The New York Times | https://nyti.ms/2hBJis3

POLITICS

The Perfect Weapon: How Russian Cyberpower Invaded the U.S.

Читать статью по-русски

By ERIC LIPTON, DAVID E. SANGER and SCOTT SHANE DEC. 13, 2016

WASHINGTON — When Special Agent Adrian Hawkins of the Federal Bureau of Investigation called the Democratic National Committee in September 2015 to pass along some troubling news about its computer network, he was transferred, naturally, to the help desk.

His message was brief, if alarming. At least one computer system belonging to the D.N.C. had been compromised by hackers federal investigators had named "the Dukes," a cyberespionage team linked to the Russian government.

The F.B.I. knew it well: The bureau had spent the last few years trying to kick the Dukes out of the unclassified email systems of the White House, the State Department and even the Joint Chiefs of Staff, one of the government's best-protected networks.

Yared Tamene, the tech-support contractor at the D.N.C. who fielded the call, was no expert in cyberattacks. His first moves were to check Google for "the Dukes" and conduct a cursory search of the D.N.C. computer system logs to look for hints of such a cyberintrusion. By his own account, he did not look too hard even after

Special Agent Hawkins called back repeatedly over the next several weeks — in part because he wasn't certain the caller was a real F.B.I. agent and not an impostor.

"I had no way of differentiating the call I just received from a prank call," Mr. Tamene wrote in an internal memo, obtained by The New York Times, that detailed his contact with the F.B.I.

It was the cryptic first sign of a cyberespionage and information-warfare campaign devised to disrupt the 2016 presidential election, the first such attempt by a foreign power in American history. What started as an information-gathering operation, intelligence officials believe, ultimately morphed into an effort to harm one candidate, Hillary Clinton, and tip the election to her opponent, Donald J. Trump.

Like another famous American election scandal, it started with a break-in at the D.N.C. The first time, 44 years ago at the committee's old offices in the Watergate complex, the burglars planted listening devices and jimmied a filing cabinet. This time, the burglary was conducted from afar, directed by the Kremlin, with spear-phishing emails and zeros and ones.

An examination by The Times of the Russian operation — based on interviews with dozens of players targeted in the attack, intelligence officials who investigated it and Obama administration officials who deliberated over the best response — reveals a series of missed signals, slow responses and a continuing underestimation of the seriousness of the cyberattack.

The D.N.C.'s fumbling encounter with the F.B.I. meant the best chance to halt the Russian intrusion was lost. The failure to grasp the scope of the attacks undercut efforts to minimize their impact. And the White House's reluctance to respond forcefully meant the Russians have not paid a heavy price for their actions, a decision that could prove critical in deterring future cyberattacks.

The low-key approach of the F.B.I. meant that Russian hackers could roam freely through the committee's network for nearly seven months before top D.N.C. officials were alerted to the attack and hired cyberexperts to protect their systems. In the meantime, the hackers moved on to targets outside the D.N.C., including Mrs.

Clinton's campaign chairman, John D. Podesta, whose private email account was hacked months later.

Even Mr. Podesta, a savvy Washington insider who had written a 2014 report on cyberprivacy for President Obama, did not truly understand the gravity of the hacking.

By last summer, Democrats watched in helpless fury as their private emails and confidential documents appeared online day after day — procured by Russian intelligence agents, posted on WikiLeaks and other websites, then eagerly reported on by the American media, including The Times. Mr. Trump gleefully cited many of the purloined emails on the campaign trail.

The fallout included the resignations of Representative Debbie Wasserman Schultz of Florida, the chairwoman of the D.N.C., and most of her top party aides. Leading Democrats were sidelined at the height of the campaign, silenced by revelations of embarrassing emails or consumed by the scramble to deal with the hacking. Though little-noticed by the public, confidential documents taken by the Russian hackers from the D.N.C.'s sister organization, the Democratic Congressional Campaign Committee, turned up in congressional races in a dozen states, tainting some of them with accusations of scandal.

In recent days, a skeptical president-elect, the nation's intelligence agencies and the two major parties have become embroiled in an extraordinary public dispute over what evidence exists that President Vladimir V. Putin of Russia moved beyond mere espionage to deliberately try to subvert American democracy and pick the winner of the presidential election.

Many of Mrs. Clinton's closest aides believe that the Russian assault had a profound impact on the election, while conceding that other factors — Mrs. Clinton's weaknesses as a candidate; her private email server; the public statements of the F.B.I. director, James B. Comey, about her handling of classified information — were also important.

While there's no way to be certain of the ultimate impact of the hack, this much is clear: A low-cost, high-impact weapon that Russia had test-fired in elections from

Ukraine to Europe was trained on the United States, with devastating effectiveness. For Russia, with an enfeebled economy and a nuclear arsenal it cannot use short of all-out war, cyberpower proved the perfect weapon: cheap, hard to see coming, hard to trace.

"There shouldn't be any doubt in anybody's mind," Adm. Michael S. Rogers, the director of the National Security Agency and commander of United States Cyber Command, said at a postelection conference. "This was not something that was done casually, this was not something that was done by chance, this was not a target that was selected purely arbitrarily," he said. "This was a conscious effort by a nation-state to attempt to achieve a specific effect."

