


Strategic Negligence and the Sony Sideshow

 The NAPSNet Policy Forum provides expert analysis of contemporary peace and security issues in Northeast Asia. As always, we invite your responses to this report and hope you will take the opportunity to participate in discussion of the analysis.



Recommended Citation

Peter Hayes, "Strategic Negligence and the Sony Sideshow", NAPSNet Policy Forum, December 22, 2014, <https://nautilus.org/napsnet/napsnet-policy-forum/strategic-negligence-and-the-sony-sideshow/>

NAPSNet Policy Forum

Peter Hayes

December 22, 2014

I. Introduction

Peter Hayes argues, "It is urgent to correct the fish-tailing, improvised response that the United States has adopted in response to the Sony attack and aftermath."

"Each day that passes, North Korea is enriching uranium that can be used in nuclear weapons, it is improving its missile and other delivery systems, and it is reconstructing its plutonium-producing reactor. Time is on North Korea's side, not that of the United States."

"There is simply no substitute for the tedious, painstaking work of constructing a meaningful diplomatic and security relationship with the North Koreans. Not doing so is strategically negligent."

Peter Hayes is Co-founder and Executive Director of Nautilus Institute for Security and Sustainability; Honorary Professor at the Center for International Security Studies, Sydney University, Australia.

II. Policy Forum by Peter Hayes

The imbroglio over *The Interview* is a sideshow that reveals that the Obama Administration, like the Bush Administration before it, has lost the plot with regard to North Korea. The real game is to stop, reverse and end North Korea's nuclear weapons breakout. Its handling of *The Interview* has managed to distract the US government from this strategic imperative, increase the risk of war, including nuclear war, and made it harder than ever to advance American vital security interests in relation to North Korea's nuclear threat.

The real video we should be watching is not *The Interview* but US Strategic Command's deterrence [symposium](#) from August 14, 2014. At [minute 23.35](#), recently retired US Major General John MacDonald who served until recently in US Forces Korea/Combined Forces Command/UN Command in Korea, advocates including assassination of North Koreans in STRATCOM's policy options kitbag for dealing with Kim Jong Un over the next three years.

Unlike *The Interview*, this movie is not satirical, nor is it fictional. It is posted by US Strategic Command, the military command that plans for using nuclear weapons against North Korea. Cyber Command that may lead US retaliation against North Korea is a component of Strategic Command.

[Stratcom.mil](#) is the one website that we can be assured that the North Koreans monitor on a daily basis. This video is on a US government website. As Commander-in-Chief, President Obama owns this assassination video.

That it appears on-line today reveals the same attitude towards managing the North Korean threat as the Administration's handling of *The Interview*. If Sony's internal emails are to be believed, a senior US State Department official [advised](#) Sony CEO Michael Lynton that because the US-DPRK relationship was already so toxic, releasing a movie showing KJU's head being blown off by a shell fired from a tank by Seth Rogen would not do any additional damage to US security interests in the region.*

He was wrong. There were and are consequential and potentially catastrophic risks, and there was no reason to not tender sound advice to that effect to Sony's CEO who at least asked for guidance. The careless advice reportedly given to Sony is an indicator of the Obama Administration's attitude toward the DPRK which can be described fairly as negligent. Nothing can be done, so what we do doesn't matter.

President Obama's threat to retaliate against North Korean-controlled computer infrastructure that is physically located in or transiting China may be an attempt to pressure China to address its [earlier request](#) that it address Chinese hacking against American firms, using North Korea as the lever. The

White House may also be counting on China to act unilaterally against [North Korea's cyber capacities](#) in response to [US requests](#) to this effect due to the threat of American cyber-attack on this infrastructure located in China if they don't, or simply because China may be upset that North Korea's abuse of [its access to China](#) is drawing attention to China and can be ended at little or no cost.

Unfortunately, the US response to the Sony attacks aims does not offer China any shift in the American attitude towards the DPRK and how to solve the DPRK nuclear issue. In short, the US move is disingenuous, China knows it, the DPRK knows it, and the Sony-Rogen low point in American handling of the US-DPRK relationship will, like any protracted tempest in a teapot, eventually blow away—provided it doesn't escalate into war.

Unlike the Sony sideshow, managing the national security dimensions of the US relationship with North Korea is an urgent, vital interest. The retaliation threatened by Obama, whether or not it comes to pass, will have counterproductive impact in Pyongyang. The North Koreans are fearful about pre-emptive nuclear and conventional strikes, for many reasons. These include specific reference to North Korea as a candidate for preventive strike in the US 2010 announced nuclear declaratory doctrine, and the long trail of US hostility expressed in words and deed towards North Korea. Much of this hostility is deserved given North Korea's own bad faith, outrageous actions, and inflammatory and irresponsible rhetoric. Some is cultural, and is based on a realistic appreciation that North Korea embodies the antithesis of values that define what it is to be American. And some is purely ideological, based on American misreading of North Korea and responding to stereotypes and rabid fear-mongering.

