INQUIRING MINDS… JANUARY 9, 2015

MODERATOR… AL KAPLAN

TOPIC…. CYBER ATTACKS

The Internet has made, and is making profound changes in the world. Not the least of the changes is the advent of the World of Cyber Attacks. The enclosed three articles from the Washington Post, the Wall Street Journal, and the New York Times illustrate just three aspects of the new world. Whether we use the terms Cyber vandalism, Cyber espionage, Cyber crime, Cyber terrorism, or Cyber warfare, or many other names offered, this new world presents attacks of a sort never before seen.

For starters, we ask:

Are there significant different meanings and consequences expected from the different forms of attack we see?

Do we, or should we, react differently whether the attacks are against an individual, or individuals, or against a business entity, or a against a governmental unit?

How can the individual, or a business, or a government act effectively to prevent such activity?

How can or should an individual, or business, or governmental organization respond after the fact, or action, to fix or remedy the situation, or should there be a penal action considered.

And what about the possible prevention or consequences of action against public utilities, such as power, power transmission lines, water and sewage facilities?

And what about compensatory insurance after the fact to repair, and remedy the consequences of a

+++

Opinions

By Robert J. Samuelson December 21 at 8:03 PM.From the Washington Post

"In light of the decision by the majority of our exhibitors not to show the film 'The Interview,' we have decided not to move forward with the planned Dec. 25 theatrical release."

— Sony Pictures Entertainment, Dec. 17

We have just witnessed the first major incident of cyber-blackmail or cyberterrorism. Sony Pictures Entertainment capitulated. This cannot be good, but it obscures a more unsettling message: Our digital dependence exposes us to catastrophic failures of basic services.

Before the surrender of Sony Pictures, the media had generally treated the massive breach of its computer networks as an entertaining yarn. Tens of thousands of e-mails released. Embarrassing comments made by studio executives (Angelina Jolie a "spoiled brat"). Sensitive pay data dumped. All this fed the public appetite for celebrity gossip.

No more. This is no joke.

It seems a landmark event. Other aggrieved groups may imitate the attack — which the FBI blames on North Korea. They will invade their adversaries' computers and, if successful, use the resulting torrent of documents to cripple, extort or embarrass their opponents.

But this is only the first-order consequence. The hacking of Sony Pictures also alerts us to the ultimate cybersecurity horror: the breakdown of vital electronic systems — power plants, financial networks, water supplies — that creates anarchy.

Imagine a major city without power for an extended period. We don't know the odds of this, but they are far greater than zero because so much of daily life depends on vulnerable digital networks.

Sony Pictures is simply the latest big organization to be hacked. The list includesJPMorgan Chase, Home Depot, Target, the U.S. Postal Service and the National Oceanic and Atmospheric Administration, reports James A. Lewis of the Center for Strategic and International Studies (CSIS). If these major institutions couldn't protect their computers, why should we believe that power plants and other essential systems can completely protect theirs?

Until now, the motives for hacking have mostly been criminal and commercial. Thieves steal credit card data or a whole range of personal information to construct false identities. Companies pilfer the trade secrets, business plans and technologies of rivals. The Chinese are widely accused of this sort of heist, which has been characterized — rightly or wrongly — as the greatest theft of intellectual property in human history.

Business is booming. A CSIS study puts the worldwide cost of cybersecurity between $375 billion and $575 billion annually, covering everything from stolen credit cards to the expense of protecting systems. The bill is rising. Symantec Corp., a security firm, says the number of significant breaches rose 62 percent in 2013 to 253.

But cybercrime and cyberwarfare are different animals. To its victims, cybercrime can be tragic personally or fatal commercially. But it's not a social breakdown. That's what

cyberwarfare threatens. The motives are political. The Sony Pictures hack was of this sort. It may be a harbinger.

