1833, the DHS Industrial Control Systems Capabilities Enhancement Act of 2021.

As I have said from day one as ranking member of this committee, we need to continue to bolster cybersecurity capabilities at CISA to defend our Federal networks and the Nation's critical infrastructure from cyber threats.

The volume of cyberattacks and ransomware attacks in 2021 alone shows that no one is immune from nation-state cyber actors or cyber criminals. Cyber threats, particularly ransomware, are the preeminent national security threat facing our Nation today. From Colonial Pipeline to a local water facility in Florida, we have witnessed the real-world consequences cyberattacks can have on our critical infrastructure.

In the cyberattack against a water treatment plant in Florida, hackers were able to gain access to industrial control systems, or ICS for short, and attempted to alter the mixture of water chemicals to what could have been catastrophic fatal levels.

Cyber incidents are very rarely sector specific. CISA is a central agency that can quickly connect the dots when a malicious cyber campaign spans multiple sectors. It is vital that we continue to enhance its visibility across the critical infrastructure ecosystem.

This bill requires the CISA director to maintain capabilities to detect and mitigate threats and vulnerabilities affecting automated control of critical infrastructure, particularly industrial control systems.

This includes maintaining cross-sector incident response capabilities to respond to cybersecurity incidents and providing cybersecurity technical assistance to stakeholders.

We must continue to solidify CISA's lead role in protecting our Nation's critical infrastructure from cyber threats, particularly the industrial control systems that underpin vital components of our daily lives.

This bill is one step in the committee's continued efforts to build up CISA's authorities and resources to effectively carry out its mission, and it is a resounding statement to have such heavy-hitting, bipartisan support.

Madam Speaker, I urge all Members to join me in supporting H.R. 1833, and I reserve the balance of my time.

Ms. CLARKE of New York. Madam Speaker, I have no further speakers, and I am prepared to close after the gentleman from New York closes. I reserve the balance of my time.

Mr. KATKO. Madam Speaker, I have no further speakers. I urge Members to support this bill. I yield back the balance of my time.

Ms. CLARKE of New York. Madam Speaker, I yield myself the balance of my time to close.

I would like to start by thanking the gentleman from New York for his outstanding leadership in this regard.

Industrial control systems are a rich target for cyber adversaries looking to disrupt, extort, and simply wreak havoc. These systems underpin the functions and services we rely on for our day-to-day lives, and the threats they face have never been higher.

Successful disruption of one of these systems could have dire consequences for public health and safety, public confidence, and even the national and economic security of the United States.

CISA is well-positioned to help owners and operators better understand risks to operational technology and work with them to close security gaps.

I again want to congratulate the gentleman from New York (Mr. KATKO), my committee colleague and ranking member, on authoring this bill to codify the role that CISA plays in leading Federal efforts to secure industrial control systems.

Enactment of H.R. 1833 will help to raise our cybersecurity posture across the board.

Madam Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from New York (Ms. CLARKE) that the House suspend the rules and pass the bill, H.R. 1833, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. BISHOP of North Carolina. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

CYBERSECURITY VULNERABILITY REMEDIATION ACT

Ms. CLARKE of New York. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 2980) to amend the Homeland Security Act of 2002 to provide for the remediation of cybersecurity vulnerabilities, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2980

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cybersecurity Vulnerability Remediation Act''.

SEC. 2. CYBERSECURITY VULNERABILITIES.

Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking ''and'' after the semicolon at the end;

(B) by redesignating paragraph (6) as paragraph (7); and

(C) by inserting after paragraph (5) the following new paragraph:

''(6) the term 'cybersecurity vulnerability' has the meaning given the term 'security vulnerability' in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and''.

(2) in subsection (c)—

(A) in paragraph (5)—

(i) in subparagraph (A), by striking ''and'' after the semicolon at the end;

(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting after subparagraph (A) the following new subparagraph:

''(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n); and''; and

(iv) in subparagraph (C), as so redesignated, by inserting ''and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B)'' before ''with Federal'';

(B) in paragraph (7)(C), by striking ''sharing'' and inserting ''share''; and

(C) in paragraph (9), by inserting ''mitigation protocols to counter cybersecurity vulnerabilities,'' after ''measures,'';

(3) in subsection (e)(1)(G), by striking the semicolon after ''and'' at the end;

(4) by redesignating subsection (o) as subsection (p); and

(5) by inserting after subsection (n) following new subsection:

''(o) PROTOCOLS TO COUNTER CERTAIN CYBERSECURITY VULNERABILITIES.—The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.''.

SEC. 3. REPORT ON CYBERSECURITY VULNERABILITIES.

(a) REPORT.—Not later than one year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on how the Agency carries out subsection (n) of section 2209 of the Homeland Security Act of 2002 to coordinate vulnerability disclosures, including disclosures of cybersecurity vulnerabilities (as such term is defined in such section), and subsection (o) of such section (as added by section 2) to disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, that includes the following:

(1) A description of the policies and procedures relating to the coordination of vulnerability disclosures.

(2) A description of the levels of activity in furtherance of such subsections (n) and (o) of such section 2209.

(3) Any plans to make further improvements to how information provided pursuant to such subsections can be shared (as such term is defined in such section 2209) between the Department and industry and other stakeholders.

(4) Any available information on the degree to which such information was acted upon by industry and other stakeholders.