For the people whose emails were stolen, this new form of political sabotage has left a trail of shock and professional damage. Neera Tanden, president of the Center for American Progress and a key Clinton supporter, recalls walking into the busy Clinton transition offices, humiliated to see her face on television screens as pundits discussed a leaked email in which she had called Mrs. Clinton's instincts "suboptimal."

"It was just a sucker punch to the gut every day," Ms. Tanden said. "It was the worst professional experience of my life."

The United States, too, has carried out cyberattacks, and in decades past the C.I.A. tried to subvert foreign elections. But the Russian attack is increasingly understood across the political spectrum as an ominous historic landmark — with one notable exception: Mr. Trump has rejected the findings of the intelligence agencies he will soon oversee as "ridiculous," insisting that the hacker may be American, or Chinese, but that "they have no idea."

Mr. Trump cited the reported disagreements between the agencies about whether Mr. Putin intended to help elect him. On Tuesday, a Russian government spokesman echoed Mr. Trump's scorn.

"This tale of 'hacks' resembles a banal brawl between American security officials over spheres of influence," Maria Zakharova, the spokeswoman for the Russian Foreign Ministry, wrote on Facebook.

Over the weekend, four prominent senators — two Republicans and two Democrats — joined forces to pledge an investigation while pointedly ignoring Mr. Trump's skeptical claims.

"Democrats and Republicans must work together, and across the jurisdictional lines of the Congress, to examine these recent incidents thoroughly and devise comprehensive solutions to deter and defend against further cyberattacks," said Senators John McCain, Lindsey Graham, Chuck Schumer and Jack Reed.

"This cannot become a partisan issue," they said. "The stakes are too high for our country."

A Target for Break-Ins

Sitting in the basement of the Democratic National Committee headquarters, below a wall-size 2012 portrait of a smiling Barack Obama, is a 1960s-era filing cabinet missing the handle on the bottom drawer. Only a framed newspaper story hanging on the wall hints at the importance of this aged piece of office furniture.

"GOP Security Aide Among 5 Arrested in Bugging Affair," reads the headline from the front page of The Washington Post on June 19, 1972, with the bylines of Bob Woodward and Carl Bernstein.

Andrew Brown, 37, the technology director at the D.N.C., was born after that famous break-in. But as he began to plan for this year's election cycle, he was well aware that the D.N.C. could become a break-in target again.

There were aspirations to ensure that the D.N.C. was well protected against cyberintruders — and then there was the reality, Mr. Brown and his bosses at the organization acknowledged: The D.N.C. was a nonprofit group, dependent on donations, with a fraction of the security budget that a corporation its size would have.

"There was never enough money to do everything we needed to do," Mr. Brown said.

The D.N.C. had a standard email spam-filtering service, intended to block phishing attacks and malware created to resemble legitimate email. But when Russian hackers started in on the D.N.C., the committee did not have the most advanced systems in place to track suspicious traffic, internal D.N.C. memos show.

Mr. Tamene, who reports to Mr. Brown and fielded the call from the F.B.I. agent, was not a full-time D.N.C. employee; he works for a Chicago-based contracting firm called The MIS Department. He was left to figure out, largely on his own, how to respond — and even whether the man who had called in to the D.N.C. switchboard was really an F.B.I. agent.

"The F.B.I. thinks the D.N.C. has at least one compromised computer on its network and the F.B.I. wanted to know if the D.N.C. is aware, and if so, what the D.N.C. is doing about it," Mr. Tamene wrote in an internal memo about his contacts with the F.B.I. He added that "the Special Agent told me to look for a specific type of malware dubbed 'Dukes' by the U.S. intelligence community and in cybersecurity circles."

Part of the problem was that Special Agent Hawkins did not show up in person at the D.N.C. Nor could he email anyone there, as that risked alerting the hackers that the F.B.I. knew they were in the system.

Mr. Tamene's initial scan of the D.N.C. system — using his less-than-optimal tools and incomplete targeting information from the F.B.I. — found nothing. So when Special Agent Hawkins called repeatedly in October, leaving voice mail messages for Mr. Tamene, urging him to call back, "I did not return his calls, as I had nothing to report," Mr. Tamene explained in his memo.

In November, Special Agent Hawkins called with more ominous news. A D.N.C. computer was "calling home, where home meant Russia," Mr. Tamene's memo says, referring to software sending information to Moscow. "SA Hawkins added that the F.B.I. thinks that this calling home behavior could be the result of a state-sponsored attack."

Mr. Brown knew that Mr. Tamene, who declined to comment, was fielding calls from the F.B.I. But he was tied up on a different problem: evidence suggesting that

the campaign of Senator Bernie Sanders of Vermont, Mrs. Clinton's main Democratic opponent, had improperly gained access to her campaign data.

Ms. Wasserman Schultz, then the D.N.C.'s chairwoman, and Amy Dacey, then its chief executive, said in interviews that neither of them was notified about the early reports that the committee's system had likely been compromised.

