Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Period: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**National Security: Cyber Security**

**North Korea's unsuccessful missile launch 'may have been thwarted by US cyber attack'**

A North Korean missile launch that failed shortly after it was fired may have been thwarted by cyber attacks from the US.

The medium-range missile exploded seconds after it was launched on Sunday from a site near the port city of Sinpo, as Mike Pence, the US vice president, arrived in Seoul for talks with the South Korean government over how to deal with Pyongyang's belligerence.

"It could have failed because the system is not competent enough to make it work, but there is a very strong belief that the US - through cyber methods - has been successful on several occasions in interrupting these sorts of tests and making them fail," the former Conservative foreign secretary Sir Malcolm Rifkind told the BBC on Sunday.

In 2014, former US president Barack Obama ordered that efforts be stepped up to counter North Korea's missile capabilities with cyber attacks and electronic warfare. North Korea has seen a significant increase in failed launches in the years since, though there has been no official claim of the program’s success.

A US foreign policy adviser travelling with Mr. Pence on Air Force Two said the test had come as no surprise.

"We had good intelligence before the launch and good intelligence after the launch," the adviser told reporters on condition of anonymity.

"It's a failed test. It follows another failed test, so really no need to reinforce their failure. We don't need to expend any resources against that."

South Korea's joint chiefs of staff said analysts have not yet identified the type of missile that was launched, but it comes just a day after the North Korean military paraded through the streets of Pyongyang with an array of weapons that included what might be a new generation of intercontinental ballistic missile that is capable of striking the American mainland.

The parade was part of celebrations marking the 105th anniversary of the birth of Kim Il-sung, the founder of the North Korean state, and included a total of 56 missiles of 10 different models.

They included Pukkuksong-1 submarine-launched ballistic missiles, which the regime has been testing off its east coast.

The North's previous attempted missile launch, on April 5, also suffered an in-flight failure before the weapon crashed into the Sea of Japan. "North Korea attempted to test an unidentified type of missile from the Sinpo area in South Hamkyong Province this morning, but we suspect the launch has failed," the South Korean defense ministry said in a statement.

There was also an unsuccessful missile launch in late March.

The US Pacific Command had detected and tracked what it assessed to be a North Korean ballistic missile launch at 11.21am Hawaii time (21.21 GMT) on Saturday, according to US Navy Commander Dave Benham, a spokesman for Pacific Command. Experts have suggested that the United States may be carrying out "left-of-launch" attacks on the missiles using electromagnetic propagation or cyber attacks, including through infected electronics aboard the weapon that confuse its command and control or targeting systems.

"The missile blew up almost immediately. The type of missile is still being assessed," he said.

South Korea will hold a national security meeting about the failed launch later this morning.

President Donald Trump, who is at his Mar-a-Lago retreat in Florida, has been briefed on the latest developments, Jim Mattis, the U.S. Defense Secretary, said.

North Korean state media has made no comment on the launch, which analysts say is normal for the Pyongyang regime when things go awry.

North Korea is subject to United Nations sanctions because of its determination to pursue its nuclear weapons program in defiance of the international community.

It has already carried out five nuclear tests, including two last year, as well as multiple missile launches.

The deployment of the fleet reflects a tougher line being taken by the US. But at the same time, President Trump, who met his Chinese counterpart, Xi Jinping, just over a week ago, hopes that Beijing will be able to rein in Pyongyang.

A Foreign Office spokesman said: "We are concerned by reports of a missile test by North Korea and are monitoring the situation closely."

|  |
| --- |
| List any cyber threats you can think of. In your opinion, how significant are cyber security threats? Explain. |

|  |
| --- |
| Describe your understanding of cyber security: |

|  |
| --- |
| Who might be interested in committing cyber attacks? |

|  |
| --- |
| How significant is cyber security for America (1-10 scale)? Explain. |

**Read the following story**

WASHINGTON — Lawmakers heading the Senate intelligence committee focused squarely on Russia as they opened a hearing Thursday on attempts at undermining the 2016 U.S. presidential election.

