BOSTON GLOBAL FORUM

IDEAS THAT MATTER.

SHORT OF WAR

The Politics of Conducting (and Revealing) State-Sponsored Cyber Attacks

David E. Sanger

Chief Washington correspondent of The New York Times

The World Nine Years Ago..

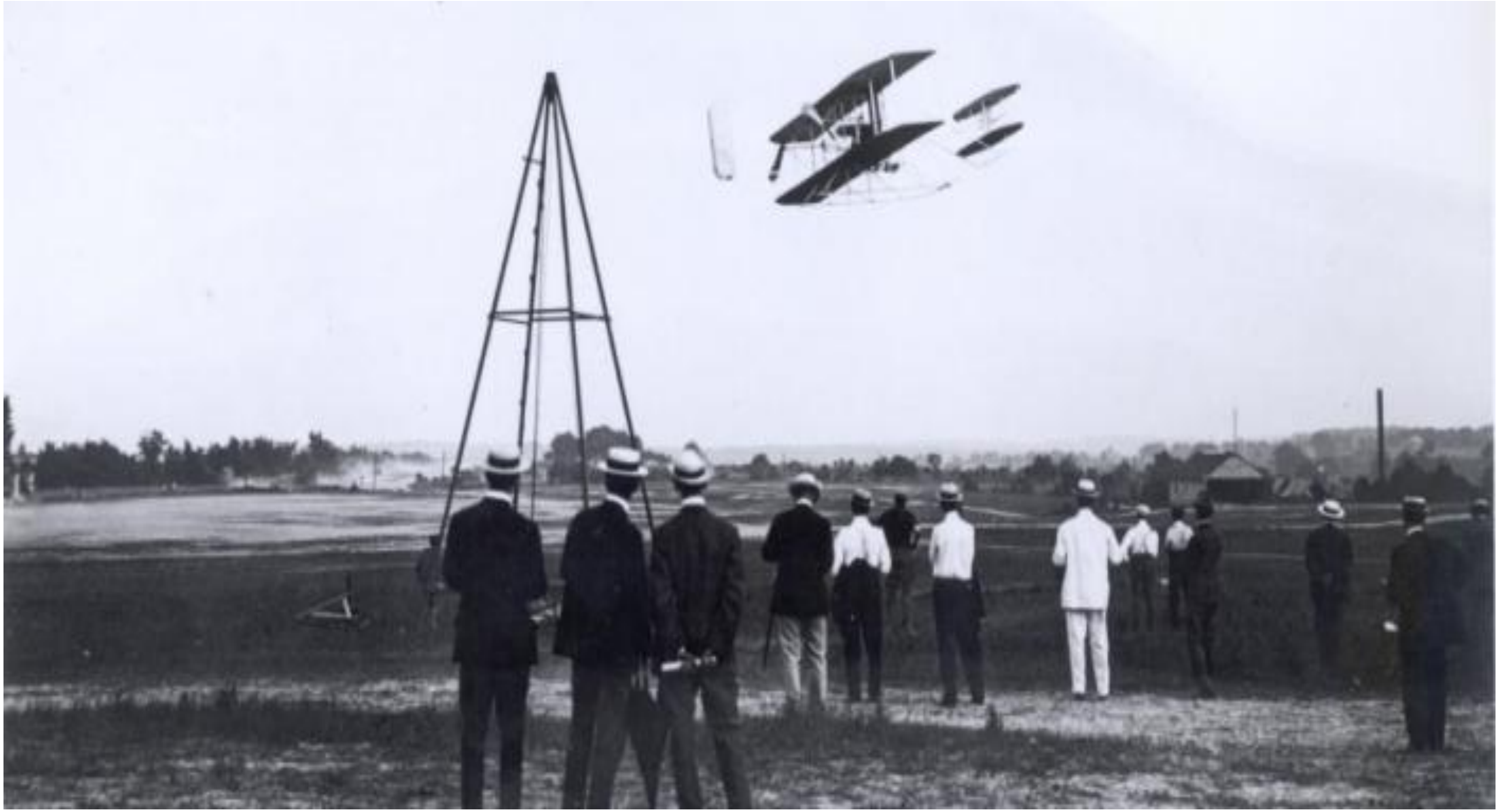
- Jan. 2007 – The Bush Administration presented Congress with its annual “Worldwide Threat Assessment”
- No surprise: “Terrorism remains the pre-eminent threat to the homeland.’’
- Cyber attacks? Didn’t make the list

What Else Happened that Week?