But some of North Korea's actions respond to what Americans say. General MacDonald is not the only one to say that the United States should be in the business of assassinating North Koreans. RAND Corporation's Bruce Bennett, for example, [reportedly told](#) Sony in June 2014 that the only way to get rid of the North Korean regime is to assassinate its leader. Moreover, Sony CEO Lynton asserted that a senior US official agreed with Bennett's views (the State Department [declined](#) to clarify what this official said although it did say that he had not viewed the movie). Bennett also told Sony that the ending whereby the assassination guys awry but Rogen gruesomely kills Kim by head demolition leading ultimately to the overthrow of the regime by a "free North Korea"* in *The Interview* should be kept so that it could leak into North Korea as samizdat DVD that would destabilize North Korea. (According to the [leaked emails](#), Rogen later modified the killing imagery as follows: "We took out three out of four face embers," Rogen writes of shrapnel set to hit Kim's face. "Reduced the hair burning by 50%, and significantly darkened the chunks of Kim's head.").

It is urgent to correct the fish-tailing, improvised response that the United States has adopted in response to the Sony attack and aftermath. Perhaps the White House was driven by the need to divert journalists from focusing on the CIA torture story, or to counter accusations that by recognizing Cuba, President Obama is soft on dictatorships.

However, the situation is now spiraling out of control and is already beyond fair game in Washington's partisan politics. The reality is that no-one knows [who has escalation dominance](#) in a purely cyber-warfare between the United States and the DPRK. A great deal of military and civilian critical infrastructure in the United States, at home and abroad, is vulnerable to cyber-attack, unlike North Korea which has a [substantial intra-net](#), but whose economy and military mostly still live and work in a pre-Internet era without Internet connection or even significant dependence on the DPRK intra-net.

According to the Pentagon's spokesman, Rear Admiral John Kirby, there are [no clear international rules](#) or even norms that demarcate commercial or vandalistic cyber-attacks from cyber-warfare,

unlike in kinetic warfare in Korea where a military demarcation line is physically inscribed on the strategic landscape. President Obama has thrown down the gauntlet to the DPRK by suggesting that Sony should show the movie, thereby revealing at the same time his own estimate that the alleged DPRK threats to the safety of movie-goers was not credible. Sony [reportedly is exploring](#) how best to release *The Interview* live on-line, possibly via its own streaming video service, [Spackle](#), possibly to fend off the White House's criticism that it caved to threats.

That the DPRK will respond is entirely predictable, especially President Obama's [promised retaliation](#) involves information warfare aimed at spreading anti-regime propaganda inside the DPRK or converting *The Interview* into some kind of DVD samizdat. Indeed, the DPRK has already [threatened](#) to respond. It is a short distance from the merely symbolic cyber-domain to kinetic and radioactive battlefields in a place as heavily armed as in Korea. Whether the [DPRK Internet link outage on December 22 2014](#) is the first American retaliatory shot (or some third party denial of service attack) is anyone's guess. But it shows just how dangerous the game being played over a fictional assassination movie has become.

It is not obvious who will have the last laugh in this pathetic Sony sideshow. Certainly it will undermine US reputation for sound strategic decision-making and an ability to maintain stability in the Korean Peninsula, let alone facilitate negotiations to capture and reverse North Korean nuclear armament. Assuredly, the United States will not gain reputation abroad, and especially in East Asia, by defending a movie that depicts the assassination of a living head of state, especially one as potentially dangerous as Kim Jong Un.

Each day that passes, North Korea is enriching uranium that can be used in nuclear weapons, it is improving its missile and other delivery systems, and it is reconstructing its plutonium-producing reactor. Time is on North Korea's side, not that of the United States. This is what matters in terms of vital national security interest, not the fate of *The Interview*.

The United States is still the world's only superpower. It can still shape Kim Jong Un's strategic calculus, rather than merely imagine his denouement via its cultural industry. There is no shortage of small, medium, and large strategic [options](#) for the United States to reduce the danger of war and nuclear war involving North Korea.

Admittedly, it is [not easy](#) to negotiate with North Korea; but has been [done before](#) successfully, and must be done again. Doing so means determining how to hold North Korea accountable for its alleged [cyber-vandalism](#) and reduce the probability of war, nuclear war, and nuclear proliferation at the same time. Everything else should be set aside.