“Russian President Vladimir Putin ordered a deliberate campaign carefully constructed to undermine our election,” Virginia Democratic Sen. Mark Warner said.

“Russian President Vladimir Putin ordered a deliberate campaign carefully constructed to undermine our election,” Virginia Democratic Sen. Mark Warner said.

Earlier Thursday, Putin again dismissed what he called “endless and groundless” accusations of Russian meddling in the U.S. election, describing them as part of the U.S. domestic political struggle. He also said he is ready to meet with President Donald Trump at an upcoming arctic summit.

The hearing Thursday is to address how the Kremlin allegedly uses technology to spread disinformation in the U.S. and Europe. Warner and the panel’s chairman, Sen. Richard Burr, R-N.C., provided an update Wednesday of the committee’s investigation into activities Russia might have taken to alter or influence the 2016 elections and whether there were any campaign contacts with Russian government officials that might have interfered with the election process.

“There were upwards of 1,000 paid internet trolls working out of a facility in Russia, in effect, taking over series of computers, which is then called a botnet,” Warner told reporters on Capitol Hill Wednesday.

Warner said the committee is investigating to find out whether voters in key states, such as Wisconsin, Michigan and Pennsylvania, might have been served up Russian-generated fake news and propaganda along with information from their traditional news outlets.

“We are in a whole new realm around cyber that provides opportunity for huge, huge threats to our basic democracy,” Warner said. “You are seeing it right now.”

Burr added that Russians are trying to influence elections in Europe as well.

Rep. Mike Pompeo, Trump's CIA nominee, agrees Russia tried to interfere in election

Russia’s election intervention is ‘new reality, new weapon’

“I think it’s safe by everybody’s judgment that the Russians are actively involved in the French elections,” Burr said. The first round of the French presidential election is to be held next month.

Scheduled to appear at the committee’s open hearing are: Eugene Rumer, director of the Russia and Eurasia program at the Carnegie Endowment for International Peace; Roy Godson, professor of government emeritus at Georgetown University; Clint Watts, senior fellow at the Foreign Policy Research Institute Program on National Security; Kevin Mandia, chief executive officer of the cybersecurity firm FireEye Inc.; and retired Gen. Keith Alexander, former director of the National Security Agency and president of IronNet Cybersecurity.

Pledging cooperation, Burr and Warner said they would steer clear of politics in their panel’s probe of Russian meddling. They made a point of putting themselves at arm’s length from the House investigation that has been marked by partisanship and disputes.

Democrats have called for House intelligence committee Chairman Rep. Devin Nunes to recuse himself because of his ties to the Trump team, especially because the investigation includes looking at contacts that Russians had with President Donald Trump’s associates. Nunes, R-Calif., met with a secret source on the White House grounds last week to review classified material, which he says indicates that Trump associates’ communications were captured in “incidental” surveillance of foreigners. Nunes says he sees no reason to step aside.

Burr said that so far, the Senate committee has requested 20 individuals to be interviewed. Five have been scheduled, and the remaining 15 are likely to be scheduled within the next 10 days. Additional witnesses could also be interviewed.

Burr identified just one of the witnesses: Trump’s son-in-law, Jared Kushner. The White House has said that Kushner, a senior adviser to Trump, has volunteered to answer questions about arranging meetings with the Russian ambassador and other officials.

Asked whether the committee had spoken to former national security adviser Michael Flynn or his representatives, Burr told reporters, “It’s safe to say that we have had conversations with a lot of people, and you would think less of us if Gen. Flynn wasn’t in that list.”

An attorney for Flynn said his client had not yet been interviewed by the Senate committee. One of Flynn’s lawyers, Robert Kelner, said they have had discussions with committee staff members, but Flynn has not been contacted directly.

Trump asked Flynn, a former director of the Defense Intelligence Agency, to step down last month from his post as national security adviser. The president said he made the decision because Flynn had misled Vice President Mike Pence and other White House officials about his conversations with Russia’s ambassador to the U.S.