Shawn Henry, who once led the F.B.I.'s cyber division and is now president of CrowdStrike Services, the cybersecurity firm retained by the D.N.C. in April, said he was baffled that the F.B.I. did not call a more senior official at the D.N.C. or send an agent in person to the party headquarters to try to force a more vigorous response.

"We are not talking about an office that is in the middle of the woods of Montana," Mr. Henry said. "We are talking about an office that is half a mile from the F.B.I. office that is getting the notification."

"This is not a mom-and-pop delicatessen or a local library. This is a critical piece of the U.S. infrastructure because it relates to our electoral process, our elected officials, our legislative process, our executive process," he added. "To me it is a high-level, serious issue, and if after a couple of months you don't see any results, somebody ought to raise that to a higher level."

The F.B.I. declined to comment on the agency's handling of the hack. "The F.B.I. takes very seriously any compromise of public and private sector systems," it said in a statement, adding that agents "will continue to share information" to help targets "safeguard their systems against the actions of persistent cybercriminals."

By March, Mr. Tamene and his team had met at least twice in person with the F.B.I. and concluded that Agent Hawkins was really a federal employee. But then the situation took a dire turn.

A second team of Russian-affiliated hackers began to target the D.N.C. and other players in the political world, particularly Democrats. Billy Rinehart, a former D.N.C. regional field director who was then working for Mrs. Clinton's campaign, got an odd email warning from Google.

"Someone just used your password to try to sign into your Google account," the March 22 email said, adding that the sign-in attempt had occurred in Ukraine. "Google stopped this sign-in attempt. You should change your password immediately."

Mr. Rinehart was in Hawaii at the time. He remembers checking his email at 4 a.m. for messages from East Coast associates. Without thinking much about the notification, he clicked on the "change password" button and half asleep, as best he can remember, he typed in a new password.

What he did not know until months later is that he had just given the Russian hackers access to his email account.

Hundreds of similar phishing emails were being sent to American political targets, including an identical email sent on March 19 to Mr. Podesta, chairman of the Clinton campaign. Given how many emails Mr. Podesta received through this personal email account, several aides also had access to it, and one of them noticed the warning email, sending it to a computer technician to make sure it was legitimate before anyone clicked on the "change password" button.

"This is a legitimate email," Charles Delavan, a Clinton campaign aide, replied to another of Mr. Podesta's aides, who had noticed the alert. "John needs to change his password immediately."

With another click, a decade of emails that Mr. Podesta maintained in his Gmail account — a total of about 60,000 — were unlocked for the Russian hackers. Mr. Delavan, in an interview, said that his bad advice was a result of a typo: He knew this was a phishing attack, as the campaign was getting dozens of them. He said he had meant to type that it was an "illegitimate" email, an error that he said has plagued him ever since.

During this second wave, the hackers also gained access to the Democratic Congressional Campaign Committee, and then, through a virtual private network connection, to the main computer network of the D.N.C.

The F.B.I. observed this surge of activity as well, again reaching out to Mr. Tamene to warn him. Yet Mr. Tamene still saw no reason to be alarmed: He found copies of the phishing emails in the D.N.C.'s spam filter. But he had no reason, he said, to believe that the computer systems had been infiltrated.

One bit of progress had finally been made by the middle of April: The D.N.C., seven months after it had first been warned, finally installed a "robust set of monitoring tools," Mr. Tamene's internal memo says.

Honing Stealthy Tactics

The United States had two decades of warning that Russia's intelligence agencies were trying to break into America's most sensitive computer networks. But the Russians have always managed to stay a step ahead.

Their first major attack was detected on Oct. 7, 1996, when a computer operator at the Colorado School of Mines discovered some nighttime computer activity he could not explain. The school had a major contract with the Navy, and the operator warned his contacts there. But as happened two decades later at the D.N.C., at first "everyone was unable to connect the dots," said Thomas Rid, a scholar at King's College in London who has studied the attack.

Investigators gave it a name — Moonlight Maze — and spent two years, often working day and night, tracing how it hopped from the Navy to the Department of Energy to the Air Force and NASA. In the end, they concluded that the total number of files stolen, if printed and stacked, would be taller than the Washington Monument.

Whole weapons designs were flowing out the door, and it was a first taste of what was to come: an escalating campaign of cyberattacks around the world.

But for years, the Russians stayed largely out of the headlines, thanks to the Chinese — who took bigger risks, and often got caught. They stole the designs for the F-35 fighter jet, corporate secrets for rolling steel, even the blueprints for gas pipelines that supply much of the United States. And during the 2008 presidential election cycle, Chinese intelligence hacked into the campaigns of Mr. Obama and

Mr. McCain, making off with internal position papers and communications. But they didn't publish any of it.

The Russians had not gone away, of course. "They were just a lot more stealthy," said Kevin Mandia, a former Air Force intelligence officer who spent most of his days fighting off Russian cyberattacks before founding Mandiant, a cybersecurity firm that is now a division of FireEye — and the company the Clinton campaign brought in to secure its own systems.