There is simply no substitute for the tedious, painstaking work of constructing a meaningful diplomatic and security relationship with the North Koreans. Not doing so is strategically negligent.

* edited December 29, 2014 1.11 pm PST after viewing the film and in response to private communications explaining that the killing scene was an "act of self defense" by Rogen against Kim Jong-un's armed helicopter firing on the tank driven by Rogen, not an assassination attempt (which goes awry earlier in the movie); also, the munition that Rogen fires from a tank that kills Kim Jong Un is not the capsule containing poison as is earlier hidden in Rogen's rectum and sent by the CIA via a drone fired from US Forces Korea to deliver the lethal weapon to their guesthouse in Pyongyang. Such are the subtleties of this movie in which Seth Rogen takes on the mission of assassinating Kim Jong Un and ends up unleashing a successful free North Korea insurgency.

III. ATTACHMENT 1: PRESIDENT OBAMA'S YEAR-END PRESS CONFERENCE, DECEMBER 19, 2014

On December 19, President Obama held a year-end press conference at the White House. Below are excerpts from that press conference related to U.S. foreign policy and international engagement. A full transcript of the press conference will be available on [the White House website](http://iipdigital.usembassy.gov/st/english/texttrans/2014/12/20141219312317.html#axzz3MZ9YXIYp).

THE WHITE HOUSE
Office of the Press Secretary
Washington, D.C.
December 19, 2014

<http://iipdigital.usembassy.gov/st/english/texttrans/2014/12/20141219312317.html#axzz3MZ9YXIYp>

My presidency is entering the fourth quarter; interesting stuff happens in the fourth quarter. And I'm looking forward to it. But going into the fourth quarter, you usually get a timeout. I'm now looking forward to a quiet timeout -- Christmas with my family. So I want to wish everybody a Merry Christmas, a Happy Hanukkah, a Happy New Year. I hope that all of you get some time to spend with your families as well, because one thing that we share is that we're away too much from them.

And now, Josh has given me the "who's been naughty and who's been nice" list -- (laughter) -- and I'm going to use it to take some questions. And we're going to start with Carrie Budoff Brown of Politico. There you go, Carrie.

Q: Thank you, Mr. President. I'll start on North Korea -- that seems to be the biggest topic today. What does a proportional response look like to the Sony hack? And did Sony make the right decision in pulling the movie? Or does that set a dangerous precedent when faced with this kind of situation?

THE PRESIDENT: Well, let me address the second question first. Sony is a corporation. It suffered significant damage. There were threats against its employees. I am sympathetic to the concerns that they faced. Having said all that, yes, I think they made a mistake.

In this interconnected, digital world, there are going to be opportunities for hackers to engage in cyber assaults both in the private sector and the public sector. Now, our first order of business is making sure that we do everything to harden sites and prevent those kinds of attacks from taking place. When I came into office, I stood up a cybersecurity interagency team to look at everything that we could at the government level to prevent these kinds of attacks. We've been coordinating with the private sector, but a lot more needs to be done. We're not even close to where we need to be.

And one of the things in the New Year that I hope Congress is prepared to work with us on is strong cybersecurity laws that allow for information-sharing across private sector platforms, as well as the public sector, so that we are incorporating best practices and preventing these attacks from happening in the first place.

But even as we get better, the hackers are going to get better, too. Some of them are going to be state actors; some of them are going to be non-state actors. All of them are going to be sophisticated and many of them can do some damage.

We cannot have a society in which some dictator someplace can start imposing censorship here in the United States. Because if somebody is able to intimidate folks out of releasing a satirical movie, imagine what they start doing when they see a documentary that they don't like, or news reports

that they don't like. Or even worse, imagine if producers and distributors and others start engaging in self-censorship because they don't want to offend the sensibilities of somebody whose sensibilities probably need to be offended.

So that's not who we are. That's not what America is about.

Again, I'm sympathetic that Sony as a private company was worried about liabilities, and this and that and the other. I wish they had spoken to me first. I would have told them, do not get into a pattern in which you're intimidated by these kinds of criminal attacks. Imagine if, instead of it being a cyber-threat, somebody had broken into their offices and destroyed a bunch of computers and stolen disks. Is that what it takes for suddenly you to pull the plug on something?