Steve Jobs introduced the first iPhone

In Washington, a group of intelligence officials and generals were working on accelerating a new approach to the Iranian nuclear program.

Why Does This Story Seem Familiar?



The World Today

- For the past two years, the No. 1 threat in the assessment: Cyber attacks on the United States. Soared in “scale, sophistication and severity of impact.”
- But as Gen. James Clapper (Ret.), the DNI, said: “Although we must be prepared for large Armageddon-scaled strike that would debilitate the entire U.S. infrastructure, that is not, we believe, the most likely scenario.’’

Intel Community’s Fear for Future

- Manipulated or corrupted data
- Bad targeting data – bombs on hospitals, market-moving data
- Psychological effects of disinformation
- Misbehaving physical infrastructure
- Create crises based on false indicators

The New York Times

NEW YORK, FRIDAY, JUNE 1, 2012

HASAN SARBAKHSHIAN/ ASSOCIATED PRESS

IRANIAN TELEVISION, VIA REUTERS

IRAN PRESIDENCY OFFICE, VIA EUROPEAN PRESSPHOTO AGENCY

Iran's nuclear enrichment facility at Natanz, which President Mahmoud Ahmadinejad, right, visited in 2007. A computer worm temporarily disabled 1,000 centrifuges, officials said.

Obama Order Sped Up Wave Of Cyberattacks Against Iran

Officials Cite Wide Effort to Hinder Nuclear Work

By DAVID E. SANGER

WASHINGTON

FROM his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room.

What Has Happened Since ‘Olympic Games?’

-- When OG was first described in the summer of 2010, there were almost no documented, highly sophisticated, well understood state-sponsored attacks to compare it to.

-- Today the list is long – more than we can discuss in a few minutes’ presentation.

-- But the TYPE and MOTIVES differ greatly, and in the popular media – yes, it’s the media’s fault – there is very little differentiation.

Reasons for State Sponsored Uses of Cyber

- For Espionage
- For Manipulation of Data
- For Destructive Purposes:

  To Do Via Cyber What Previously Could
  Be Accomplished by Sabotage, Covert
  or Plain Old Bombing

‘Exploit and Attack’

- Since Olympic Games, an evolution of attacks.
- Espionage and intellectual property theft remain predominant. (Anonymity important)
- Attacks for clear military effects remain rare – though that is where much US/Chinese/Russian effort appears to be going. (Again, deniability)
- Politically motivated attacks are on the rise:

-- Tied to a political event or confrontation.

-- Attacker may or may not want to remain anonymous

-- Sometimes wants political message, if not identity, to be easily surmised.

Attacks Aimed at Infrastructure With Destructive Intent

- Stuxnet – directed at Natanz, intended to delay the program
- Planning for additional Iran-related attacks – military advantage
- German steel mill – still a mystery
- Ukraine power grid – briefly destructive, by design, a sign of political message-sending

Political Messaging, Show of Power

- Sony – directed to destroy Sony Picture Entertainment computer systems, mostly protest
- Saudi Aramco – 30,000 computers, but mostly Iranian demonstration of power
- Sands Casino – aimed at Sheldon Adelson’s crown jewel, in retaliation.

Attacks Aimed at Espionage (Selected List)

- State Department/ White House (Russia)
- (Possibility of HRC server as well)
- Unit 61398 – espionage and intl. property theft (Chinese PLA)
- Office of Personnel Management (China)
- Huawei – (U.S.)

Questions for the Administration (Many Unanswered)

- Assuming attribution is reliable, what are the factors in deciding whether to publicly identify the suspected attacker?
- What are the criteria for responding – with diplomacy, sanctions, cyber and/or kinetic response?
- When is a cyber attack not a cyber attack?
- What are the criteria for using cyber as an offensive weapon?

FROM THE WESTERN CAPITALIST PIGS WHO BROUGHT YOU
NEIGHBORS AND THIS IS THE END
전쟁은 시작될것이다
전쟁은 시작될것이다
SETH ROGEN
JAMES FRANCO
이 무식한 미국놈들을 믿지 마십시오!
THE INTERVIEW
인터뷰
인터뷰
전쟁은 시작될것이다
전쟁은 시작될것이다
THIS FILM IS NOT YET RATED.
FOR FUTURE INFO GO TO FILMRATINGS.COM
FALL
/ TheInterview
COLUMBIA PICTURES
a Sony Company
★ 네이버스와 디스이즈 디 엔드를 만든 서부 자본주의 돼지들의 야심작 ★

What Made the Sony Hack Interesting?

