The New York Times | https://nyti.ms/2i0LCVK

POLITICS

Obama Confronts Complexity of Using a Mighty Cyberarsenal Against Russia

By DAVID E. SANGER DEC. 17, 2016

WASHINGTON — Over the past four months, American intelligence agencies and aides to President Obama assembled a menu of options to respond to Russia's hacking during the election, ranging from the obvious — exposing President Vladimir V. Putin's financial ties to oligarchs — to the innovative, including manipulating the computer code that Russia uses in designing its cyberweapons.

But while Mr. Obama vowed on Friday to "send a clear message to Russia" as both a punishment and a deterrent, some of the options were rejected as ineffective, others as too risky. If the choices had been better, one of the aides involved in the debate noted recently, the president would have acted by now.

In his last weeks in office, that Situation Room debate has confronted a naturally cautious president with a complex calculus that President-elect Donald J. Trump will soon inherit: how to use the world's most powerful cyberarsenal at a moment when the United States, as the election showed, remains highly vulnerable.

"Is there something we can do to them, that they would see, they would realize 98 percent that we did it, but that wouldn't be so obvious that they would then have to respond for their own honor?" David H. Petraeus, the former director of the Central Intelligence Agency under Mr. Obama, asked on Friday, at a conference here

sponsored by Harvard's Belfer Center for Science and International Affairs. "The question is how subtle do you want it, how damaging do you want it, how do you try to end it here rather than just ratchet it up?"

The idea of exposing Mr. Putin's links to oligarchs was set aside after some aides argued that it would not come as a shock to Russians. Still, there are proposals to cut off leaders in Mr. Putin's inner circle from their hidden bank accounts in Europe and Asia. There is an option to use sanctions under a year-old executive order to ban international travel for senior officials in the G.R.U., the Russian military intelligence unit that American spy agencies say stole emails from the Democratic National Committee and Hillary Clinton's campaign chairman, then doled them out to WikiLeaks, betting that media outlets eager for insider details would amplify them, doing the Kremlin's work for it.

The National Security Agency and its military cousin, the United States Cyber Command, which is responsible for computer-network warfare, have worked up other ideas, officials said, though some have been rejected by the Pentagon.

Those plans could deploy the world-class arsenal of cyberweapons assembled at a cost of billions of dollars during Mr. Obama's tenure to expose or neutralize some of the hacking tools favored by Russia's spies — the digital equivalent of a pre-emptive strike. But the selection of targets by Americans and the accuracy of that retaliation could also expose software "implants" that the United States has patiently inserted and nurtured in Russian networks, in case of future cyberconflicts.

And the revelation in August about some of the N.S.A.'s own tools for breaking into foreign computer networks has raised the possibility that the Russians are already inside American networks and are sending a warning that they can respond in kind.

All of this has led Mr. Obama to ask how the Russians might escalate the confrontation, and whether the United States in the end may have more to lose than Russia.

"He doesn't have great options," said Michael D. McFaul, formerly one of Mr. Obama's top national security aides and then his ambassador to Moscow.

Mr. Obama is the president who, in his first year in office, reached for some of the most sophisticated cyberweapons on earth to blow up parts of Iran's nuclear facilities. Now, at the end of his presidency, he has run headlong into a different challenge in the cyberwarfare arena.

The president has reached two conclusions, senior officials report: The only thing worse than not using a weapon is using it ineffectively. And if he does choose to retaliate, he has insisted on maintaining what is known as "escalation dominance," the ability to ensure you can end a conflict on your terms.

Mr. Obama hinted as much at his news conference on Friday, as he was set to leave for his annual Hawaii vacation, his last as president.

"Our goal continues to be to send a clear message to Russia or others not to do this to us because we can do stuff to you," he said. "But it is also important to us to do that in a thoughtful, methodical way. Some of it, we will do publicly. Some of it we will do in a way that they know, but not everybody will."

He rejected calls for a big, symbolic show of power, dismissing the idea that if the United States "thumped our chests about a bunch of stuff, that somehow that would potentially spook the Russians." The goal, Mr. Obama said, was to come up with a response "that increases costs for them for behavior like this in the future but does not create problems for us."

