2018-fe54c23c

CYBER NEWS & HIGHLIGHTS: NOVEMBER 14, 2018

Please see below for Full Text (p. 2) and Opinion & Longer reads (p. 8)

- **Russia jammed GPS during major NATO military exercise with US troops,** *CNN, Nov. 14*
  The Russian military jammed GPS signals during a major NATO military exercise in Norway that involved thousands of US and NATO troops, the alliance said Wednesday, citing the Norwegian government. The NATO exercise, Trident Juncture, concluded Sunday and involved some 50,000 personnel. It was labeled the alliance's largest exercise since the Cold War. Non-NATO members Finland and Sweden also participated in the exercise.
  Link to full story here (or see below)

- **Bill cementing cybersecurity agency at DHS heads to Trump's desk,** *The Hill, Nov. 14*
  A bill that will solidify the Department of Homeland Security's (DHS) role as the main federal agency overseeing civilian cybersecurity is heading to President Trump's desk. The House on Tuesday unanimously passed a bill to establish a new cybersecurity agency, known as the Cybersecurity and Infrastructure Security Agency (CISA), that is the same stature as other units within DHS, such as Secret Service or FEMA.
  Link to full story here (or see below)

- **Russian cyber security firm moves away from Moscow after allegations of Kremlin spying,** *Sky News, Nov. 14*
  Russian cyber security firm Kaspersky Lab is moving key parts of its business out of Moscow in a bid to address the risks arising from its exposure to the Russian intelligence services. Last year, the US Department for Homeland Security (DHS) and the UK's National Cyber Security Centre (NCSC) issued warnings regarding the use of Kaspersky software on critical government systems, citing legal powers in Russia, allowing the state to exert control over private companies.
  Link to full story here (or see below)

- **US Air Force moves to fortify F-35 weak points against hacking,** *Defense News, Nov. 14*
  The U.S. Air Force is devoting fresh energy to plugging cybersecurity holes in the F-35's external support systems, as they are deemed the easiest entry points for hackers into the fifth-generation combat jet, according to Brig. Gen. Stephen Jost, director of the Air Force F-35 Integration Office. "It's a software-based aircraft, and any software-based platform is going to be susceptible to hacking," he said.
  Link to full story here (or see below)

- **Congressional panel warns of national security threat from Chinese tech,** *The Hill, Nov. 14*
  A congressional advisory panel warned that internet-linked electronics manufactured in China could pose a national security threat to the United States. The U.S.-China Economic and Security Review Commission on Tuesday explained the dangers of having the U.S.'s public and private sectors rely on supply-chains linked to China.
  Link to full story here (or see below)

Form # b891-4755-9eaa-47d6fb0af943

2018-fe54c23c

---

1. Russia jammed GPS during major NATO military exercise with US troops, *CNN, Nov. 14*

The Russian military jammed GPS signals during a major NATO military exercise in Norway that involved thousands of US and NATO troops, the alliance said Wednesday, citing the Norwegian government.

The NATO exercise, Trident Juncture, concluded Sunday and involved some 50,000 personnel. It was labeled the alliance's largest exercise since the Cold War. Non-NATO members Finland and Sweden also participated in the exercise.

A spokesperson for the Norwegian ministry of defense acknowledged the jamming to CNN, which it said took place between October 16 and November 7, and said it would defer to the Ministry of Foreign Affairs on further questions to Russian authorities.

"Norway has determined that Russia was responsible for jamming GPS signals in the Kola Peninsula during Exercise Trident Juncture. Finland has expressed concern over possible jamming in Lapland," NATO spokesperson Oana Lungescu told CNN Wednesday.

"In view of the civilian usage of GPS, jamming of this sort is dangerous, disruptive and irresponsible," she added.

A US defense official told CNN that the jamming had "little or no affect" on US military assets during the NATO exercise.

Asked about the report of Russian jamming, NATO's Secretary General Jens Stoltenberg said the alliance was aware of the reports but did not offer additional information.

