means. Remember the quote from a Sony CIO interview? I'll add another possibility: They hired a marketing person who probably worked at Hollywood previously. This marketing person said: "No publicity is bad publicity", if life keeps giving you lemons (like the IT lemons they have), make lemonade :) The movie made $10 million so far, I hear. Now the CIO can save this money to pay for the next 10 incidents ;)

sooth_sayer • **January 10, 2015 11:33 PM**

Pay the gangs in Russia -- Moldova, Romania $100K and they will do it gladly -- they might do it for even less!
NK didn't have to write the code .. maybe they did .. maybe the hackers left the hint... maybe NK wanted the hint left .. more than Sony NK wants the dunce in WH to deliver some oil like 2 presidents before this one have done it.

It worked then, it will work better this time too.

Subscribe to comments on this entry

Leave a comment

Login

Name (required):

NAME_FULL

E-mail Address:

EMAIL_ADDRESS

URL:

UNKNOWN_TYPE

Remember personal info?

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

UNKNOWN_TYPE

Comments:

UNKNOWN_TYPE

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

Preview Submit