

United States Senate
WASHINGTON, DC 20510

RELEASE IN FULL

November 1, 2016

President Barack Obama
The White House
1600 Pennsylvania Avenue, NW
Washington, D.C. 20500

Dear Mr. President:

We are writing to urge a direct and proportionate response to the Russian Federation's state-sponsored cyberattacks on the United States' democratic institutions and the 2016 electoral process. Such attacks cannot be tolerated and the United States must take immediate measures to ensure that those responsible are held to account.

On October 7th, the Department of Homeland Security and Office of the Director of National Intelligence stated that the "U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts." The statement went on to say that "only Russia's senior-most officials could have authorized these activities."

The seminal event in a functioning democracy is an election, and the international implications of the results of a U.S. election are far reaching. Russia's actions threaten to undermine our democratic process. Our electoral infrastructure is strong, but it is incumbent upon us to ensure that our institutions are protected. A cyberattack on our electoral process or any part of our critical political, economic, or military infrastructure is a hostile action that must be countered.

We urge you to consider a range of options in response, including some or all the following measures:

First, the administration should utilize existing authorities under Executive Order 13694 to freeze the assets of those individuals who have engaged in significant malicious cyber activity that has affected or been intended to affect our electoral infrastructure.

Second, the administration should consider expanding the use of secondary sanctions to include those who engage with and assist the Russian governmental entities involved in these attacks.

REVIEW AUTHORITY: Geoffrey Chapman, Senior Reviewer

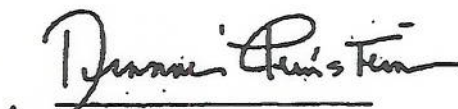
RECEIVED
2016 NOV - 1 P 2:08
LEGISLATIVE AFFAIRS

Third, the administration should consider taking proportional cyber responses beyond sanctions that would shine a direct spotlight on those responsible for the cyberattacks, including those in the Russian government who directed and carried out the attacks. Using existing national security and criminal authorities, the administration should indict those responsible for these cyberattacks in U.S. courts, as has been done in other instances of state-sponsored cyber intrusions. We would also welcome any actions that would afford vulnerable human rights defenders and civil society activists inside of Russia the capability and tools they need to protect themselves from the Russian government's cyber repression. The United States should make clear that there are costs to engaging in these sorts of cyberattacks, whether by Russia or any other actor.

We look forward to your response and working with you to better defend against hostile Russian cyber activities and counter Russia's efforts to destabilize not only the United States' electoral process and system of government, but the integrity of democratic institutions and nations worldwide.

Sincerely,


Benjamin L. Cardin
United States Senator


Dianne Feinstein
United States Senator



United States Department of State

Washington, D.C. 20520

DEC 7 2016

RELEASE IN FULL

The Honorable
Benjamin L. Cardin
United States Senate
Washington, DC 20510

Dear Senator Cardin:

Thank you for your November 1 letter to President Obama concerning Russia and its recent activities in cyberspace. We have been asked to respond on the President's behalf.

We share your concerns over Russian malicious cyber activity, including the Russian government – directed compromises of email from U.S. persons and institutions and their subsequent disclosure that were highlighted in the October 7 press statement by the Department of Homeland Security and the Office of the Director of National Intelligence. In addition to the public announcement, we have raised our concerns over these activities directly with the Russian government.

As we have made clear to the Russian government and others, we will not tolerate attempts to interfere with the U.S. democratic process, and we will take action to protect our interests, including in cyberspace, and we will do so at a time and place of our choosing. We are also taking steps to protect our critical cyber infrastructure – and will continue to harden those defenses.

We appreciate your thoughts on steps that could be taken to respond to cyber threats, and assure you that the Administration is undertaking a comprehensive strategy to respond to malicious cyber activities and significant cyber threats, using a full range of diplomatic, law enforcement, economic, and other public and private tools. We will also continue to pursue the establishment of international norms to ensure that countries around the world act responsibly in the cyber sphere.

REVIEW AUTHORITY: Geoffrey Chapman, Senior Reviewer

-2-

We hope this information is helpful. If we can be of further assistance, please do not hesitate to contact us.

Sincerely,

A handwritten signature in cursive script, appearing to read "Julia Frifield".

Julia Frifield
Assistant Secretary
Legislative Affairs



United States Department of State

Washington, D.C. 20520

DEC 7 2016

RELEASE IN FULL

The Honorable
Dianne Feinstein
United States Senate
Washington, DC 20510

Dear Senator Feinstein:

Thank you for your November 1 letter to President Obama concerning Russia and its recent activities in cyberspace. We have been asked to respond on the President's behalf.