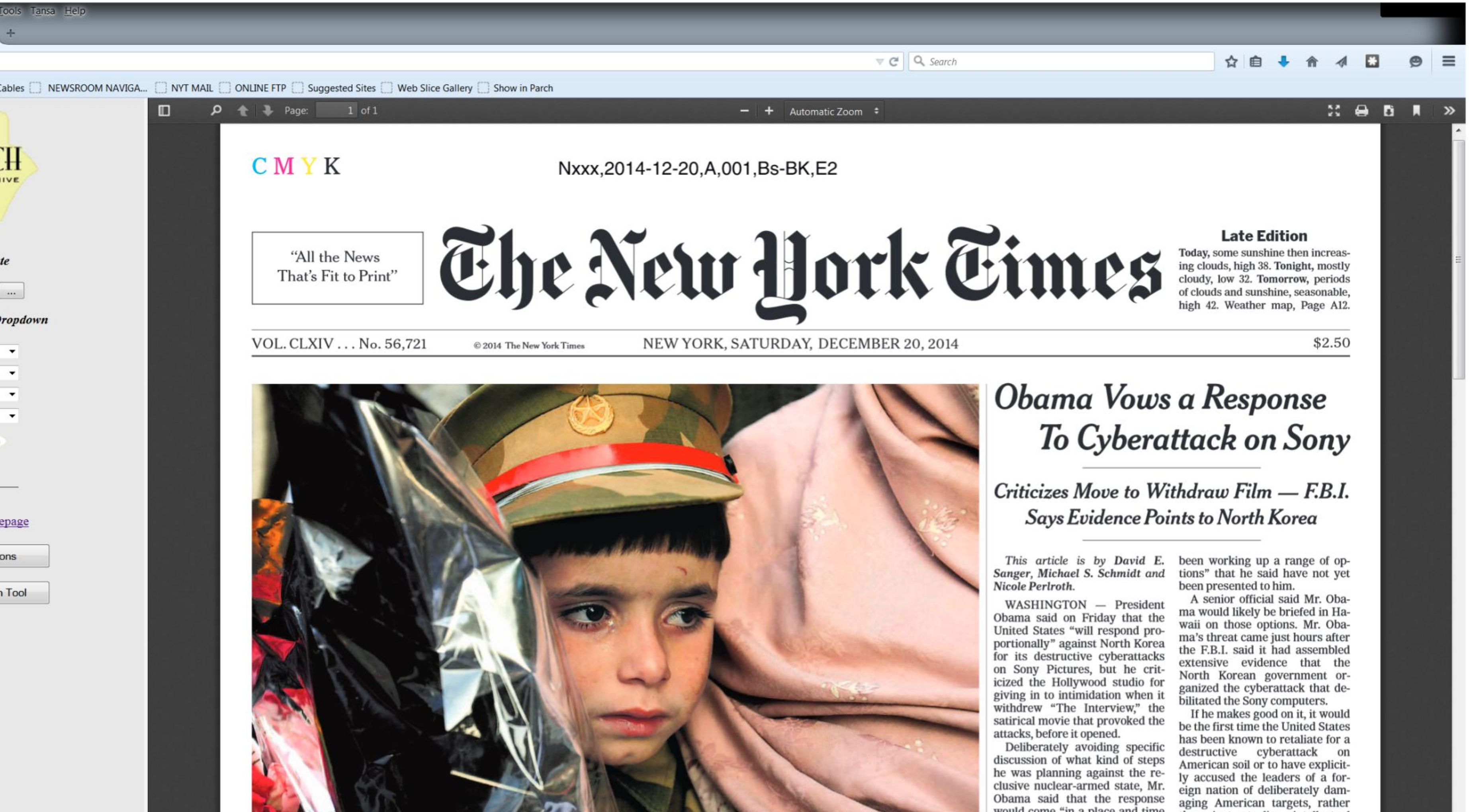
- The Sony incident encapsulated many of the themes and some of the surprises of cyber conflict
- Target was not critical infrastructure
- Objective was not theft, but political coercion
- Code was destructive.
- Hackers had some cultural awareness

  ie. Angelina Jolie emails, salary data

What Made The Sony Hack Interesting? (cont.)