There are other signs. In October, the Department of Homeland Security warnedthat some industrial control systems — software used to run power plants and factories — are being attacked by malware (software that corrupts the network) associated with Russian users. "This campaign has been ongoing since at least 2011," DHS noted dryly. The fear: that hostile actors are planting destructive software in crucial U.S. systems that could be activated at will.

The Russians, Chinese, Iranians and many rogue groups have reason to hack U.S. computers. We may not spot all the incoming malware (Sony Pictures didn't) and, even if we did, the damage done to the network may take weeks or months to discover and remove.

What's emerging is a new form of warfare with its own weapons. The advantage lies with the cyberattackers for three reasons.

First, they need to find only one entry point into a computer system, while the defenders must guard all possible entry points. In the face of a determined attack, the defense must be almost perfect, not just superior.

Second, it's often hard to determine who the attacker is. This frustrates retaliation, enhancing the appeal of attacking. Although intelligence assessments quickly connected North Korea to the Sony Pictures hack, some observers initially found the hard evidence thin.

Third, companies may under-invest in cybersecurity, says Allan Friedman of George Washington University. The reason: If it succeeds, it doesn't show any return on investment. It doesn't generate revenue or profits. There's a tendency to skimp. Of course, without it, companies could suffer huge losses.

Are we staring down a cyber-abyss? If you talk to security experts, many are relatively optimistic. They say that our systems have ample redundancy and backup. There may be failures, but rebounds will occur rapidly. The United States is also developing its own cyberattack capabilities that would surely deter some possible adversaries. Still, to have any redeeming value, the Sony Pictures debacle needs to awaken us to our growing digital vulnerability.

++++

North Korea and the Internet

North Korea's internet access appeared to be restored Tuesday, nine hours after the country was hit by an outage. WSJ's Ramy Inocencio speaks with Seoul reporter Jonathan Cheng.

North Korea lost what little access it had to the Internet on Monday as outside connections to the small communist country went dark.

The digital blackout came as tensions remained high over Pyongyang's alleged role in a cyberattack on Sony Pictures that destroyed company computers and pushed the studio to cancel the release of a satirical movie about an assassination plot against North Korea's leader Kim Jong Un.

Websites for North Korea's Korean Central News Agency, and a major daily newspaper, the Rodong Sinmun, as well as another propaganda website, Naenara, were restored Tuesday morning, suggesting Internet service had returned.

The timing of Monday's outage caused many to speculate the U.S. played some role in it. But a senior Obama administration official said Monday that the debate about how to respond to North Korea appeared to be continuing, suggesting Washington hadn't directed the outage.

"We have no new information to share regarding North Korea today," said Bernadette Meehan, spokeswoman for the National Security Council. "If in fact North Korea's Internet

has gone down, we'd refer you to that government for comment."

President Barack Obama has said that the U.S. "will respond proportionately" to North Korea over the incident. Options floated for such action include additional economic sanctions and placing North Korea back on the U.S. list of state sponsors of terrorism.

Nevertheless, the outage reflected the murkiness of conflict in cyberspace, where many incidents fall short of war but rise above everyday nuisance. It also demonstrated the variety of actors in cyberwar: While speculation centered on the U.S. and North Korean governments, the operator of a Twitter account linked to the activist group Anonymous claimed credit for the counterpunch. The claim couldn't be verified.

North Korea's single known connection to the Internet runs through China United Network Communications Group Co. , or China Unicom . It went dark late Monday morning East Coast time, according to Internet-monitoring and security companies. It remained out late Monday.

North Korea isn't a hotbed of Internet connectivity—most of its citizens have no access to the World Wide Web—which complicates theories on what did or didn't happen in light of the Sony breach.

Outside investigators weren't able on Monday to immediately inspect what was clogging up North Korea's Internet pipes, and there are no other ways for the few citizens in the North who would have noticed the outage to spread details.

Attackers conceivably could have knocked the country offline by flooding North Korea's small sliver of the Internet with useless traffic, making it inaccessible for legitimate

users. People familiar with the discussions have said the U.S. saw several drawbacks to launching a counterattack against North Korea.