So we'll engage with not just the film industry, but the news industry and the private sector around these issues. We already have. We will continue to do so. But I think all of us have to anticipate occasionally there are going to be breaches like this. They're going to be costly. They're going to be serious. We take them with the utmost seriousness. But we can't start changing our patterns of behavior any more than we stop going to a football game because there might be the possibility of a terrorist attack; any more than Boston didn't run its marathon this year because of the possibility that somebody might try to cause harm. So let's not get into that way of doing business.

Q: Can you just say what the response would be to this attack? Would you consider taking some sort of symbolic step like watching the movie yourself or doing some sort of screening here that --

THE PRESIDENT: I've got a long list of movies I'm going to be watching. (Laughter.)

Q: Will this be one of them?

THE PRESIDENT: I never release my full movie list.

But let's talk of the specifics of what we now know. The FBI announced today and we can confirm that North Korea engaged in this attack. I think it says something interesting about North Korea that they decided to have the state mount an all-out assault on a movie studio because of a satirical movie starring Seth Rogen and James Franco [Franco]. (Laughter.) I love Seth and I love James, but the notion that that was a threat to them I think gives you some sense of the kind of regime we're talking about here.

They caused a lot of damage, and we will respond. We will respond proportionally, and we'll respond in a place and time and manner that we choose. It's not something that I will announce here today at a press conference.

More broadly, though, this points to the need for us to work with the international community to start setting up some very clear rules of the road in terms of how the Internet and cyber operates. Right now, it's sort of the Wild West. And part of the problem is, is you've got weak states that can engage in these kinds of attacks, you've got non-state actors that can do enormous damage. That's part of what makes this issue of cybersecurity so urgent.

Again, this is part of the reason why it's going to be so important for Congress to work with us and get a actual bill passed that allows for the kind of information-sharing we need. Because if we don't put in place the kind of architecture that can prevent these attacks from taking place, this is not just going to be affecting movies, this is going to be affecting our entire economy in ways that are extraordinarily significant.

IV. ATTACHMENT 2: FBI PRESS RELEASE UPDATE ON SONY INVESTIGATION

<http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>

Update on Sony Investigation

Washington DC

December 19, 2014

Today, the FBI would like to provide an update on the status of our investigation into the cyber attack targeting Sony Pictures Entertainment (SPE). In late November, SPE confirmed that it was the victim of a cyber attack that destroyed systems and stole large quantities of personal and commercial data. A group calling itself the “Guardians of Peace” claimed responsibility for the attack and subsequently issued threats against SPE, its employees, and theaters that distribute its movies.

The FBI has determined that the intrusion into SPE’s network consisted of the deployment of destructive malware and the theft of proprietary information as well as employees’ personally identifiable information and confidential communications. The attacks also rendered thousands of SPE’s computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company’s business operations.

After discovering the intrusion into its network, SPE requested the FBI’s assistance. Since then, the FBI has been working closely with the company throughout the investigation. Sony has been a great partner in the investigation, and continues to work closely with the FBI. Sony reported this incident within hours, which is what the FBI hopes all companies will do when facing a cyber attack. Sony’s quick reporting facilitated the investigators’ ability to do their jobs, and ultimately to identify the source of these attacks.

As a result of our investigation, and in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions. While the need to protect sensitive sources and methods precludes us from sharing all of this information, our conclusion is based, in part, on the following:

- Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks.
- The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack.
- Separately, the tools used in the SPE attack have similarities to a cyber attack in March of last year against South Korean banks and media outlets, which was carried out by North Korea.

We are deeply concerned about the destructive nature of this attack on a private sector entity and the ordinary citizens who worked there. Further, North Korea’s attack on SPE reaffirms that cyber threats pose one of the gravest national security dangers to the United States. Though the FBI has

seen a wide variety and increasing number of cyber intrusions, the destructive nature of this attack, coupled with its coercive nature, sets it apart. North Korea's actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves. Such acts of intimidation fall outside the bounds of acceptable state behavior. The FBI takes seriously any attempt—whether through cyber-enabled means, threats of violence, or otherwise—to undermine the economic and social prosperity of our citizens.

The FBI stands ready to assist any U.S. company that is the victim of a destructive cyber attack or breach of confidential business information. Further, the FBI will continue to work closely with multiple departments and agencies as well as with domestic, foreign, and private sector partners who have played a critical role in our ability to trace this and other cyber threats to their source. Working together, the FBI will identify, pursue, and impose costs and consequences on individuals, groups, or nation states who use cyber means to threaten the United States or U.S. interests.