The Russians were also quicker to turn their attacks to political purposes. A 2007 cyberattack on Estonia, a former Soviet republic that had joined NATO, sent a message that Russia could paralyze the country without invading it. The next year cyberattacks were used during Russia's war with Georgia.

But American officials did not imagine that the Russians would dare try those techniques inside the United States. They were largely focused on preventing what former Defense Secretary Leon E. Panetta warned was an approaching "cyber Pearl Harbor" — a shutdown of the power grid or cellphone networks.

But in 2014 and 2015, a Russian hacking group began systematically targeting the State Department, the White House and the Joint Chiefs of Staff. "Each time, they eventually met with some form of success," Michael Sulmeyer, a former cyberexpert for the secretary of defense, and Ben Buchanan, now both of the Harvard Cyber Security Project, wrote recently in a soon-to-be published paper for the Carnegie Endowment.

The Russians grew stealthier and stealthier, tricking government computers into sending out data while disguising the electronic "command and control" messages that set off alarms for anyone looking for malicious actions. The State Department was so crippled that it repeatedly closed its systems to throw out the intruders. At one point, officials traveling to Vienna with Secretary of State John Kerry for the Iran nuclear negotiations had to set up commercial Gmail accounts just to communicate with one another and with reporters traveling with them.

Mr. Obama was briefed regularly on all this, but he made a decision that many in the White House now regret: He did not name Russians publicly, or issue

sanctions. There was always a reason: fear of escalating a cyberwar, and concern that the United States needed Russia's cooperation in negotiations over Syria.

"We'd have all these circular meetings," one senior State Department official said, "in which everyone agreed you had to push back at the Russians and push back hard. But it didn't happen."

So the Russians escalated again — breaking into systems not just for espionage, but to publish or broadcast what they found, known as "doxing" in the cyberworld.

It was a brazen change in tactics, moving the Russians from espionage to influence operations. In February 2014, they broadcast an intercepted phone call between Victoria Nuland, the assistant secretary of state who handles Russian affairs and has a contentious relationship with Mr. Putin, and Geoffrey Pyatt, the United States ambassador to Ukraine. Ms. Nuland was heard describing a little-known American effort to broker a deal in Ukraine, then in political turmoil.

They were not the only ones on whom the Russians used the steal-and-leak strategy. The Open Society Foundation, run by George Soros, was a major target, and when its documents were released, some turned out to have been altered to make it appear as if the foundation was financing Russian opposition members.

Last year, the attacks became more aggressive. Russia hacked a major French television station, frying critical hardware. Around Christmas, it attacked part of the power grid in Ukraine, dropping a portion of the country into darkness, killing backup generators and taking control of generators. In retrospect, it was a warning shot.

The attacks "were not fully integrated military operations," Mr. Sulmeyer said. But they showed an increasing boldness.

Cozy Bear and Fancy Bear

The day before the White House Correspondents' Association dinner in April, Ms. Dacey, the D.N.C.'s chief executive, was preparing for a night of parties when she got an urgent phone call.

With the new monitoring system in place, Mr. Tamene had examined administrative logs of the D.N.C.'s computer system and found something very suspicious: An unauthorized person, with administrator-level security status, had gained access to the D.N.C.'s computers.

"Not sure it is related to what the F.B.I. has been noticing," said one internal D.N.C. email sent on April 29. "The D.N.C. may have been hacked in a serious way this week, with password theft, etc."

No one knew just how bad the breach was — but it was clear that a lot more than a single filing cabinet worth of materials might have been taken. A secret committee was immediately created, including Ms. Dacey, Ms. Wasserman Schultz, Mr. Brown and Michael Sussmann, a former cybercrimes prosecutor at the Department of Justice who now works at Perkins Coie, the Washington law firm that handles D.N.C. political matters.

"Three most important questions," Mr. Sussmann wrote to his clients the night the break-in was confirmed. "1) What data was accessed? 2) How was it done? 3) How do we stop it?"

Mr. Sussmann instructed his clients not to use D.N.C. email because they had just one opportunity to lock the hackers out — an effort that could be foiled if the hackers knew that the D.N.C. was on to them.

"You only get one chance to raise the drawbridge," Mr. Sussmann said. "If the adversaries know you are aware of their presence, they will take steps to burrow in, or erase the logs that show they were present."

The D.N.C. immediately hired CrowdStrike, a cybersecurity firm, to scan its computers, identify the intruders and build a new computer and telephone system from scratch. Within a day, CrowdStrike confirmed that the intrusion had originated in Russia, Mr. Sussmann said.

The work that such companies do is a computer version of old-fashioned crime scene investigation, with fingerprints, bullet casings and DNA swabs replaced by an electronic trail that can be just as incriminating. And just as police detectives learn

to identify the telltale methods of a veteran burglar, so CrowdStrike investigators recognized the distinctive handiwork of Cozy Bear and Fancy Bear.

Those are CrowdStrike's nicknames for the two Russian hacking groups that the firm found at work inside the D.N.C. network. Cozy Bear — the group also known as the Dukes or A.P.T. 29, for "advanced persistent threat" — may or may not be associated with the F.S.B., the main successor to the Soviet-era K.G.B., but it is widely believed to be a Russian government operation. It made its first appearance in 2014, said Dmitri Alperovitch, CrowdStrike's co-founder and chief technology officer.