There is not much new in tampering with elections, except for the technical sophistication of the tools. For all the outrage voiced by Democrats and Republicans in the past week about the Russian action — with the notable exception of Mr. Trump, who has dismissed the intelligence findings as politically motivated — it is worth remembering that trying to manipulate elections is a well-honed American art form.

The C.I.A. got its start trying to influence the outcome of Italy's elections in 1948, as the author Tim Weiner documented in his book "Legacy of Ashes," in an effort to keep Communists from taking power. Five years later, the C.I.A. engineered a coup against Mohammad Mossadegh, Iran's democratically elected leader, when the United States and Britain installed the Shah.

"The military coup that overthrew Mosaddeq and his National Front cabinet was carried out under CIA direction as an act of U.S. foreign policy, conceived and approved at the highest levels of government," the agency concluded in one of its own reports, declassified around the 60th anniversary of those events, which were engineered in large part by Kermit Roosevelt Jr., a grandson of President Theodore Roosevelt.

There were similar interferences over the years in Guatemala, Chile and even in Japan, hailed as a model of post-World War II democracy, where the Liberal Democratic Party owes its early grip on power in the 1950s and 1960s to millions of dollars in covert C.I.A. support.

The only differences this year are that the effort was directed at the United States, and that it was cyberenabled, giving Moscow a tool to amplify its efforts through the echo chamber of social media and news organizations that quoted from the leaked emails.

"What has changed is that this was using cyberspace for advancing a political objective," said Adm. James A. Winnefeld Jr., who served as vice chairman of the Joint Chiefs of Staff until he retired last year. Cybertechniques, he said, have amplified an old form of "political warfare, and the issue is not whether it successfully influenced the election — but the fact that they did it."

Over the past few months, an administration that prided itself on its work on cyberoffense and cyberdefense has learned a hard lesson: When it came to the 2016 election, an economically failing Russia, dismissed by Mr. Obama on Friday for its inability to grow or to innovate, exploited giant holes in the American system.

Mr. Obama conceded that he first heard about the attack on the Democratic National Committee "early last summer," or nine months after the F.B.I. first alerted low-level D.N.C. officials about what had happened. That now appears to be critical lost time.

If Mr. Obama had confronted the Russians immediately, in public or in the kind of private warning he said he delivered to Mr. Putin only three months ago during a

meeting in China, the United States might have derailed the hacking campaign before it harvested and revealed thousands of emails.

But the election hacking also raised questions about whether the American fixation on a "cyber Pearl Harbor" — a devastating attack on the power grid, cellphone network, financial system or computer-controlled gas pipelines — overlooked a more obvious vulnerability.

As a detailed account in The New York Times last Wednesday revealed, the D.N.C. had virtually no protections for its electronic systems, and Mrs. Clinton's campaign chairman, John D. Podesta, had failed to sign up for the "two-factor authentication" on his Gmail account. Doing so probably would have foiled what Mr. Obama called a fairly primitive attack.

Now the question facing Mr. Obama is how public a retaliation to execute.

The president laid out a case on Friday for acting with subtlety, so as not to start a tit-for-tat conflict.

But as Joseph Nye, a strategist on so-called soft power, noted on Friday, "The reason to make some of this public is not just to deter the Russians, it is to deter others as well," in future elections.

It is possible, said Mr. McFaul, the former ambassador to Russia, that Mr. Obama's most lasting contribution may be to get the details of the Russian hack declassified and to publish a report he has instructed the intelligence community to assemble before he leaves office.

"Given that Obama only has a few more weeks in office, I think he needs to focus his remaining time on attribution — that is declassification of intelligence so that there is no ambiguity about the Russian actions," Mr. McFaul said. That "is completely within his powers," he added, and would spur more congressional investigations regardless of the stance taken by Mr. Trump on the hack.

Mr. Obama's comments on Friday have led Democrats to demand further action. Representative Adam B. Schiff of California, the ranking Democrat on the House Intelligence Committee, said the response should mix "additional economic

sanctions along with our allies, and clandestine means of exacting a cost on the Russians for their flagrant meddling in our election."

"I have little confidence," he continued, "that the incoming president will take the actions necessary to make the Russians pay any price for the most consequential 'active measures' campaign against us in history."

A version of this article appears in print on December 18, 2016, on Page A1 of the New York edition with the headline: Wary President Takes On Riddles of Cyberwarfare.