Notes:

|  |
| --- |
| Definition of Cyber Threats: |

|  |
| --- |
| Statistics: |

|  |
| --- |
| Most frequent categories of Cyber Attacks: |
| Read through the examples of Cyber Attacks. Are there any commonalities between the organizations that have been attacked? |

**2015**

**Bowman Dam (infrastructure)**

Iranian hackers reportedly gained control of this New York dam’s sluice system in 2013, although the controls were manually disconnected at the time of the cyber breach.[3] In March 2016, the Department of Justice (DOJ) indicted one of the hackers employed at an Iran-based computer company with possible ties to the Islamic Revolutionary Guard Corps.[4]

**Hyatt Hotels Corporation (hotel)**

The hotel chain owner announced that it had identified malware on payment processing systems used at a number of locations.[5] Weeks of investigation revealed that malware had affected the systems at 250 locations between August and December 2015.[6] The malware collected payment information specific to credit card information.

**MacKeeper (technology)**

Security researcher Chris Vickery discovered in Shodan (a specialized search engine and online database) the usernames, passwords, and other information for 13 million users of MacKeeper, a performance optimizing software for Apple computers.

**A Whole Lot of Nothing LLC (spam e-mail company)**

The DOJ arrested three men linked to a hacking and scamming scheme that originated as early as 2011. The group targeted the personal information of almost 60 million people—often contained in targeted corporate databases—to be used in spam campaigns. Their operations ultimately generated $2 million in illegal profits.

**Voter records**

Vickery found the information of 191 million registered U.S. voters in a public-facing database.[10] While there were only 142 million register voters in 2014, information in the database goes as far back as 2000—meaning it could still contain the information of deceased registered voters. There also may be instances of duplication from combining multiple databases. As of yet, no one has come forward as the owner of the database.

**Alliance Health (online health portal)**

The online portal that facilitates support and information communities across health providers may have exposed personal health information of its 1.5 million users. The exposure likely came from a misconfiguration with its MongoDB database installation.[11] Forty thousand individuals were eventually informed their information had been exposed for 30 months.[12]

**January 2016**

**Voter records**

Vickery discovered another public-facing database, storing upwards of 56 million voters’ information.[13]

The Wendy’s Company (restaurant). Wendy’s first reported it would be investigating a possible breach that compromised customer payment information at its franchise stores. By June, investigators determined that at least 1,025 Wendy’s locations had been affected, beginning as early as fall 2015.[14]

**February 2016**

**U.S. Department of Homeland Security, Federal Bureau of Investigation (government).**

A hacker with the Twitter handle @DotGovs released online the names and contact information of 29,000 Department of Homeland Security and FBI employees.[15]

**March 2016**

**Verizon Enterprise Solutions (network management).**

One-and-a-half million Verizon Enterprise customers’ contact information was possibly compromised by a security vulnerability. A prominent hacker offered access to the online database for $100,000.[16]

**May 2016**

**LinkedIn (online social networking).**

Updating the impact of a 2012 breach that saw the exposure of 6.5 million users’ passwords, the company confirmed that the true number is now likely closer to 167 million users, 117 million of whom had both their e-mails and passwords exposed.[17]

**Myspace (online social media).**

The same hacker who advertised the compromised LinkedIn database online claim to have a database of Myspace users’ credentials—427 million passwords and 360 million e-mail addresses.[18]

**Noodle & Company (restaurant chain).**

The food chain first began investigating its networks after unusual activity was noticed by its credit card processor. Malware led to customers’ credit and debit card information being compromised at a number of its locations between January and June.[19]

**June 2016**

**Democratic National Committee (political organization).**

The political organization’s networks were illegally accessed by two separate cyber groups with possible affiliation to the Russian government’s Russia Main Intelligence Directorate (GRU) and Federal Security Service (FSB).[20]

Voter information. Chris Vickery found another online database holding 154 million U.S. voters’ information and discovered that an IP address based out of Serbia had been interacting with the database as early as April 2016.[21]

**CiCi’s Pizza (restaurant chain).**

News of this point-of-sale breach affecting customers’ payment information first broke on KrebsOnSecurity. CiCi’s Pizza eventually acknowledged the breach and that the compromise to its systems began as early as March 2016.[22] CiCi’s Pizza has 135 locations.