- The government decision to attribute the hack to North Korea but, initially, to provide no evidence.
- The immediate questioning of the government’s story, a reflection of post-Iraq distrust of all intel.
- The FBI’s decision to provide partial evidence.
- The ultimate revelation of NSA penetration of North Korea, and its central role in investigation

The Response



C M Y K

Nxxx,2014-12-20,A,001,Bs-BK,E2

"All the News
That's Fit to Print"

The New York Times

Late Edition

Today, some sunshine then increasing clouds, high 38. **Tonight,** mostly cloudy, low 32. **Tomorrow,** periods of clouds and sunshine, seasonable, high 42. Weather map, Page A12.

VOL. CLXIV . . . No. 56,721 © 2014 The New York Times NEW YORK, SATURDAY, DECEMBER 20, 2014 $2.50

Obama Vows a Response To Cyberattack on Sony

Criticizes Move to Withdraw Film — F.B.I. Says Evidence Points to North Korea

This article is by ***David E. Sanger, Michael S. Schmidt*** *and* ***Nicole Perlroth.***

WASHINGTON — President Obama said on Friday that the United States "will respond proportionally" against North Korea for its destructive cyberattacks on Sony Pictures, but he criticized the Hollywood studio for giving in to intimidation when it withdrew "The Interview," the satirical movie that provoked the attacks, before it opened.

Deliberately avoiding specific discussion of what kind of steps he was planning against the reclusive nuclear-armed state, Mr. Obama said that the response would come "in a place and time

been working up a range of options" that he said have not yet been presented to him.

A senior official said Mr. Obama would likely be briefed in Hawaii on those options. Mr. Obama's threat came just hours after the F.B.I. said it had assembled extensive evidence that the North Korean government organized the cyberattack that debilitated the Sony computers.

If he makes good on it, it would be the first time the United States has been known to retaliate for a destructive cyberattack on American soil or to have explicitly accused the leaders of a foreign nation of deliberately damaging American targets, rather

The Sit Room Debate

- Decided to name North Korea because there were no real diplomatic tradeoffs

- Goal: By calling them out, showing NK leadership that cyber not a free throw. (They went back to nuclear tests and missile launches.)

-- Did modest sanctions, which had little real effect.

- Resistance within the intel community to revealing sources and methods, which undercut the case.