(5) A description of how privacy and civil liberties are preserved in the collection, retention, use, and sharing of vulnerability disclosures.

(b) FORM.—The report required under subsection (b) shall be submitted in unclassified form but may contain a classified annex.

SEC. 4. COMPETITION RELATING TO CYBERSECURITY VULNERABILITIES.

The Under Secretary for Science and Technology of the Department of Homeland Security, in consultation with the Director of the

Cybersecurity and Infrastructure Security Agency of the Department, may establish an incentive-based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities (as such term is defined in section 2209 of the Homeland Security Act of 2002, as amended by section 2) to information systems (as such term is defined in such section 2209) and industrial control systems, including supervisory control and data acquisition systems.

SEC. 5. TITLE XXII TECHNICAL AND CLERICAL AMENDMENTS.

(a) TECHNICAL AMENDMENTS.—

(1) HOMELAND SECURITY ACT OF 2002.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(A) in the first section 2215 (6 U.S.C. 665; relating to the duties and authorities relating to .gov internet domain), by amending the section enumerator and heading to read as follows:

"SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV INTERNET DOMAIN.";

(B) in the second section 2215 (6 U.S.C. 665b; relating to the joint cyber planning office), by amending the section enumerator and heading to read as follows:

"SEC. 2216. JOINT CYBER PLANNING OFFICE.";

(C) in the third section 2215 (6 U.S.C. 665c; relating to the Cybersecurity State Coordinator), by amending the section enumerator and heading to read as follows:

"SEC. 2217. CYBERSECURITY STATE COORDINATOR.";

(D) in the fourth section 2215 (6 U.S.C. 665d; relating to Sector Risk Management Agencies), by amending the section enumerator and heading to read as follows:

"SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.";

(E) in section 2216 (6 U.S.C. 665e; relating to the Cybersecurity Advisory Committee), by amending the section enumerator and heading to read as follows:

"SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE."; and

(F) in section 2217 (6 U.S.C. 665f; relating to Cybersecurity Education and Training Programs), by amending the section enumerator and heading to read as follows:

"SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.".

(2) CONSOLIDATED APPROPRIATIONS ACT, 2021.—Paragraph (1) of section 904(b) of division U of the Consolidated Appropriations Act, 2021 (Public Law 116–260) is amended, in the matter preceding subparagraph (A), by inserting ''of 2002'' after ''Homeland Security Act''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the items relating to sections 2214 through 2217 and inserting the following new items:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint cyber planning office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity Education and Training Programs.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from New York (Ms. CLARKE) and the gentleman from New York (Mr. KATKO) each will control 20 minutes.

The Chair recognizes the gentlewoman from New York.

GENERAL LEAVE

Ms. CLARKE of New York. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from New York?

There was no objection.

Ms. CLARKE of New York. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, 5 years ago a Government Accountability Office survey found that 12 out of 12 Federal agencies used obsolete information technology. In other words, 12 out of 12 Federal agencies were using software or hardware for which vendors no longer provided support, updates, or patches.

The Federal Government is hardly alone. It has been widely reported that State and local governments and critical infrastructure owners and operators across the country rely on legacy technology.

We have seen malicious cyber actors wreak havoc by exploiting known vulnerabilities.

H.R. 2980 would authorize CISA to develop and distribute playbooks to provide procedures and mitigation strategies for the most critical, known vulnerabilities, especially those affecting software or hardware that is no longer supported by a vendor. The playbooks would be available to Federal agencies, industry, and other stakeholders.

The bill, as introduced by the gentlewoman from Texas (Ms. JACKSON LEE), also authorizes the Department of Homeland Security Science and Technology Directorate, in consultation with CISA, to establish a competition program for industry, individuals, academia, and others to provide remediation solutions for cybersecurity vulnerabilities that are no longer supported.

Importantly, in response to recent cyberattacks, H.R. 2980 prioritizes efforts to address vulnerabilities of industrial control systems of critical infrastructure that may be targeted, like water systems and pipelines.

H.R. 2980 is no substitute for investing in new technology, but it will provide important support to government and private sector entities that cannot replace legacy technology or rapidly patch known vulnerabilities because of resource limitations or other system complications.

Madam Speaker, I urge all of my colleagues to support H.R. 2980, and I reserve the balance of my time.

Mr. KATKO. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 2980, the Cybersecurity Vulnerability Remediation Act. I would like to thank the gentlewoman from Texas (Ms. JACKSON LEE), my friend, for being a staunch advocate of CISA and these important cybersecurity issues. I look forward to continuing to work with her and my other colleagues on the preeminent national security threat facing our Nation today.

Madam Speaker, I urge Members to join me in supporting H.R. 2980, and I reserve the balance of my time.

Ms. CLARKE of New York. Madam Speaker, I yield 5 minutes to the gentlewoman from Texas (Ms. JACKSON LEE).

Ms. JACKSON LEE. Madam Speaker, I thank the gentlewoman from New York for her leadership, and I thank the ranking member of the full committee and the chair of the full committee for bringing these matters to the attention of the Nation.

Madam Speaker, I rise in support of my bill, H.R. 2980, the Cybersecurity Vulnerability Remediation Act, which authorizes the Department of Homeland Security to take actions to counter cybersecurity vulnerabilities in our Nation's critical infrastructure.