It was Cozy Bear, CrowdStrike concluded, that first penetrated the D.N.C. in the summer of 2015, by sending spear-phishing emails to a long list of American government agencies, Washington nonprofits and government contractors. Whenever someone clicked on a phishing message, the Russians would enter the network, "exfiltrate" documents of interest and stockpile them for intelligence purposes.

"Once they got into the D.N.C., they found the data valuable and decided to continue the operation," said Mr. Alperovitch, who was born in Russia and moved to the United States as a teenager.

Only in March 2016 did Fancy Bear show up — first penetrating the computers of the Democratic Congressional Campaign Committee, and then jumping to the D.N.C., investigators believe. Fancy Bear, sometimes called A.P.T. 28 and believed to be directed by the G.R.U., Russia's military intelligence agency, is an older outfit, tracked by Western investigators for nearly a decade. It was Fancy Bear that got hold of Mr. Podesta's email.

Attribution, as the skill of identifying a cyberattacker is known, is more art than science. It is often impossible to name an attacker with absolute certainty. But over time, by accumulating a reference library of hacking techniques and targets, it is possible to spot repeat offenders. Fancy Bear, for instance, has gone after military and political targets in Ukraine and Georgia, and at NATO installations.

That largely rules out cybercriminals and most countries, Mr. Alperovitch said. “There’s no plausible actor that has an interest in all those victims other than Russia,” he said. Another clue: The Russian hacking groups tended to be active during working hours in the Moscow time zone.

To their astonishment, Mr. Alperovitch said, CrowdStrike experts found signs that the two Russian hacking groups had not coordinated their attacks. Fancy Bear, apparently not knowing that Cozy Bear had been rummaging in D.N.C. files for months, took many of the same documents.

In the six weeks after CrowdStrike’s arrival, in total secrecy, the computer system at the D.N.C. was replaced. For a weekend, email and phones were shut off; employees were told it was a system upgrade. All laptops were turned in and the hard drives wiped clean, with the uninfected information on them imaged to new drives.

Though D.N.C. officials had learned that the Democratic Congressional Campaign Committee had been infected, too, they did not notify their sister organization, which was in the same building, because they were afraid that it would leak.

All of this work took place as the bitter contest for the Democratic nomination continued to play out between Mrs. Clinton and Mr. Sanders, and it was already causing a major distraction for Ms. Wasserman Schultz and the D.N.C.’s chief executive.

“This was not a bump in the road — bumps in the road happen all the time,” she said in an interview. “Two different Russian spy agencies had hacked into our network and stolen our property. And we did not yet know what they had taken. But we knew they had very broad access to our network. There was a tremendous amount of uncertainty. And it was chilling.”

The D.N.C. executives and their lawyer had their first formal meeting with senior F.B.I. officials in mid-June, nine months after the bureau’s first call to the tech-support contractor. Among the early requests at that meeting, according to participants: that the federal government make a quick “attribution” formally

blaming actors with ties to Russian government for the attack to make clear that it was not routine hacking but foreign espionage.

"You have a presidential election underway here and you know that the Russians have hacked into the D.N.C.," Mr. Sussmann said, recalling the message to the F.B.I. "We need to tell the American public that. And soon."

The Media's Role

In mid-June, on Mr. Sussmann's advice, D.N.C. leaders decided to take a bold step. Concerned that word of the hacking might leak, they decided to go public in The Washington Post with the news that the committee had been attacked. That way, they figured, they could get ahead of the story, win a little sympathy from voters for being victimized by Russian hackers and refocus on the campaign.

But the very next day, a new, deeply unsettling shock awaited them. Someone calling himself Guccifer 2.0 appeared on the web, claiming to be the D.N.C. hacker — and he posted a confidential committee document detailing Mr. Trump's record and half a dozen other documents to prove his bona fides.

"And it's just a tiny part of all docs I downloaded from the Democrats networks," he wrote. Then something more ominous: "The main part of the papers, thousands of files and mails, I gave to WikiLeaks. They will publish them soon."

It was bad enough that Russian hackers had been spying inside the committee's network for months. Now the public release of documents had turned a conventional espionage operation into something far more menacing: political sabotage, an unpredictable, uncontrollable menace for Democratic campaigns.

Guccifer 2.0 borrowed the moniker of an earlier hacker, a Romanian who called himself Guccifer and was jailed for breaking into the personal computers of former President George W. Bush, former Secretary of State Colin L. Powell and other notables. This new attacker seemed intent on showing that the D.N.C.'s cyberexperts at CrowdStrike were wrong to blame Russia. Guccifer 2.0 called himself a "lone hacker" and mocked CrowdStrike for calling the attackers "sophisticated."

But online investigators quickly undercut his story. On a whim, Lorenzo Franceschi-Bicchierai, a writer for Motherboard, the tech and culture site of Vice, tried to contact Guccifer 2.0 by direct message on Twitter.