"It's a little early to say what the explanation is," said Matthew Prince, chief executive of CloudFlare Inc., a San Francisco security and network company monitoring the outage. Absent the Sony hack, "I would have thought North Korea decided to turn the Internet off for some reason."

Governments that tightly control information, including Turkey and Syria, often shut access to the outside Web, especially during global tensions.

Another option is that China Unicom could have killed North Korea's access, experts said. "China could be reminding North Korea who owns 'the pipes' it depends on," said Peter Singer, co-author of the 2014 book "Cybersecurity and Cyberwar: What Everyone Needs to Know."

U.S. officials have said they are reaching out to China to help respond to North Korea following the Sony hack, but there have been no indications China would be willing to pressure its bellicose neighbor. The U.S. and China have had their own spats over hacking, U.S. officials note.

Secretary of State John Kerry spoke with his Chinese counterpart over the weekend about the attack on Sony. "We have discussed this issue with China specifically in order to share information and express our concerns about the attack and ask for its cooperation," State Department spokeswoman Marie Harf said.

China Unicom couldn't be reached to comment.

Doug Madory, a researcher at Dyn Inc., a U.S. Internet company, offered a possible benign explanation: network-router software gone haywire. But he said North Korea's network is so small that an accidental outage for several hours is less likely.

"This is out of character for North Korea," Mr. Madory said.

For all the talk about cyberwar Monday, a person familiar with the discussions said U.S. officials are leaning toward a non-cyber response. Cyberattacks, the person said, often "aren't worth the risk."

—Carol E. Lee and Julian E. Barnes in Washington and Jonathan Cheng in Seoul contributed to this article.

++++

<u>Cyber insurance</u>

A high-profile hack at JPMorgan Chase – to say nothing of monstrous breaches at Sony and Home Depot – has made cybersecurity a daily concern for executives at big banks and

corporations. One partial protection is to take out insurance. It's a confusing market, but growing fast. With a United States government campaign on top of all the publicity, coverage may become standard.

The recent break into the internal email servers of Sony Pictures and the subsequent WikiLeaks-like data dump, stated by the F.B.I. to be the work of North Korean hackers opposed to a comedy depicting the assassination of the North Korean leader, Kim Jong-un, may prove costly as well as embarrassing. But the Japanese conglomerate already knows that the failure to secure personal data can be expensive: it shelled out $171 million to cover a 2011 breach of its PlayStation Network.

Yet that pales beside the possible fallout for a big bank like JPMorgan, which suffered a hack potentially exposing certain data for up to 83 million accounts. That's where the government is focusing its efforts, with a Treasury official in December publicly urging banks to get insurance.

There are dozens of underwriters offering cyber-related cover. It's a market on track to double in 2014, to $2 billion of gross premiums in the United States, according to Marsh & McLennan. The frequency of relevant events ticked up sharply last year to about 10 times the rate a decade ago, according to Advisen, a provider of data and analytics to insurers. Yet there are also dozens of different structures and definitions of insurance on offer.

That's where efforts by the banks and Washington may combine to create a bigger, more standardized market for cyberinsurance. That would provide financial cover for at least some of the liabilities arising from hacks. And if the criteria for getting insurance include demonstrating a base level of what Treasury Deputy Secretary Sarah Bloom Raskin called "cyber-hygiene" then it may also improve security, to a point.

But the bad guys are always going to be a step ahead. While governments no doubt want banks to have insurance, part of the motivation may also be to avoid ending up on the hook – just as the Feds have become for terror risks under the Terrorism Risk Insurance Act, which Congress failed to extend before the end of its last session of 2014.

The message to banks and insurers may be to get together and figure out coverage. But the companies involved still need to invest in cyberprotection and detection. Whether from North Korea or elsewhere, the threat will only increase in the coming year.

Richard Beales is assistant editor for Reuters Breakingviews. For more independent commentary and analysis, visit breakingviews.com.