Interestingly enough, when we introduced this bill some years ago, we called it the zero-day bill, which was to presuppose what would happen when everything collapsed. When we introduced it, it was before the Colonial Pipeline, it was before the Solaris attack, it was before knowing about the gangs in Russia, cyber gangs that proliferate before the activity of China.

I thank Chairman THOMPSON and Ranking Member KATKO for their leadership in putting the security of our Nation's cyber access first, whether they are computing resources used in voting technology or industrial control systems that support delivery of electricity, oil, and gas, or management of transportation systems that are vital to our Nation's economic health.

The Cybersecurity Vulnerability Remediation Act was introduced, as I said, and passed the House during the 115th and 116th Congresses and has been updated again in the 117th Congress to meet the ever-evolving nature of cyber threats faced by Federal and private sector information systems and our Nation's critical infrastructure.

As I said before, it will be very important that the other body seriously considers the cyber threats against this Nation. This bill goes significantly further than the first cybersecurity vulnerability act that I introduced in the 115th Congress to address the instance of zero-day events that can lead to catastrophic cybersecurity failures of information and computing systems.

It is estimated that 85 percent of critical infrastructure is owned by the private sector, and for far too long this fact has hampered efforts to establish stronger requirements for cybersecurity by owners and operators.

Private sector critical infrastructure failure due to a cyberattack is no longer a private matter when it can have massive impacts on the public, such as disruption of gasoline flowing to filling stations, which we saw recently.

My bill, the Cybersecurity Vulnerability Remediation Act, will expand

the definition of security vulnerability to include cybersecurity vulnerability; add sharing mitigation protocols to counter cybersecurity vulnerabilities; establish protocols to counter cybersecurity vulnerabilities involving information system and industrial control systems, which will include vulnerabilities related to software or hardware that is no longer supported by a vendor; direct the undersecretary for DHS Office of Science and Technology to stand up a competition to find solutions to known cybersecurity vulnerabilities; provide greater transparency on how the Department of Homeland Security CISA is coordinating cybersecurity vulnerability disclosures through the sharing of actionable protocols to mitigate cybersecurity vulnerabilities with information systems and industrial control systems owners and operators.

□ 1330

H.R. 2980 bolsters the efforts to engage critical infrastructure owners and operators in communicating cybersecurity threats and lays the foundation for greater transparency on the real threats posed by cyberterrorists to private and government sector critical infrastructure and information systems, which impact the people of this Nation.

This legislation allows the science and technology director, in consultation with CISA, to establish an incentive-based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities to information systems and industrial control systems, including supervisory control and data acquisition systems.

This bill, when it becomes law, will put our Nation's best minds to work on closing the vulnerabilities that cyber thieves and terrorists use to access, disrupt, corrupt, or take control of critical infrastructure information systems.

In addition to these changes, the bill requires a report to Congress that may contain a classified annex.

The report will provide information on how DHS coordinates cybersecurity vulnerability disclosures and disseminates actionable protocols to mitigate cybersecurity vulnerabilities involving information systems and industrial systems.

Congress needs to know how prevalent and persistent cybersecurity threats targeting critical infrastructure and information systems might be, especially if those threats result in a payment of ransom. They need to know about a payment of ransom.

Paying a ransom for ransomware emboldens and encourages bad cyber actors and places everyone at greater risk for the financial and societal costs of increases in threats as others seek payouts.

The SPEAKER pro tempore. The time of the gentlewoman has expired.

Ms. CLARKE of New York. Madam Speaker, I yield the gentlewoman an additional 1 minute.

Ms. JACKSON LEE. Madam Speaker, as long as there is silence about cyberattacks like ransomware, the criminals and terrorists will remain out of reach and continue to feel safe and emboldened in carrying out these attacks, often from the soil of our enemies or peer competitors.

I applaud and thank the Biden administration for its quick action in responding to the attack against Colonial Pipeline, but it did shut down the whole East Coast, and he did it by an executive order.

Today, our Nation is in a cybersecurity crisis. The attacks against Federal, State, local, territorial, and Tribal Governments, as well as threats posed to private information systems and critical information systems make this bill necessary.

So I am hoping, along with those who have been attacked, like the Metropolitan Police Department, the medical system in Houston—the gang known as the Babuk group released thousands of Metropolitan Police sensitive documents, and it goes on and on.

Madam Speaker, I include in the RECORD four articles regarding this issue.

[From the Forbes Magazine, July 20, 2021]

TURNING UP THE HEAT: A RANSOMWARE ATTACK ON CRITICAL INFRASTRUCTURE IS A NIGHTMARE SCENARIO

(By Richard Tracy, Forbes Councils Member)

Ransomware attacks in 2020 were up more than 150% compared to the previous year, while ransomware payments were up over 300%.

Over the past six months, we've seen a number of ransomware attacks against critical infrastructure—from a water treatment facility to a gas pipeline and multiple food distribution companies—all of which present clear and present danger to society. The impact was so dire—with recent research finding over seven ransomware attacks per hour—that the Department of Justice elevated ransomware attacks to a similar priority as terrorism.

The recent Colonial Pipeline hack, in particular, appears to have struck a nerve, as there is finally discussion about cybersecurity standards for the pipeline industry. That would be a good start and one that is long overdue considering the importance of fuel distribution for our economy and overall way of life.