"Surprisingly, he answered right away," Mr. Franceschi-Bicchierai said. But whoever was on the other end seemed to be mocking him. "I asked him why he did

it, and he said he wanted to expose the Illuminati. He called himself a Gucci lover. And he said he was Romanian."

That gave Mr. Franceschi-Bicchierai an idea. Using Google Translate, he sent the purported hacker some questions in Romanian. The answers came back in Romanian. But when he was offline, Mr. Franceschi-Bicchierai checked with a couple of native speakers, who told him Guccifer 2.0 had apparently been using Google Translate as well — and was clearly not the Romanian he claimed to be.

Cyberresearchers found other clues pointing to Russia. Microsoft Word documents posted by Guccifer 2.0 had been edited by someone calling himself, in Russian, Felix Edmundovich — an obvious nom de guerre honoring the founder of the Soviet secret police, Felix Edmundovich Dzerzhinsky. Bad links in the texts were marked by warnings in Russian, generated by what was clearly a Russian-language version of Word.

When Mr. Franceschi-Bicchierai managed to engage Guccifer 2.0 over a period of weeks, he found that his interlocutor's tone and manner changed. "At first he was careless and colloquial. Weeks later, he was curt and more calculating," he said. "It seemed like a group of people, and a very sloppy attempt to cover up."

Computer experts drew the same conclusion about DCLeaks.com, a site that sprang up in June, claiming to be the work of "hacktivists" but posting more stolen documents. It, too, seemed to be a clumsy front for the same Russians who had stolen the documents. Notably, the website was registered in April, suggesting that the Russian hacking team planned well in advance to make public what it stole.

In addition to what Guccifer 2.0 published on his site, he provided material directly on request to some bloggers and publications. The steady flow of Guccifer 2.0 documents constantly undercut Democratic messaging efforts. On July 6, 12 days before the Republican National Convention began in Cleveland, Guccifer released the D.N.C.'s battle plan and budget for countering it. For Republican operatives, it was insider gold.

Then WikiLeaks, a far more established outlet, began to publish the hacked material — just as Guccifer 2.0 had promised. On July 22, three days before the start

of the Democratic National Convention in Philadelphia, WikiLeaks dumped out 44,053 D.N.C. emails with 17,761 attachments. Some of the messages made clear that some D.N.C. officials favored Mrs. Clinton over her progressive challenger, Mr. Sanders.

That was no shock; Mr. Sanders, after all, had been an independent socialist, not a Democrat, during his long career in Congress, while Mrs. Clinton had been one of the party's stars for decades. But the emails, some of them crude or insulting, infuriated Sanders delegates as they arrived in Philadelphia. Ms. Wasserman Schultz resigned under pressure on the eve of the convention where she had planned to preside.

Mr. Trump, by now the Republican nominee, expressed delight at the continuing jolts to his opponent, and he began to use Twitter and his stump speeches to highlight the WikiLeaks releases. On July 25, he sent out a lighthearted tweet: "The new joke in town," he wrote, "is that Russia leaked the disastrous D.N.C. e-mails, which should never have been written (stupid), because Putin likes me."

But WikiLeaks was far from finished. On Oct. 7, a month before the election, the site began the serial publication of thousands of private emails to and from Mr. Podesta, Mrs. Clinton's campaign manager.

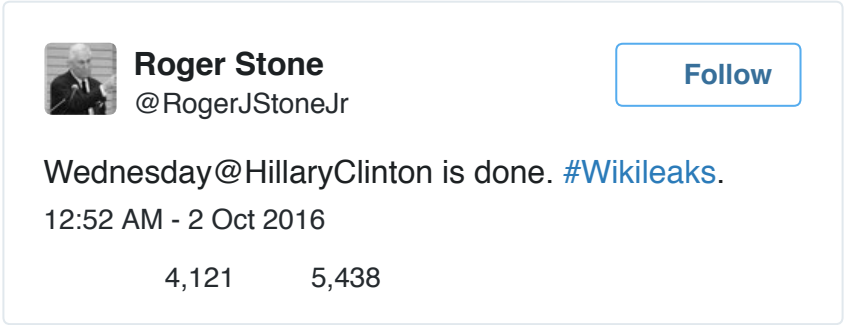
The same day, the United States formally accused the Russian government of being behind the hackings, in a joint statement by the director of national intelligence and the Department of Homeland Security, and Mr. Trump suffered his worst blow to date, with the release of a recording in which he bragged about sexually assaulting women.

The Podesta emails were nowhere near as sensational as the Trump video. But, released by WikiLeaks day after day over the last month of the campaign, they provided material for countless news reports. They disclosed the contents of Mrs. Clinton's speeches to large banks, which she had refused to release. They exposed tensions inside the campaign, including disagreements over donations to the Clinton Foundation that staff members thought might look bad for the candidate and Ms. Tanden's complaint that Mrs. Clinton's instincts were "suboptimal."

"I was just mortified," Ms. Tanden said in an interview. Her emails were released on the eve of one of the presidential debates, she recalled. "I put my hands over my head and said, 'I can't believe this is happening to me.'" Though she had regularly appeared on television to support Mrs. Clinton, she canceled her appearances because all the questions were about what she had said in the emails.