We share your concerns over Russian malicious cyber activity, including the Russian government – directed compromises of email from U.S. persons and institutions and their subsequent disclosure that were highlighted in the October 7 press statement by the Department of Homeland Security and the Office of the Director of National Intelligence. In addition to the public announcement, we have raised our concerns over these activities directly with the Russian government.

As we have made clear to the Russian government and others, we will not tolerate attempts to interfere with the U.S. democratic process, and we will take action to protect our interests, including in cyberspace, and we will do so at a time and place of our choosing. We are also taking steps to protect our critical cyber infrastructure – and will continue to harden those defenses.


We appreciate your thoughts on steps that could be taken to respond to cyber threats, and assure you that the Administration is undertaking a comprehensive strategy to respond to malicious cyber activities and significant cyber threats, using a full range of diplomatic, law enforcement, economic, and other public and private tools. We will also continue to pursue the establishment of international norms to ensure that countries around the world act responsibly in the cyber sphere.

REVIEW AUTHORITY: Geoffrey Chapman, Senior Reviewer

-2-

We hope this information is helpful. If we can be of further assistance, please do not hesitate to contact us.

Sincerely,

A handwritten signature in cursive script, appearing to read "Julia Frifield".

Julia Frifield
Assistant Secretary
Legislative Affairs

UNCLASSIFIED
Official - Transitory

RELEASE IN PART
B5

Trudeau, Elizabeth K

From: Trudeau, Elizabeth K
Sent: Wednesday, December 28, 2016 6:23 AM
To: PO List
Subject: Reminder: POs: On WaPo RU story

Reminder on this.

Official - Transitory
UNCLASSIFIED

From: Trudeau, Elizabeth K
Sent: Tuesday, December 27, 2016 7:26 PM
To: PO List
Subject: POs: On WaPo RU story

On background,

B5

WashPost: Obama administration is close to announcing measures to punish Russia for election interference

The Obama administration is close to announcing a series of measures to punish Russia for its interference in the 2016 presidential election, including economic sanctions and diplomatic censure, according to U.S. officials.

The administration is still finalizing the details, which are also expected to include covert action that likely will involve cyber operations, the officials said. An announcement on the public elements of the response could come as early as this week.

The sanctions part of the package culminates weeks of debate in the White House about how to revise an executive order from last year meant to give the president authority to respond to cyberattacks from overseas, but which did not originally cover efforts to influence the electoral system.

The Obama administration last year rolled the order out to great fanfare as a way to punish and deter foreign hackers who harm the United States' economic or national security.

The threat to use it last year helped wring a pledge out of China's president that his country would cease hacking U.S. companies' secrets to benefit Chinese firms.

In December, during a closed door briefing with senators, the CIA shared a secret assessment. The agency concluded it was now "quite clear" that Russia's goal was to help Donald Trump win the White House. (Jason Aldag/The Washington Post)

But officials this fall concluded that it could not, as written, be used to punish the most significant cyber-provocation in recent memory against the United States — Russia's hacking of Democratic organizations, targeting of state election systems and meddling in the presidential election.

With the clock ticking, the White House is working on adapting the authority to punish the Russians, according to the officials, who spoke on the condition of anonymity to discuss internal deliberations. President Obama last week pledged there would be a response to Moscow's interference in the U.S. elections.

Russia had denied involvement in the hacking.

Trudeau, Elizabeth K

UNCLASSIFIED
Official - Transitory

UNCLASSIFIED
Official - Transitory

One clear way to use the order against the Russian suspects would be to declare the electoral systems part of the "critical infrastructure" of the United States. Or it could be amended to clearly apply to the new threat — interfering in elections.

Administration officials would also like to make it difficult for President-elect Donald Trump to roll back any action they take. "Part of the goal here is to make sure that we have as much of the record public or communicated to Congress in a form that would be difficult to simply walk back," said one senior administration official, who like others spoke on the condition of anonymity to discuss internal deliberations.

Obama issued the executive order in April 2015, creating the sanctions tool as a way to hold accountable people who harm computer systems related to critical functions such as electricity generation or transportation or who gain a competitive advantage through cybertheft of commercial secrets.

President Obama and Chinese President Xi Jinping attend a news conference in November 2014 in Beijing. (Feng Li/Getty Images) The order allows the government to freeze the assets in the United States of people overseas who have engaged in cyber acts that have threatened U.S. national security or financial stability. The sanctions would also block commercial transactions with the designated individuals and bar their entry into the country.