However, the oil and gas industry is just one element in a single critical infrastructure sector—the energy sector. DHS has defined sixteen critical infrastructure sectors, and each is deemed critical for the proper functioning of our society. Due to the connected nature of everything these days, each sector is a potential cyber target. Disruption to any critical infrastructure segment has potentially dire economic, safety and national security consequences. As such, it only makes sense to address cybersecurity risk management for all sectors, not just oil and gas.

The threat goes beyond the pipeline.

To better understand the need to focus on all critical infrastructure, let's look at the power grid. Imagine a ransomware attack against the power grid that services highly populated areas in the desert southwest. Now, imagine this attack takes place during the hottest part of the summer.

Think about the heat-related deaths that would likely occur and the impact on medical supplies that require refrigeration. Yes, there are generator backups in hospitals where supplies are stored, but we already know from the pipeline hack that the fuel needed to run these generators can be disrupted too. It's also important to note that hospitals, also considered critical infrastructure, have also suffered from ransomware attacks. In fact, hospitals have had an even bigger target on their backs in recent months. The connected nature of our critical infrastructure compounds the problem and potential impacts.

To further illustrate how important the power grid is to our citizens, Protect Our Power, an independent, non-profit advocacy and educational organization focused solely on driving increased resilience of the U.S. electric grid to attacks, recently conducted a public opinion poll of 1,095 Americans. Most notably, the study found:

86 percent of Americans are concerned that the grid is vulnerable to a serious cyberattack.

70 percent say they would feel unsafe in the event of an extended power outage of two weeks or more.

66 percent believe their quality of life will suffer from an outage lasting more than seven days.

64 percent say they are unprepared for an extended power outage that will last more than two weeks.

70 percent say the infrastructure bill should include funding to address this important issue.

Only 16 percent believe the federal government is doing all it can to prevent an attack on the grid.

As most Americans agree, the federal government can and should do more to help secure all of our critical infrastructures.

Recent ransomware attacks against critical infrastructure help us understand standards and practices that would have helped. For example, multi-factor authentication (MFA), a widely recognized best practice, may have prevented the Colonial Pipeline hack. According to GAO, greater and more consistent adoption of the NIST CSF, which was specifically developed to help critical infrastructure manage cyber risk, would benefit cyber risk management efforts across all critical infrastructure sectors.

In summary, we need to secure all critical infrastructure sectors. The power grid example used here illustrates how dire the consequences could be. It's time to move. Summer is upon us, and the desert southwest is getting hot.

[From the New York Times, July 19, 2021]

U.S. FORMALLY ACCUSES CHINA OF HACKING MICROSOFT

(By Zolan Kanno-Youngs, David E. Sanger)

WASHINGTON.—The Biden administration on Monday formally accused the Chinese government of breaching Microsoft email systems used by many of the world's largest companies, governments and military contractors, as the United States joined a broad group of allies, including all NATO members, to condemn Beijing for cyberattacks around the world.

The United States accused China for the first time of paying criminal groups to conduct large-scale hackings, including ransomware attacks to extort companies for millions of dollars, according to a statement from the White House. Microsoft had pointed to hackers linked to the Chinese Ministry of State Security for exploiting holes in the company's email systems in March; the U.S. announcement on Monday morning was the first suggestion that the Chinese government hired criminal groups to hack tens of thousands of computers and networks around the

world for ''significant remediation costs for its mostly private sector victims,'' according to the White House.

Secretary of State Antony J. Blinken said in a statement on Monday that China's Ministry of State Security ''has fostered an ecosystem of criminal contract hackers who carry out both state-sponsored activities and cybercrime for their own financial gain.''

''These contract hackers cost governments and businesses billions of dollars in stolen intellectual property, ransom payments, and cybersecurity mitigation efforts, all while the MSS had them on its payroll,'' Mr. Blinken said.

Condemnation from NATO and the European Union is unusual, because most of their member countries have been deeply reluctant to publicly criticize China, a major trading partner. But even Germany, whose companies were hit hard by the hacking of Microsoft Exchange—email systems that companies maintain on their own, rather than putting them in the cloud—cited the Chinese government for its work.

''We call on all states, including China, to uphold their international commitments and obligations and to act responsibly in the international system, including in cyberspace,'' according to a statement from NATO.

Despite the broadside, the announcement lacked sanctions similar to ones that the White House imposed on Russia in April, when it blamed the country for the extensive SolarWinds attack that affected U.S. government agencies and more than 100 companies. (The Justice Department on Friday did unseal an indictment from May charging for Chinese residents with a campaign to hack computer systems of dozens of companies, universities and government entities in the United States between 2011 and 2018. The hackers developed front companies to hide any role the Chinese government had in backing the operation, according to the Justice Department.)

By imposing sanctions on Russia and organizing allies to condemn China, the Biden administration has delved deeper into a digital Cold War with its two main geopolitical adversaries than at any time in modern history.

While there is nothing new about digital espionage from Russia and China—and efforts by Washington to block it—the Biden administration has been surprisingly aggressive in calling out both countries and organizing a coordinated response.

But so far, it has not yet found the right mix of defensive and offensive actions to create effective deterrence, most outside experts say. And the Russians and the Chinese have grown bolder. The SolarWinds attack, one of the most sophisticated ever detected in the United States, was an effort by Russia's lead intelligence service to alter code in widely used network-management software to gain access to more than 18,000 businesses, federal agencies and think tanks.