Ms. Tanden, like other Democrats whose messages became public, said it was obvious to her that WikiLeaks was trying its best to damage the Clinton campaign. "If you care about transparency, you put all the emails out at once," she said. "But they wanted to hurt her. So they put them out 1,800 to 3,000 a day."

The Trump campaign knew in advance about WikiLeaks' plans. Days before the Podesta email release began, Roger Stone, a Republican operative working with the Trump campaign, sent out an excited tweet about what was coming.



But in an interview, Mr. Stone said he had no role in the leaks; he had just heard from an American with ties to WikiLeaks that damning emails were coming.

Julian Assange, the WikiLeaks founder and editor, has resisted the conclusion that his site became a pass-through for Russian hackers working for Mr. Putin's government or that he was deliberately trying to undermine Mrs. Clinton's candidacy. But the evidence on both counts appears compelling.

In a series of email exchanges, Mr. Assange refused to say anything about WikiLeaks' source for the hacked material. He denied that he had made his animus toward Mrs. Clinton clear in public statements ("False. But what is this? Junior high?") or that the site had timed the releases for maximum negative effect on her campaign. "WikiLeaks makes its decisions based on newsworthiness, including for its recent epic scoops," he wrote.

Mr. Assange disputed the conclusion of the Oct. 7 statement from the intelligence agencies that the leaks were "intended to interfere with the U.S. election process."

"This is false," he wrote. "As the disclosing party we know that this was not the intent. Publishers publishing newsworthy information during an election is part of a free election."

But asked whether he believed the leaks were one reason for Mr. Trump's election, Mr. Assange seemed happy to take credit. "Americans extensively engaged with our publications," he wrote. "According to Facebook statistics WikiLeaks was the most referenced political topic during October."

Though Mr. Assange did not say so, WikiLeaks' best defense may be the conduct of the mainstream American media. Every major publication, including The Times, published multiple stories citing the D.N.C. and Podesta emails posted by WikiLeaks, becoming a de facto instrument of Russian intelligence.

Mr. Putin, a student of martial arts, had turned two institutions at the core of American democracy — political campaigns and independent media — to his own ends. The media's appetite for the hacked material, and its focus on the gossipy content instead of the Russian source, disturbed some of those whose personal emails were being reposted across the web.

"What was really surprising to me?" Ms. Tanden said. "I could not believe that reporters were covering it."

Devising a Government Response

Inside the White House, as Mr. Obama's advisers debated their response, their conversation turned to North Korea.

In late 2014, hackers working for Kim Jong-un, the North's young and unpredictable leader, had carried out a well-planned attack on Sony Pictures Entertainment intended to stop the Christmastime release of a comedy about a C.I.A. plot to kill Mr. Kim.

In that case, embarrassing emails had also been released. But the real damage was done to Sony's own systems: More than 70 percent of its computers melted down when a particularly virulent form of malware was released. Within weeks, intelligence agencies traced the attack back to the North and its leadership. Mr. Obama called North Korea out in public, and issued some not-very-effective sanctions. The Chinese even cooperated, briefly cutting off the North's internet connections.

As the first Situation Room meetings on the Russian hacking began in July, "it was clear that Russia was going to be a much more complicated case," said one participant. The Russians clearly had a more sophisticated understanding of American politics, and they were masters of "kompromat," their term for compromising information.

But a formal "attribution report" still had not been forwarded to the president.

"It took forever," one senior administration official said, complaining about the pace at which the intelligence assessments moved through the system.

In August a group that called itself the "Shadow Brokers" published a set of software tools that looked like what the N.S.A. uses to break into foreign computer networks and install "implants," malware that can be used for surveillance or attack. The code came from the Tailored Access Operations unit of the N.S.A., a secretive group that mastered the arts of surveillance and cyberwar.

The assumption — still unproved — was that the code was put out in the open by the Russians as a warning: Retaliate for the D.N.C., and there are a lot more secrets, from the hackings of the State Department, the White House and the Pentagon, that might be spilled as well. One senior official compared it to the scene in "The Godfather" where the head of a favorite horse is left in a bed, as a warning.

The N.S.A. said nothing. But by late August, Admiral Rogers, its director, was pressing for a more muscular response to the Russians. In his role as director of the Pentagon's Cyber Command, he proposed a series of potential counter-cyberstrikes.

While officials will not discuss them in detail, the possible counterstrikes reportedly included operations that would turn the tables on Mr. Putin, exposing his financial links to Russia's oligarchs, and punching holes in the Russian internet to allow dissidents to get their message out. Pentagon officials judged the measures too unsubtle and ordered up their own set of options.

But in the end, none of those were formally presented to the president.

In a series of "deputies meetings" run by Avril Haines, the deputy national security adviser and a former deputy director of the C.I.A., several officials warned that an overreaction by the administration would play into Mr. Putin's hands.

"If we went to Defcon 4," one frequent participant in Ms. Haines's meetings said, using a phrase from the Cold War days of warnings of war, "we would be saying to the public that we didn't have confidence in the integrity of our voting system."