"We have seen there have been similar reports from Norway, and I cannot share more precise information with you," Stoltenberg said Sunday at a news conference marking the end of Trident Juncture.

"What I can say is that we see that cyber, electronic warfare, electronic means are used more and more frequent in different operations, and therefore we take all these issues very seriously," Stoltenberg added.

"The US is keenly aware cyber-attacks and electronic warfare are being used on and off the battlefield with alarmingly greater frequency and severity. We have experienced this in many areas where we operate, and we have observed the potentially devastating impact such measure could pose to civilian aviation," Pentagon spokesman Eric Pahon told CNN in a statement.

Form # b891-4755-9eaa-47d6fb0af943

"We are directly addressing these expanding threats, increasing our ability to deal with these challenges and developing new ways to defend against them," he added.

The Kola Peninsula is close to the Norwegian-Russian border and is where the Russian Navy bases its northern fleet.

Although Norway is a founding member of NATO, Moscow has voiced strong opposition to the presence of NATO and US troops in the country.

2. Bill cementing cybersecurity agency at DHS heads to Trump's desk, *The Hill, Nov. 14*

A bill that will solidify the Department of Homeland Security's (DHS) role as the main federal agency overseeing civilian cybersecurity is heading to President Trump's desk.

The House on Tuesday unanimously passed a bill to establish a new cybersecurity agency, known as the Cybersecurity and Infrastructure Security Agency (CISA), that is the same stature as other units within DHS, such as Secret Service or FEMA.

The bill will also rebrand DHS' main cybersecurity unit, known as National Protection and Programs Directorate (NPPD), as the Cybersecurity and Infrastructure Protection Agency. That means that the headquarters will be a full-fledged operational component of DHS.

The legislation passed the Senate in a unanimous consent vote last month. The Senate had made some changes to an earlier version of the House-passed bill, which required it to be sent back to the lower chamber for final approval.

Members in the House passed the bill Tuesday in the first series of votes following last week's midterm elections.

Top DHS officials have been pushing for the bill to pass, arguing it would better communicate their mission to the private sector and help DHS recruit top cyber talent.

"Today's vote is a significant step to stand up a federal government cybersecurity agency," said DHS Secretary Kirstjen Nielsen said in a statement. "The cyber threat landscape is constantly evolving, and we need to ensure we're properly positioned to defend America's infrastructure from threats digital and physical. It was time to reorganize and operationalize NPPD into the Cybersecurity and Infrastructure Security Agency."

"Elevating the cybersecurity mission within the Department of Homeland Security, streamlining our operations, and giving NPPD a name that reflects what it actually does will help better secure the nation's critical infrastructure and cyber platforms," Krebs said in a statement. "The changes will also improve the Department's ability to engage with industry and government stakeholders and recruit top cybersecurity talent."

Form # b891-4755-9eaa-47d6fb0af943

The bill, which stalled during the Senate earlier this year, is responsible for securing federal networks and protecting critical infrastructure from cyber and physical threats.

NPPD has seen its responsibilities rapidly expand in the decade since its inception, most recently taking the lead on engaging with states to protect digital election infrastructure from sabotage following Russian interference in the 2016 election.

3. **Russian cyber security firm moves away from Moscow after allegations of Kremlin spying,** *Sky News, Nov. 14*

Russian cyber security firm Kaspersky Lab is moving key parts of its business out of Moscow in a bid to address the risks arising from its exposure to the Russian intelligence services.

Last year, the US Department for Homeland Security (DHS) and the UK's National Cyber Security Centre (NCSC) issued warnings regarding the use of Kaspersky software on critical government systems, citing legal powers in Russia, allowing the state to exert control over private companies.

The warnings left Kaspersky Lab needing to reassure customers that their data was handled properly in what it has called a global transparency initiative.

Crucial parts of its customer data processing and software production are being relocated to an automated data centre in a secured facility in the privacy haven of Zurich, where they will be open for inspection and audit by trusted third parties.