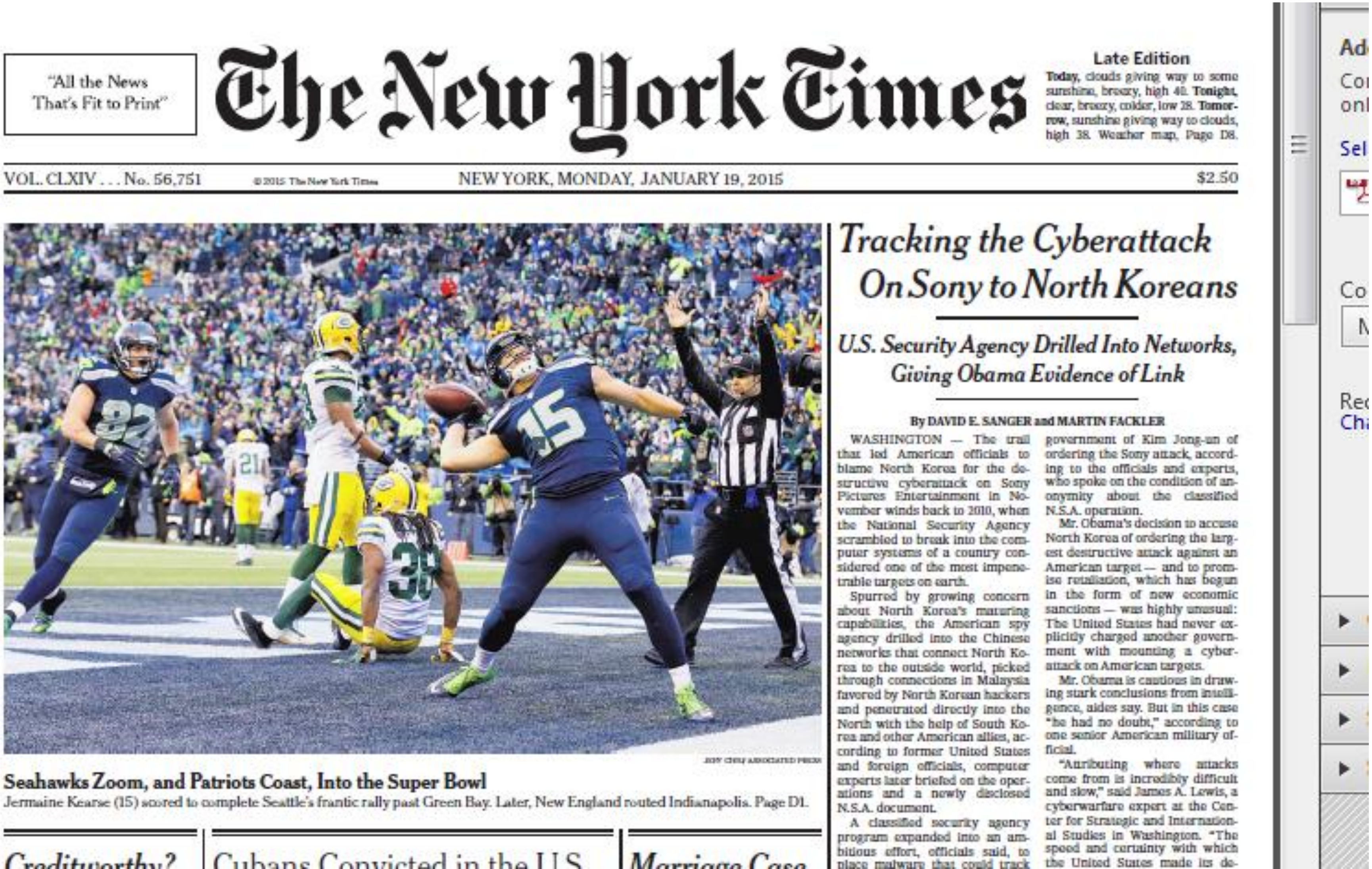
Why Intel Community was Reluctant

- Fall, 2010:
- Two codenamed NSA operations to get into North Korea, including through a “fourth party hack.’’
- “There was a project that I was working last year with regard to the South Korean CNE program. While we are super interested in SK…we were interested in North Korea and SK puts a lot of resources against them….
- www.spiegel.de/media/media-35679.pdf

The NSA cable…

- *“At that point our access to NK was next to nothing but we were able to make some inroads to the SK CNE program. We found a few instances where there were NK officials with SK implants on their boxes, so we got on the exfil points, and sucked back the data…’’*
- *“Some of the individuals that SK was targeting were also part of the NK CNE program….*

The Times Account Jan. 19, 2014: “Nighttrain’’ and Its Follow-ons



“All the News That’s Fit to Print”

The New York Times

Late Edition

Today, clouds giving way to some sunshine, breezy, high 40. **Tonight,** clear, breezy, colder, low 28. **Tomorrow,** sunshine giving way to clouds, high 38. Weather map, Page D8.

VOL. CLXIV . . . No. 56,751 ©2015 The New York Times NEW YORK, MONDAY, JANUARY 19, 2015 $2.50

[illegible]/ASSOCIATED PRESS

Seahawks Zoom, and Patriots Coast, Into the Super Bowl

Jermaine Kearse (15) scored to complete Seattle’s frantic rally past Green Bay. Later, New England routed Indianapolis. Page D1.

Tracking the Cyberattack On Sony to North Koreans

U.S. Security Agency Drilled Into Networks, Giving Obama Evidence of Link

By DAVID E. SANGER and MARTIN FACKLER

WASHINGTON — The trail that led American officials to blame North Korea for the destructive cyberattack on Sony Pictures Entertainment in November winds back to 2010, when the National Security Agency scrambled to break into the computer systems of a country considered one of the most impenetrable targets on earth.

Spurred by growing concern about North Korea’s maturing capabilities, the American spy agency drilled into the Chinese networks that connect North Korea to the outside world, picked through connections in Malaysia favored by North Korean hackers and penetrated directly into the North with the help of South Korea and other American allies, according to former United States and foreign officials, computer experts later briefed on the operations and a newly disclosed N.S.A. document.

A classified security agency program expanded into an ambitious effort, officials said, to place malware that could track

government of Kim Jong-un of ordering the Sony attack, according to the officials and experts, who spoke on the condition of anonymity about the classified N.S.A. operation.