Even something seemingly straightforward — using the president's executive powers, bolstered after the Sony incident, to place economic and travel sanctions on cyberattackers — seemed too risky.

"No one was all that eager to impose costs before Election Day," said another participant in the classified meeting. "Any retaliatory measures were seen through the prism of what would happen on Election Day."

Instead, when Mr. Obama's national security team reconvened after summer vacation, the focus turned to a crash effort to secure the nation's voting machines and voter-registration rolls from hacking. The scenario they discussed most frequently — one that turned out not to be an issue — was a narrow vote in favor of Mrs. Clinton, followed by a declaration by Mr. Trump that the vote was "rigged" and more leaks intended to undercut her legitimacy.

Donna Brazile, the interim chairwoman of the D.N.C., became increasingly frustrated as the clock continued to run down on the presidential election — and still there was no broad public condemnation by the White House, or Republican Party leaders, of the attack as an act of foreign espionage.

Ms. Brazile even reached out to Reince Priebus, the chairman of the Republican National Committee, urging him twice in private conversations and in a letter to join her in condemning the attacks — an offer he declined to take up.

"We just kept hearing the government would respond, the government would respond," she said. "Once upon a time, if a foreign government interfered with our election we would respond as a nation, not as a political party."

But Mr. Obama did decide that he would deliver a warning to Mr. Putin in person at a Group of 20 summit meeting in Hangzhou, China, the last time they would be in the same place while Mr. Obama was still in office. When the two men met for a tense pull-aside, Mr. Obama explicitly warned Mr. Putin of a strong American response if there was continued effort to influence the election or manipulate the vote, according to White House officials who were not present for the one-on-one meeting.

Later that day, Mr. Obama made a rare reference to America's own offensive cybercapacity, which he has almost never talked about. "Frankly, both offensively and defensively, we have more capacity," he told reporters.

But when it came time to make a public assertion of Russia's role in early October, it was made in a written statement from the director of national intelligence and the secretary of homeland security. It was far less dramatic than the president's appearance in the press room two years before to directly accuse the North Koreans of attacking Sony.

The reference in the statement to hackings on "political organizations," officials now say, encompassed a hacking on data stored by the Republicans as well. Two senior officials say the forensic evidence was accompanied by "human and technical" sources in Russia, which appears to mean that the United States' implants or taps in Russian computer and phone networks helped confirm the country's role.

But that may not be known for decades, until the secrets are declassified.

A week later Vice President Joseph R. Biden Jr. was sent out to transmit a public warning to Mr. Putin: The United States will retaliate "at the time of our

choosing. And under the circumstances that have the greatest impact."

Later, after Mr. Biden said he was not concerned that Russia could "fundamentally alter the election," he was asked whether the American public would know if the message to Mr. Putin had been sent.

"Hope not," Mr. Biden responded.

Some of his former colleagues think that was the wrong answer. An American counterstrike, said Michael Morell, the former deputy director of the C.I.A. under Mr. Obama, has "got to be overt. It needs to be seen."

A covert response would significantly limit the deterrence effect, he added. "If you can't see it, it's not going to deter the Chinese and North Koreans and Iranians and others."

The Obama administration says it still has more than 30 days to do exactly that.

The Next Target

As the year draws to a close, it now seems possible that there will be multiple investigations of the Russian hacking — the intelligence review Mr. Obama has ordered completed by Jan. 20, the day he leaves office, and one or more congressional inquiries. They will wrestle with, among other things, Mr. Putin's motive.

Did he seek to mar the brand of American democracy, to forestall anti-Russian activism for both Russians and their neighbors? Or to weaken the next American president, since presumably Mr. Putin had no reason to doubt American forecasts that Mrs. Clinton would win easily? Or was it, as the C.I.A. concluded last month, a deliberate attempt to elect Mr. Trump?

In fact, the Russian hack-and-dox scheme accomplished all three goals.

What seems clear is that Russian hacking, given its success, is not going to stop. Two weeks ago, the German intelligence chief, Bruno Kahl, warned that Russia might target elections in Germany next year. "The perpetrators have an interest to

delegitimize the democratic process as such," Mr. Kahl said. Now, he added, "Europe is in the focus of these attempts of disturbance, and Germany to a particularly great extent."

But Russia has by no means forgotten its American target. On the day after the presidential election, the cybersecurity company Volexity reported five new waves of phishing emails, evidently from Cozy Bear, aimed at think tanks and nonprofits in the United States.

One of them purported to be from Harvard University, attaching a fake paper. Its title: "Why American Elections Are Flawed."

Correction: December 13, 2016

Editors' Note: An earlier version of the main photograph with this article, of a filing cabinet and computer at the Democratic National Committee headquarters, should not have been published. The photographer had removed a framed image from the wall over the filing cabinet — showing a Washington Post Watergate front page — because it was causing glare with the lighting. The new version shows the scene as it normally appears, with the framed newspaper page in place.

Kitty Bennett contributed research.

Get politics and Washington news updates via Facebook, Twitter and in the Morning Briefing newsletter.

A version of this article appears in print on December 14, 2016, on Page A1 of the New York edition with the headline: Hacking the Democrats.