China's effort was not as sophisticated, but it took advantage of a vulnerability that Microsoft had not discovered and used it to conduct espionage and undercut confidence in the security of systems that companies use for their primary communications. It took the Biden administration months to develop what officials say is ''high confidence'' that the hacking of the Microsoft email system was done at the behest of the Ministry of State Security, the senior administration official said, and abetted by private actors who had been hired by Chinese intelligence.

The last time China was caught in such broad-scale surveillance was in 2014, when it stole more than 22 million security-clearance files from the Office of Personnel Management, allowing a deep understanding of the lives of Americans who are cleared to keep the nation's secrets.

President Biden has promised to fortify the government, making cybersecurity a focus of his summit meeting in Geneva with President Vladimir V. Putin of Russia last month. But his administration has faced questions about how it will also address the growing threat from China, particularly after the public exposure of the Microsoft hacking.

Speaking to reporters on Sunday, the senior administration official acknowledged that the public condemnation of China would only do so much to prevent future attacks.

''No one action can change China's behavior in cyberspace,'' the official said. ''And neither could just one country acting on its own.''

But the decision not to impose sanctions on China was also telling: It was a step many allies would not agree to take.

Instead, the Biden administration settled on corralling enough allies to join the public denunciation of China to maximize pressure on Beijing to curtail the cyberattacks, the official said.

The joint statement criticizing China, to be issued by the United States, Australia, Britain, Canada, the European Union, Japan and New Zealand, is unusually broad. It is also the first such statement from NATO publicly targeting Beijing for cybercrimes.

The European Union condemned on Monday ''malicious cyberactivities'' undertaken from the Chinese territory but stopped short of denouncing the responsibility of the Chinese government.

''This irresponsible and harmful behavior resulted in security risks and significant economic our loss for government institutions and private companies, and has shown significant spillover and systemic effects for our security, economy and society at large,'' Josep Borrell Fontelles, the E.U.'s foreign policy chief, said in a statement. ''These activities can be linked to the hacker groups,'' the statement added.

Mr. Borrell called on Chinese authorities not to allow ''its territory to be used'' for such activities, and to ''take all appropriate measures and reasonably available and feasible steps to detect, investigate and address the situation.''

The National Security Agency, F.B.I. and Cybersecurity and Infrastructure Security Agency also issued an advisory on Monday warning that Chinese hacking presented a ''major threat'' to the United States and its allies. China's targets include ''political, economic, military, and educational institutions, as well as critical infrastructure.''

Criminal groups hired by the government aim to steal sensitive data, critical technologies and intellectual properties, according to the advisory.

The F.B.I. took an unusual step in the Microsoft hacking: In addition to investigating the attacks, the agency obtained a court order that allowed it to go into unpatched corporate systems and remove elements of code left by the Chinese hackers that could allow follow-up attacks. It was the first time that the F.B.I. acted to remediate an attack as well as investigate its perpetrators.

[From the New York Times, Updated June 8, 2021]

PIPELINE ATTACK YIELDS URGENT LESSONS ABOUT U.S. CYBERSECURITY

(By David E. Sanger, Nicole Perlroth)

For years, government officials and industry executives have run elaborate simulations of a targeted cyberattack on the power grid or gas pipelines in the United States, imagining how the country would respond.

But when the real, this-is-not-a-drill moment arrived, it didn't look anything like the war games.

The attacker was not a terror group or a hostile state like Russia, China or Iran, as had been assumed in the simulations. It was a criminal extortion ring. The goal was not to disrupt the economy by taking a pipeline offline but to hold corporate data for ransom.

The most visible effects—long lines of nervous motorists at gas stations—stemmed not from a government response but from a decision by the victim, Colonial Pipeline, which controls nearly half the gasoline, jet fuel and diesel flowing along the East Coast, to turn off the spigot. It did so out of concern that the malware that had infected its back-office functions could make it difficult to bill for fuel delivered along the pipeline or even spread into the pipeline's operating system.

What happened next was a vivid example of the difference between tabletop simulations and the cascade of consequences that can follow even a relatively unsophisticated attack. The aftereffects of the episode are still playing out, but some of the lessons are already clear, and demonstrate how far the government and private industry have to go in preventing and dealing with cyberattacks and in creating rapid backup systems for when critical infrastructure goes down.

In this case, the long-held belief that the pipeline's operations were totally isolated from the data systems that were locked up by DarkSide, a ransomware gang believed to be operating out of Russia, turned out to be false. And the company's decision to turn off the pipeline touched off a series of dominoes including panic buying at the pumps and a quiet fear inside the government that the damage could spread quickly.

A confidential assessment prepared by the Energy and Homeland Security Departments found that the country could only afford another three to five days with the Colonial pipeline shut down before buses and other mass transit would have to limit operations because of a lack of diesel fuel. Chemical factories and refinery operations would also shut down because there would be no way to distribute what they produced, the report said.

And while President Biden's aides announced efforts to find alternative ways to haul gasoline and jet fuel up the East Coast, none were immediately in place. There was a shortage of truck drivers, and of tanker cars for trains.

''Every fragility was exposed,'' Dmitri Alperovitch, a co-founder of CrowdStrike, a cybersecurity firm, and now chairman of the think tank Silverado Policy Accelerator. ''We learned a lot about what could go wrong. Unfortunately, so did our adversaries.''