But just a year later, a Russian military spy agency would hack into the Democratic National Committee and steal a trove of emails that were released a few months later on WikiLeaks, U.S. officials said. Other releases followed, including the hacked emails of Hillary Clinton's campaign chairman, John Podesta.

"Fundamentally, it was a low-tech, high-impact event," said Zachary Goldman, a sanctions and national security expert at New York University School of Law. And the 2015 executive order was not crafted to target hackers who steal emails and dump them on WikiLeaks or seek to disrupt an election. "It was an authority published at a particular time to address a particular set of problems," he said.

So officials "need to engage in some legal acrobatics to fit the DNC hack into an existing authority, or they need to write a new authority," Goldman said.

Administration officials would like Obama to use the power before leaving office to demonstrate its utility.

"When the president came into office, he didn't have that many tools out there to use as a response" to malicious cyber-acts, said Ari Schwartz, a former senior director for cybersecurity on the National Security Council. "Having the sanctions tool is really a big one. It can make a very strong statement in a way that is less drastic than bombing a country and more impactful than sending out a cable from the State Department."

The National Security Council concluded that it would not be able to use the authority against Russian hackers because their malicious activity did not clearly fit under its terms, which require harm to critical infrastructure or the theft of commercial secrets.

"You would (a) have to be able to say that the actual electoral infrastructure, such as state databases, was critical infrastructure, and (b) that what the Russians did actually harmed it," said the administration official who spoke on the condition of anonymity. "Those are two high bars."

Though Russian government hackers are believed to have penetrated at least one state voter-registration database, they did not tamper with the data, officials said.

Some analysts believe that state election systems would fit under "government facilities," which is one of the 16 critical infrastructure sectors designated by the Department of Homeland Security.

Another option is to use the executive order against other Russian targets — say, hackers who stole commercial secrets — and then, in either a public message or a private one, make clear that the United States considers its electoral systems to be critical infrastructure. The idea is to not only punish but also deter.

"As much as I am concerned about what happened to us in the election, I am also concerned about what will happen to us in the future," a second official said. "I am firmly convinced that the Russians and others will say, 'That worked pretty well in 2016, so let's keep going.' We have elections every two years in this country."

Even the threat of sanctions can have deterrent value. Officials and experts point to the agreement Chinese President Xi Jinping reached with Obama last year that his country would stop commercial cyberspying. Xi came to the table following news reports last

Trudeau, Elizabeth K

UNCLASSIFIED
Official - Transitory

2

UNCLASSIFIED
Official - Transitory

summer that the administration was preparing to sanction Chinese companies.

Complicating matters, the Trump transition team has not yet had extensive briefings with the White House on cyber issues, including the potential use of the cyber-sanctions order. The slow pace has caused consternation among officials, who fear that the administration's accomplishments in cybersecurity could languish if the next administration fails to understand their value.

[Trump turning away intelligence briefers since election win]

Sanctions are not a silver bullet. Obama noted that "we already have enormous numbers of sanctions against the Russians" for their activities in Ukraine. So it is questionable, some experts say, whether adding new ones would have a meaningful effect in changing the Kremlin's behavior. But in combination with other measures, they could be effective.

Criminal indictments of Russians might become an option, officials said, but the FBI has so far not gathered enough evidence that could be introduced in a criminal case. At one point, federal prosecutors and FBI agents in San Francisco considered indicting Guccifer 2.0, a nickname for a person or people believed to be affiliated with the Russian influence operation and whose true identity was unknown.

Before the election, the administration used diplomatic channels to warn Russia. Obama spoke to Russian President Vladimir Putin at a Group of 20 summit in China in September. About a week before the election, the United States sent a "hotline"-style message to Moscow using a special channel for crisis communication created in 2013 as part of the State Department's Nuclear Risk Reduction Center. As part of that message, the officials said, the administration asked Russia to stop targeting state voter registration and election systems. It was the first use of that system. The Russians, officials said, appeared to comply.

Official - Transitory

UNCLASSIFIED

UNCLASSIFIED
Official - Transitory

RELEASE IN FULL

Trudeau, Elizabeth K

From: Trudeau, Elizabeth K
Sent: Thursday, December 29, 2016 2:20 PM
To: PO List
Cc: Toner, Mark C
Subject: POs: PG for background only
Attachments: EUR - Russia - Dacha and PNG [29 December].docx

The following should be used on BACKGROUND only, after the call. As much as possible, please refer people to the paper statements.

Official - Transitory
UNCLASSIFIED

Trudeau, Elizabeth K

UNCLASSIFIED
Official - Transitory

1