V. ATTACHMENT 3: SECRETARY OF STATE JOHN KERRY ON CYBERATTACK BY NORTH KOREA

<http://iipdigital.usembassy.gov/st/english/texttrans/2014/12/20141219312305.html#axzz3MZ9YXIYp>

19 December 2014

U.S. DEPARTMENT OF STATE
Office of the Spokesperson
Washington, D.C.
December 19, 2014

STATEMENT BY SECRETARY KERRY Condemning Cyber-Attack by North Korea

The United States condemns North Korea for the cyber-attack targeting Sony Pictures Entertainment and the unacceptable threats against movie theatres and moviegoers. These actions are a brazen attempt by an isolated regime to suppress free speech and stifle the creative expression of artists beyond the borders of its own country.

Freedom of expression is at the center of America's values and a founding principle of our Bill of Rights. We're a country where artists openly mock and criticize the powerful, including our own government. We don't always like what they say about us or about others, and sometimes we're even deeply offended. But those offenses have always taken a backseat to freedom of expression. That's why the United States is and always will be a staunch advocate for and protector of the right of artists to express themselves freely and creatively. Whatever one's system of government or views about free expression, there is absolutely no justification whatsoever for an attack like this.

We are deeply concerned about the destructive nature of this state sponsored cyber-attack targeting a commercial entity and its employees in the United States. These lawless acts of intimidation demonstrate North Korea's flagrant disregard for international norms. Threats in cyberspace pose one of the greatest national security challenges to the United States, and North Korea's actions - intended to inflict significant economic damage and suppress free speech - are well beyond the bounds of acceptable state behavior in cyberspace. This provocative and unprecedented attack and subsequent threats only strengthen our resolve to continue to work with partners around the world

to strengthen cybersecurity, promote norms of acceptable state behavior, uphold freedom of expression, and ensure that the Internet remains open, interoperable, secure and reliable. We encourage our allies and partners to stand with us as we defend the values of all of our people in the face of state-sponsored intimidation.

VI. ATTACHMENT 4: ADMIRAL KIRBY STATES THERE IS NO DEMARCATION LINE BETWEEN CYBER VANDALISM AND CYBER-WAR

<http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5560>

Department of Defense Press Briefing by Rear Adm. Kirby in the Pentagon Briefing Room

**Presenter: Pentagon Press Secretary Rear Admiral John Kirby
December 19, 2014**

QUESTION: Thank you Hey, general admiral [sic], a question about North Korea. There's many reports out there about the speculation of them being behind cyber attacks here in the United States. I was just curious from a military perspective what the U.S. military understanding is of North Korea's cyber capabilities? And are they a cyber threat from a military perspective?

KIRBY: Well, without speaking to anything specific with regard to Sony Pictures, as you know, we take cyber threats very, very seriously. Cyber threats come from any number of state and non-state actors. I won't get into, you know, a laundry list here today, but this is something the secretary takes very seriously. It's why he has devoted so much of his energy to the cyber domain. And, I mean, it's something we're constantly mindful of. But I -- I don't -- you know, it's also -- it's also a domain where, you know, you have to be very circumspect about the degree to which -- the specificity to which you talk about both the threats, challenges, and of course whatever responses are available to you.

But -- but more broadly speaking, the Defense Department is certainly, on a routine basis, again, separate and distinct from the Sony Pictures issue, we are on a routine basis part and parcel of the interagency, broad U.S. government approach to threats in the cyber domain.

QUESTION: Can I follow up on that?

Has the U.S. Cyber Command been tasked at all with assisting the FBI or any part of the government in its investigation into the Sony hack?

KIRBY: This is an FBI investigation. I'm not aware of any particular assistance rendered by DOD. That said, we have been part of the interagency discussions about -- about this incident.

Jen?

QUESTION: Just a follow-on to North Korea. The FBI is blaming North Korea for the attack, and says it has evidence. At what point is it an act of war? And at what point does U.S. Cyber Command react?

KIRBY: First of all, I know of no official determination about the -- that's been made about the source

of the attacks on Sony Pictures. So, I'm not in a position to speculate one way or the other. It's an ongoing investigation and I wouldn't get ahead of the FBI on that. As I said, we're part of the interagency discussion about the incident and about options that may be available.

I'm also, you know, not -- not able to lay out in any specificity for you what would be or wouldn't be an act of war in the cyber domain. We take -- it's not like there's a demarcation line that exists in some sort of fixed space on what is or isn't. The cyber domain remains challenging -- remains very fluid. Part of the reason why it's such a challenging domain for us is because there aren't internationally accepted norms and protocols. And that's something that, you know, we here in the Defense Department have been certainly arguing for.

View this online at: <https://nautilus.org/napsnet/napsnet-policy-forum/strategic-negligence-and-the-sony-sideshow/>

Nautilus Institute

608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org