Mr. Obama’s decision to accuse North Korea of ordering the largest destructive attack against an American target — and to promise retaliation, which has begun in the form of new economic sanctions — was highly unusual: The United States had never explicitly charged another government with mounting a cyberattack on American targets.

Mr. Obama is cautious in drawing stark conclusions from intelligence, aides say. But in this case “he had no doubt,” according to one senior American military official.

“Attributing where attacks come from is incredibly difficult and slow,” said James A. Lewis, a cyberwarfare expert at the Center for Strategic and International Studies in Washington. “The speed and certainty with which the United States made its de-

Creditworthy?

Cubans Convicted in the U.S.

Marriage Case

What Did We Learn from Sony?

Lessons Learned,
But Not Widely Shared

- Appears Clapper was not aware of the impending hack when he met his counterpart.
- Spear phishing was seen, but the importance of the focus on Sony was apparently not recognized.
- Sony itself missed the attacks on administrator privileges.
- In cluelessness, reminders of Snowden/NSA.

Sony as Wake-up Call

- “Until Sony, there were a lot of people in the government with lots of Power Points explaining the contours of how cyber weapons would be used in the future,’’ one of Obama’s top strategists said a few months later.
- “It turns out it was all bullsh*t. We didn’t have a clue.’’

Issues for Consideration

- Did Obama create any new kind of deterrence by naming North Korea and sanctioning the country?
- Was the deterrence sufficient?
- What precedent was set by USG intervention?
- Was there a lesson learned in attributing an attack without releasing evidence?
- Is this a “good’’ effect of Snowden leaks, from the government’s viewpoint?
- Has it changed the way companies view security?

The OPM Debacle: When Is a Cyber Attack Not a Cyber Attack

- While Sony was happening, extraordinary espionage attack into OPM
- US govt. did not detect it – for more than a year.
- Absence of understanding about where the government’s most critical security information was stored
- 22 million files, 5.6 million fingerprints

So, Was OPM a “Cyber Attack”?

- No, if you listen to General Clapper.
- It was merely espionage on a grand scale. “If we had the opportunity, we would have done the same thing.’’
- Is Clapper right? Or does scale of theft – data on roughly 7 percent of the American population -- change the nature of the espionage? At that point, does it require a response?

What Was China’s Goal?

- Traditional view is that this was classic: The Chinese were looking to identify intelligence operatives, gain data they could use in recruiting, and learn vulnerabilities (bankruptcies, past relationships
- New think: This information is for authentication. This is how you can pretend to be someone, to gain access. (Here fingerprints, wife’s maiden name, where you were married, best friends.)

Why Is This Man Smiling?

Debate over Retaliation

- No public revelation – even though Chinese attribution was widely leaked
- Consideration of an NSA proposal for a counter attack that would pierce the “Great Firewall of China.” Rejected.
- Decision not to get onto an cyber escalation ladder that was unpredictable.
- Threatened sanctions under “Cyber Sanctions Executive Order.’’

White House Goal: Create a Norm

- Susan Rice trip to China: Had U.N. Experts Group report in hand.
- Chinese authorities said “We agreed to what?’’
- Repeated threat of economic sanction.
- Eventual agreement that forestalled sanctions, at least temporarily

What Was the Deal With China, and Can it Stick?

- Xi visit had two main accomplishments.
- Chinese recognized the concept that state-sponsored theft of IP for profit had to be stopped – but mechanism unclear.
- A first “no first-use agreement’’ in peacetime (in wartime all bets are off).
- Nuclear analogy: Atmospheric test ban treaty

In 2015, Did We Make Progress on Deterrence? On Offensive Use?

- WH claims that indictment of Unit 61398, Obama executive order, and diplomatic agreement with Xi creates the basis for norms.
- Monaco statement 2/2/2016: “Our cyber deterrence policy focuses on….a range of options – cyber and non-cyber– to inflict costs and hold accountable adversaries that chose to conduct cyber attacks or other malicious activity against U.S. interests.’’

What are Criteria for Using Offensive Cyber?

- Pentagon policy is longer and more detailed, but deliberately vague on when the President would use cyber.
- Risk calculus now more complex than it was when Olympic Games was authorized.
- Far more implants in foreign networks, but a dispute between NSA and Cybercommand about when to use them, and thus reveal them.
- Debate evident in the new “equities process’’ to decide when to disclose vs. stockpile zero days.