July 2016

**Citibank (banking).**

Ninety percent of Citibank’s networks across North America were taken offline after an employee in charge of the bank’s IT systems, following a poor performance review, sent malicious code to 10 core Citibank Global Control Center routers, shutting down nine of them. He has since been sentenced to 21 months in federal prison and fined $77,200.[23]

**August 2016**

**Dropbox (online).**

The number of account credentials exposed in a 2012 breach was increased to 68 million users.[24] Hackers were reportedly able to access accounts utilizing a Dropbox employee’s password and credentials, possibly taken from the 2012 LinkedIn breach.[25] Yevgeniy Nikulin was indicted on October 20, 2016, for his involvement with both the Dropbox and LinkedIn breaches.[26]

Banner Health (health care). Almost four million patients, physicians, and customers were affected. The breach was first noticed on July 7, 2016, affecting payment card information. A subsequent breach led to the unauthorized access of patients’ personal identifiable information, such as birthdates, claims information, and possibly social security numbers.[27]

**Oracle MICROS (payment).**

Operator of 330,000 cash registers globally, this point-of-sale service was reportedly infected by malware.[28] The exploit has a possible connection to the Carbanak gang, an Eastern European hacker group linked to stealing $1 billion from up to 100 banks worldwide,[29] and may also have ties to a Russian security firm.[30]

**September 2016**

**Yahoo Inc. (online).**

The online company reported that more than 500 million of its users’ names, e-mail addresses, birthdates, phone numbers, and passwords were compromised in a 2014—possibly state-sponsored—breach. Yahoo began investigating the breach after 280 million users’ information was being offered for sale on the dark web.[31]

SS&C Technology (technology). Tillage Commodities Fund, one of SS&C’s clients, was scammed for $5.9 million by reported Chinese hackers. The hackers sent SS&C staff scam e-mails ordering wire transfers of Tillage’s money.[32]

**October 2016**

**Dyn (online).**

The domain name service server was taken offline a number of times, attributed to widespread denial of service attacks. Internet-facing devices were used in this attack after being formed into a botnet through malware. The outage affected how users could access popular sites such as Twitter, Netflix, and The New York Times.[33]

**U.S. Department of the Treasury, Office of the Comptroller of the Currency (OCC) (government).**

In November 2015, a former employee at the OCC downloaded swaths of information onto two portable storage devices before his retirement, leading to the unauthorized removal of more than 10,000 unclassified records.[34]

**November 2016**

**Friend Finder Networks (online).**

The company behind adult online websites such as Adultfriendfinder.com reported that the accounts of 412 million users were exposed online.[35] The online servers were reportedly breached by hackers in October.[36] No credit card information was exposed, but usernames, e-mails, passwords, and date-of-last-visit became available.

**Conclusion**

This list of successful and notable cyber incidents hardly scratches the surface of the number of smaller attacks or breaches that occur on a daily basis. With this in mind, Congress and the Administration should continue to encourage the sharing of threat information. Either through formal methods with the government and information-sharing centers or through informal communication, threat information sharing can help mitigate the spread of malicious software. The U.S. should continue to improve and encourage the use of existing avenues of information sharing such as those created by the Cybersecurity Act of 2015.[37]

Serious discussions need to take place on how to empower the private sector to engage in more active defense of its networks. The U.S. should create a defined system of active cyber defense that enables private companies to do more to defend their networks. This system should not allow unrestricted “hack back,” but should permit firms to use more assertive cyber tools that improve investigatory and attribution capabilities. Despite the potential threats that malicious actors may pose to U.S. online databases and network systems, the Internet and electronic devices continue to drive the economies of the world. The U.S. needs to take cybersecurity seriously while at the same time allowing innovation to continue to thrive.

—Riley Walters is a Research Associate in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.

|  |
| --- |
| With a partner, come up with a plan to defend against Cyber Attacks: |

<http://www.pbs.org/wgbh/nova/labs/lab/cyber/research#/corp/battle/network/evergreen>