The list of lessons is long. Colonial, a private company, may have thought it had an impermeable wall of protections, but it was easily breached. Even after it paid the extortionists nearly $5 million in digital currency to recover its data, the company found that the process of decrypting its data and turning the pipeline back on again was agonizingly slow, meaning it will still be days before the East Coast gets back to normal.

''This is not like flicking on a light switch,'' Mr. Biden said Thursday, noting that the 5,500-mile pipeline had never before been shut down.

For the administration, the event proved a perilous week in crisis management. Mr. Biden told aides, one recalled, that nothing could wreak political damage faster than television images of gas lines and rising prices, with the inevitable comparison to Jimmy Carter's worse moments as president.

Mr. Biden feared that, unless the pipeline resumed operations, panic receded and price gouging was nipped in the bud, the situation

would feed concerns that the economic recovery is still fragile and that inflation is rising.

Beyond the flurry of actions to get oil moving on trucks, trains and ships, Mr. Biden published a long-gestating executive order that, for the first time, seeks to mandate changes in cybersecurity.

And he suggested that he was willing to take steps that the Obama administration hesitated to take during the 2016 election hacks—direct action to strike back at the attackers.

''We're also going to pursue a measure to disrupt their ability to operate,'' Mr. Biden said, a line that seemed to hint that United States Cyber Command, the military's cyberwarfare force, was being authorized to kick DarkSide off line, much as it did to another ransomware group in the fall ahead of the presidential election.

Hours later, the group's internet sites went dark. By early Friday, DarkSide, and several other ransomware groups, including Babuk, which has hacked Washington D.C.'s police department, announced they were getting out of the game.

DarkSide alluded to disruptive action by an unspecified law enforcement agency, though it was not clear if that was the result of U.S. action or pressure from Russia ahead of Mr. Biden's expected summit with President Vladimir V. Putin. And going quiet might simply have reflected a decision by the ransomware gang to frustrate retaliation efforts by shutting down its operations, perhaps temporarily.

The Pentagon's Cyber Command referred questions to the National Security Council, which declined to comment.

The episode underscored the emergence of a new ''blended threat,'' one that may come from cybercriminals, but is often tolerated, and sometimes encouraged, by a nation that sees the attacks as serving its interests. That is why Mr. Biden singled out Russia—not as the culprit, but as the nation that harbors more ransomware groups than any other country.

''We do not believe the Russian government was involved in this attack, but we do have strong reason to believe the criminals who did this attack are living in Russia,'' Mr. Biden said. ''We have been in direct communication with Moscow about the imperative for responsible countries to take action against these ransomware networks.''

With DarkSide's systems down, it is unclear how Mr. Biden's administration would retaliate further, beyond possible indictments and sanctions, which have not deterred Russian cybercriminals before. Striking back with a cyberattack also carries its own risks of escalation.

The administration also has to reckon with the fact that so much of America's critical infrastructure is owned and operated by the private sector and remains ripe for attack.

''This attack has exposed just how poor our resilience is,'' said Kiersten E. Todt, the managing director of the nonprofit Cyber Readiness Institute. ''We are overthinking the threat, when we're still not doing the bare basics to secure our critical infrastructure.''

The good news, some officials said, was that Americans got a wake-up call. Congress came face-to-face with the reality that the federal government lacks the authority to require the companies that control more than 80 percent of the nation's critical infrastructure adopt minimal levels of cybersecurity.

The bad news, they said, was that American adversaries—not only superpowers but terrorists and cybercriminals—learned just how little it takes to incite chaos across a large part of the country, even if they do not break into the core of the electric grid, or the operational control systems that move gasoline, water and propane around the country.

Something as basic as a well-designed ransomware attack may easily do the trick, while offering plausible deniability to states like Russia, China and Iran that often tap outsiders for sensitive cyberoperations.

It remains a mystery how DarkSide first broke into Colonial's business network. The privately held company has said virtually nothing about how the attack unfolded, at least in public. It waited four days before having any substantive discussions with the administration, an eternity during a cyberattack.

Cybersecurity experts also note that Colonial Pipeline would never have had to shut down its pipeline if it had more confidence in the separation between its business network and pipeline operations.

''There should absolutely be separation between data management and the actual operational technology,'' Ms. Todt said. ''Not doing the basics is frankly inexcusable for a company that carries 45 percent of gas to the East Coast.''

Other pipeline operators in the United States deploy advanced firewalls between their data and their operations that only allow data to flow one direction, out of the pipeline, and would prevent a ransomware attack from spreading in.

Colonial Pipeline has not said whether it deployed that level of security on its pipeline. Industry analysts say many critical infrastructure operators say installing such unidirectional gateways along a 5,500-mile pipeline can be complicated or prohibitively expensive. Others say the cost to deploy those safeguards are still cheaper than the losses from potential downtime.

Deterring ransomware criminals, which have been growing in number and brazenness over the past few years, will certainly be more difficult than deterring nations. But this week made the urgency clear.

''It's all fun and games when we are stealing each other's money,'' said Sue Gordon, a former principal deputy director of national intelligence, and a longtime C.I.A. analyst with a specialty in cyber issues, said at a conference held by The Cipher Brief, an online intelligence newsletter. ''When we are messing with a society's ability to operate, we can't tolerate it.''