None of Kaspersky Lab's R&D staff will be based in Switzerland however. The company's vice president of public policy, Anton Shingarev, explained to Sky News that only certain automated parts of its infrastructure were being moved there - being hosted by the NYSE-listed Interxtion.

Despite NCSC's statement that it was working with Kaspersky Lab to develop a plan to prevent any UK data being captured by the Russian state, the company has instead offered, Mr Shingarev said, "a framework which is suicidal for us in case of abuse".

"If anything happens, it's going to be found sooner or later. And we intentionally - by ourselves, with our hands -[are creating] such a system."

This does not meet the standard of 100% proof that any transfers would be prevented, the VP acknowledged, but he claimed it did meet the NCSC's standards for a risk-based approach towards the company's software.

Robert Pritchard, who formerly worked for the UK government and has since founded the Cyber Security Expert consultancy, noted that Kaspersky Lab's products weren't being criticised in general and were well-thought of in the community.

Form # b891-4755-9eaa-47d6fb0af943

"I think it was a shame that the NCSC's announcement was misinterpreted," he told Sky News, adding that on non-sensitive networks the company's products were not an issue.

That said, he added: "I have worked with clients who have very good reason to fear they're being targeted by Russian foreign intelligence, and I would encourage them to not use Kaspersky."

At a launch event celebrating the beginning of European customers' data being processed in Zurich, Mr Shingarev denounced what he saw as growing "tech nationalism" around the world with products being banned because of their country of origin, but said Kaspersky Lab would have to find a way to overcome it regardless.

The company's infrastructure, which has been moved, was implicated in media reports alleging the firm's anti-virus product was used by the Kremlin to steal secret US hacking tools from the computer of a National Security Agency employee who had illegally taken them home.

By moving them to Zurich and keeping an audit record of all of Kaspersky Lab's Moscow-based staff's interactions with them, the company aims to preclude allegations that the Russian state could secretly interfere with its business.

Saying that the data cannot be accessed in secret is not same as saying it cannot be got at at all, and it is not clear how reassured the company's government customers will be by the proposed transparency facility.

Mr Shingarev told Sky News: "How can [the code review] guarantee that there is no GRU, GCHQ, CIA - name them - spies in our company? It's almost impossible to have a 100% guarantee.

!Of course we've got all these checks, of course we've got audits, of course we've got all these matters, but there is no simple fast solution to remove the risk," he added.

"That's why in the risk-based paradigm we are trying to reduce the risk by a few measures. Reviewing the source code is one of the measures that helps, an independent audit another measure, data centre here another measure.

"Having all these measures we are trying to reduce the risk, reduce the window of opportunity for abusers, and to guarantee as much security as possible."

Form # b891-4755-9eaa-47d6fb0af943

4. US Air Force moves to fortify F-35 weak points against hacking, *Defense News, Nov. 14*

The U.S. Air Force is devoting fresh energy to plugging cybersecurity holes in the F-35's external support systems, as they are deemed the easiest entry points for hackers into the fifth-generation combat jet, according to a key service official.

"It's a software-based aircraft, and any software-based platform is going to be susceptible to hacking," Brig. Gen. Stephen Jost, director of the Air Force F-35 Integration Office, told Defense News in an interview at the International Fighter industry conference here.

The service considers the information backbone of the actual airplane – managed by manufacturer Lockheed Martin – relatively safe. That is thanks to what Jost called "multilayer security protections" ranging from secure authentication when crafting mission data packages for each aircraft before takeoff, to pilots punching in personal identification numbers to start up the plane.

The confidence wanes "as you get further from the air vehicle," Jost said. When taking into account systems like the Autonomic Logistics Information System or the Joint Reprogramming Environment, there are "a lot of nodes of vulnerability that we're trying to shore up," he added.

The Autonomic Logistics Information System, or ALIS, is a key application meant to provide unprecedented automation in monitoring the status of the aircraft's components. The Joint Reprogramming Enterprise refers to government software labs compiling collections of updated threat characteristics – Russian tanks, for example – for upload into the aircraft so that its sensors can recognize targets.