[From MeriTalk: Improving the Outcomes of Government IT, May 20, 2021]

HOUSE HOMELAND SECURITY COMMITTEE ADVANCES SLATE OF CYBERSECURITY BILLS

(By Lamar Johnson)

The House Homeland Security Committee voted May 18 to advance five bills that would look to improve the nation's cybersecurity in several areas, including protecting pipeline infrastructure, testing cybersecurity readiness, and improving state and local cybersecurity, among others.

The bills to advance out of committee included the Pipeline Security Act, the CISA (Cybersecurity and Infrastructure Security Agency) Cyber Exercise Act, and the State and Local Cybersecurity Improvement Act. Also advanced out of committee were the Cybersecurity Vulnerability Remediation Act, introduced by Rep. Sheila Jackson Lee, D-Tex., and the Domains Critical to Homeland Security Act, introduced by Rep. John Katko, R-N.Y., the ranking member on the committee.

''Since the beginning of this Congress, this Committee has engaged in extensive oversight of these events and how the Federal government partners with others to defend our networks,'' Chairman Bennie Thompson, D-Miss., said in a release. ''The legislation we reported today was the result of this oversight. I am pleased that they received broad bipartisan support and hope they are considered on the House floor in short order.''

The Pipeline Security Act was reintroduced by Rep. Emmanuel Cleaver, D-Mo. just a day before advancing out of committee, with the Colonial Pipeline ransomware attack still top of mind. If passed, it will codify CISA and the Transportation Security Agency's responsibilities in protecting pipelines from cyberattacks and terrorist attacks.

''The Colonial Pipeline ransom ware attack that shut down one [of] our nation's largest pipelines and triggered fuel shortages across the northeast has brought new urgency to our work to protect the country's critical infrastructure. This attack also follows a string of disturbing cyberattacks against government entities and the private sector,'' Thompson said.

The CISA Cyber Exercise Act would authorize and require CISA to establish a National Cyber Exercise Program responsible for testing the nation's cyber readiness. The bill was introduced by Elissa Slotkin, D-Mich., and would direct the agency to create a set of exercises that states, local governments, and private sector businesses could use to test their cyber readiness.

State and local governments get a win with the advancement of the State and Local Cybersecurity Improvement Act. The bill was reintroduced by Rep. Yvette Clarke, D-N.Y., on May 12, and a similar version passed in the House in the last Congress. The bill would direct the Department of Homeland Security (DHS) to create a $500 million-per-year grant program to incentivize state and local governments to work to improve their cybersecurity.

The committee also advanced two bills aimed at protecting critical infrastructure and the supply chain after a recent spate of cyberattacks exposed vulnerabilities in the cybersecurity of each.

Rep. Lee's Cybersecurity Vulnerability Remediation Act would authorize CISA to work with the owners and operators of critical infrastructure on mitigation strategies around known and critical vulnerabilities. Rep. Katko's Domains Critical to Homeland Security Act would direct DHS to do research and development around supply chain risks in domains that are critical to the nation's economy. It would then be required to submit that report to Congress.

The next step for all these bills is a vote on the full House floor.

Ms. JACKSON LEE. Madam Speaker, I ask my colleagues to support this legislation because there is a known list of these attacks from the ISS World to the $50 million paid. I ask my colleagues to support this legislation, and I ask my friends in the other body, to pass this legislation so it becomes law.

Madam Speaker, I rise in support of H.R. 2980, ''The Cybersecurity Vulnerability Remediation Act,'' which authorizes the Department of Homeland Security to take actions to counter cybersecurity vulnerabilities in our nation's critical infrastructure.

I thank Chairman THOMPSON and Ranking Member KATKO for their leadership in putting the security of our nation's cyber assets first, whether they are computing resources used in voting technology or industrial control systems that support the delivery of electricity, oil and gas, or management of transportation systems that are vital to our nation's economic health.

The Cybersecurity Vulnerability Remediation Act was introduced and passed the House during the 115th and 116th Congresses and has been updated again in the 117th Congress to meet the ever-evolving nature of cyber threats faced by federal and private sector information systems and our nation's critical infrastructure.

This bill goes significantly further than the first Cybersecurity Vulnerability bill that I introduced in the 115th Congress, to address the instance of Zero Day Events that can lead to catastrophic cybersecurity failures of information and computing systems.

It is estimated that eighty-five percent of critical infrastructure is owned by the private sector and for far too long this fact has hampered efforts to establish stronger requirements for cybersecurity by owners and operators.

Private sector critical infrastructure failure due to a cyberattack is no longer a private matter when it can have massive impacts on the public such as the disruption of gasoline flowing to filling stations.

The Jackson Lee Cybersecurity Vulnerability Remediation Act will:

Expand the definition of security vulnerability to include cybersecurity vulnerability;

Adds sharing mitigation protocols to counter cybersecurity vulnerabilities;

Establish protocols to counter cybersecurity vulnerabilities involving information systems and industrial control systems, which will include vulnerabilities related to software, or hardware that is no longer supported by a vendor;

Direct the Under Secretary for the DHS Office of Science and Technology to standup a competition to find solutions to known cybersecurity vulnerabilities; and

Provide greater transparency on how the Department of Homeland Security's Cybersecurity and Information Security Agency (CISA) is coordinating cybersecurity vulnerability disclosures through the sharing of actionable protocols to mitigate cybersecurity vulnerabilities with information systems and industrial control systems owners and operators.

H.R. 2890 bolsters the efforts to engage critical infrastructure owners and operators in communicating cybersecurity threats; and lays the foundation for greater transparency on the real threats posed by cyberterrorist to private and government sector critical infrastructure and information systems.

The legislation allows the Science the Technology Directorate in consultation with CISA to establish an incentive based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities to information systems and industrial control systems including supervisory control and data acquisition systems.

This bill when it becomes law would put our nation's best minds to work on closing the vulnerabilities that cyber-thieves and terrorists to use them to access, disrupt, corrupt, or take control of critical infrastructure and information systems.

In addition to these changes, the bill requires a report to Congress that may contain a classified annex.

The report will provide information on how DHS:

Coordinates cybersecurity vulnerability disclosures; and

Disseminates actionable protocols to mitigate cybersecurity vulnerabilities involving information system and industrial systems.

Congress needs to know how prevalent and persistent cybersecurity threats targeting critical infrastructure and information systems might be, especially if those threats result in a payment of ransom.

Paying a ransom for ransomware emboldens and encourages bad cyber actors and places everyone at greater risk for the financial and societal costs of increases in threats as other seek payouts.

As long as there is silence about cyber-attacks like ransomware the criminals and terrorists will remain out of reach and continue to feel safe in carrying out these attacks often from the soil of our enemies or peer competitors.

A company cannot stand up to Russia or China, but the United States can and has done so to protect our national interest.

I applaud and thank the Biden Administration for its quick action to respond to the attack against Colonial Pipeline in issuing a new Executive Order.

Today, our nation is in a cybersecurity crisis.

My concern regarding the security of information networks began in 2015 when the Office of Personnel Management's data breach resulted in the theft of millions of sensitive personnel records on federal employees.

The attacks against federal, state, local, territorial, and tribal governments, as well as threats posed to private information systems, and critical infrastructure systems makes this bill necessary.

On May 13, 2021 it was reported that the DC Metropolitan Police Department had experienced the worst reported cyberattack against a police department in the United States.

The gang, known as the Babuk group, released thousands of the Metropolitan Police Department's sensitive documents on the dark web because the department would not pay.

Cyberthreats are not limited to information related to government employees.

In February 2021, a cyberattack on an Oldsmar, Florida water treatment facility involved increasing the levels of sodium hydroxide from 100 parts per million to 11,100 parts per million in drinking water.

However, the levels of this chemical in the water produced by Oldsmar, Florida was increased to levels that would cause harm to people if they drank or used it.

This is just one example of how terrorists can attack critical infrastructure and cause threats to health, safety and life.

Cyber terrorists and cyber criminals are also motivated to attack information networks in exchange for money.

The sources of revenue from cyberattacks has moved from demands of payment for thieves not to release information—to the sale of stolen information on the dark web and now to a sophisticated denial of service attack in the form of ransomware that locks a system using encryption until the victim pays.

A list of known ransomware attacks in 2020 that are suspected of paying ransoms, included:

ISS World (Denmark) paid an estimated cost: $74 million;

Cognizant (US) paid an estimated $50 million;

Sopra Steria (French) paid estimated $50 million;

Redcar and Cleveland Council (UK) paid an estimated $14 million; and

University of California San Francisco (US) paid an estimated $1.14 million.

There are likely many other attacks that are not publicly known and this must change if we are to defeat this threat.

Ransomware is becoming the tool of choice for those seeking a payout because it can be carried out against anyone or any entity by perpetrators who are far from U.S. shores.

The Colonial Pipeline incident is just one in a long line of successful attacks or infiltrations carried out against domestic information systems and critical infrastructure with increasing consequences for the life, health, safety, and economic security of our citizens.

CEO Joseph Blount testified before the U.S. Senate that the attack occurred using a legacy Virtual Private Network (VPN) system that did not have multifactor authentication.

In other words, hackers were able to gain access to this critical infrastructure as a result of a single compromised password.

There would be no need for the Cybersecurity Vulnerability Remediation Act if owners and operators were succeeding in meeting the cybersecurity needs of critical infrastructure.

I know that there is more that should and ought to be done to address the issue of cybercrime and I will be pursuing this avenue under the jurisdiction of the House Judiciary Committee, as the chair of the Subcommittee on Crime, Terrorism and Homeland Security.

Madam Speaker, I ask that my colleagues vote in support of H.R. 2890.

Mr. KATKO. Madam Speaker, I have no further speakers, and I urge Members to support this bill. I yield back the balance of my time.

Ms. CLARKE of New York. Madam Speaker, I yield myself the balance of my time.

Madam Speaker, our adversaries are showing no signs of slowing their efforts to undermine U.S. interests in cyberspace.

Most often, hackers exploit known vulnerabilities. The Federal Government can and should support efforts to address and mitigate known vulnerabilities.

H.R. 2980 would do just that.

I thank the gentlewoman from Texas for her foresight, and I urge my colleagues to support the bill.

Madam Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from New York (Ms. CLARKE) that the House suspend the rules and pass the bill, H.R. 2980, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. BISHOP of North Carolina. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

CISA CYBER EXERCISE ACT

Ms. CLARKE of New York. Madam Speaker, I move to suspend the rules