Additionally, officials worry about cyber-hardening F-35 flight simulators, which could be attractive targets for hackers seeking information about the plane. The introduction of wireless applications for easier maintenance on the flight line also could pose new vulnerabilities that must be addressed, Jost said.

The Government Accountability Office published a report in October warning warned about cyber vulnerabilities in almost all of the Defense Department's weapons. The shortfalls exist because many systems were conceived at a time when cyber attacks were still in their infancy.

"In operational testing, DOD routinely found mission-critical cyber vulnerabilities in systems that were under development, yet program officials GAO met with believed their systems were secure and discounted some test results as unrealistic," auditors wrote. "Using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected, due in part to basic issues such as poor password management and unencrypted communications."

Form # b891-4755-9eaa-47d6fb0af943

A key examination phase for the F-35 program, called initial operational test and evaluation, was set to begin to this week. The test plan, required for all major programs, typically includes a regimen of cyber probing.

5. Congressional panel warns of national security threat from Chinese tech, *The Hill, Nov. 14*

A congressional advisory panel warned that internet-linked electronics manufactured in China could pose a national security threat to the United States.

The U.S.-China Economic and Security Review Commission on Tuesday explained the dangers of having the U.S.'s public and private sectors rely on supply-chains linked to China.

China is the world's largest information technology product manufacturer, making its reach difficult to avoid. Still, the commission suggested that finding alternate suppliers might be necessary.

"The scale of Chinese state support for the IoT and 5G, the close supply chain integration between the United States and China, and China's role as an economic and military competitor to the United States create enormous economic, security, supply chain, and data privacy risks for the United States," the report read.

The report also warned that the rapid pace at which China is building out 5G broadband infrastructure compared to the U.S. could exacerbate the threat by making internet data-enabled products, or internet of things, more open to potential attacks.

"The rapid proliferation of unsecure IoT devices is increasing the avenues Chinese actors could exploit to deny service, collect intelligence, or launch a cyber attack," it reads. "The large amount of data collected by the ever growing number of IoT devices, the value of such data to criminal and state actors such as China, and lax U.S. security and legal protections are worsening privacy, safety, and security risks for U.S. citizens, businesses, and democracy."

The growing threat of Chinese technology has been a concern for both Democrats and Republicans in office. Lawmakers on both sides of the aisle, as government agencies have pursued policies to keep Chinese technology out of the government and military.

Their focus has been on telecommunications companies including ZTE and Huawei who have been expanding their 5G networks around the world, however many American technology companies, including some that work with the government, U.S. technology at least partially manufactured in China.

Form # b891-4755-9eaa-47d6fb0af943

2018-fe54c23c

Opinion and Longer Reads:

- **How ZTE helps Venezuela create China-style social control,** *Reuters, Nov. 14*
  Link to full story here

- **Pentagon Researchers Test 'Worst-Case Scenario' Attack on U.S. Power Grid,** *Next Gov., Nov. 13*
  Link to full story here

- **DoD and the Cloud: Moving Out Bureaucracy to Focus on National Security,** *Real Clear Defense, Nov. 14*
  Link to full story here

- **Grid planners put 'black start' technology to the test,** *E and E News, Nov. 13*
  Link to full story here

** Do not distribute outside DoD without permission of the USCYBERCOM Public Affairs Office. The summaries provided are drawn from publicly available media sources and are intended solely to inform DoD personnel regarding current cyber-related media trends. These summaries are not intended to state or imply any official USCYBERCOM position or representation regarding any matter, nor are they intended to state or imply official endorsement of any referenced media source or other non-U.S. government entity. USCYBERCOM makes no representation or guarantee regarding the accuracy and/or currency of the information as reported by the referenced sources. USCYBERCOM does not claim or assert any rights in the referenced source material. **

Form # b891-4755-9eaa-47d6fb0af943