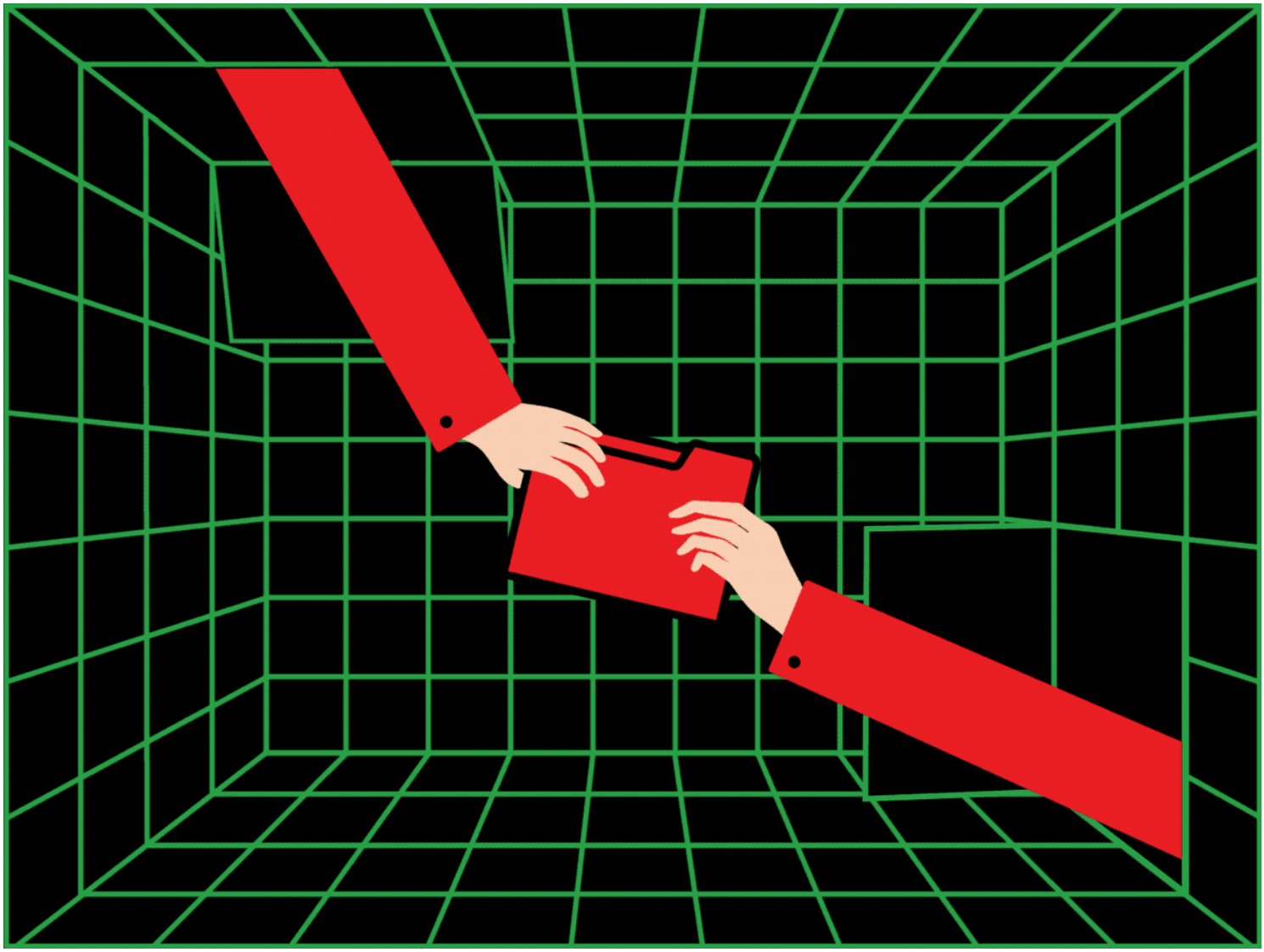
A Reporter at Large

Was There a Connection Between a Russian Bank and the Trump Campaign?

A team of computer scientists sifted through records of unusual Web traffic in search of answers.

By Dexter Filkins

October 8, 2018



A set of cryptic data has inspired a years-long argument over its meaning. Illustration by Jarek Waszul

In June, 2016, after news broke that the Democratic National Committee had been hacked, a group of prominent computer scientists went on alert. Reports said that the infiltrators were probably Russian, which suggested to most members of the group that one of the country's intelligence agencies had been involved. They speculated that if the Russians were hacking the Democrats they must be hacking the Republicans, too. "We thought there was no way in the world the Russians would just attack the Democrats," one of the computer scientists, who asked to be identified only as Max, told me.

The group was small—a handful of scientists, scattered across the country—and politically diverse. (Max described himself as "a John McCain Republican.") Its members sometimes worked with law enforcement or for private clients, but mostly they acted as self-appointed guardians of the Internet, trying to thwart hackers and to keep the system clean of malware—software that hackers use to control a computer remotely, or to extract data. "People think the Internet runs on its own," Max told me. "It doesn't. We do this to keep the Internet safe." The hack of the D.N.C. seemed like a pernicious attack on the integrity of the Web, as well as on the American political system. The scientists decided to investigate whether any Republicans had been hacked, too. "We were trying to protect them," Max said.

Max's group began combing the Domain Name System, a worldwide network that acts as a sort of phone book for the Internet, translating easy-to-remember domain

names into I.P. addresses, the strings of numbers that computers use to identify one another. Whenever someone goes online—to send an e-mail, to visit a Web site—her device contacts the Domain Name System to locate the computer that it is trying to connect with. Each query, known as a D.N.S. lookup, can be logged, leaving records in a constellation of servers that extends through private companies, public institutions, and universities. Max and his group are part of a community that has unusual access to these records, which are especially useful to cybersecurity experts who work to protect clients from attacks.

Max and the other computer scientists asked me to withhold their names, out of concern for their privacy and their security. I met with Max and his lawyer repeatedly, and interviewed other prominent computer experts. (Among them were Jean Camp, of Indiana University; Steven Bellovin, of Columbia University; Daniel Kahn Gillmor, of the A.C.L.U.; Richard Clayton, of the University of Cambridge; Matt Blaze, of the University of Pennsylvania; and Paul Vixie, of Farsight Security.) Several of them independently reviewed the records that Max's group had discovered and confirmed that they would be difficult to fake. A senior aide on Capitol Hill, who works in national security, said that Max's research is widely respected among experts in computer science and cybersecurity.

As Max and his colleagues searched D.N.S. logs for domains associated with Republican candidates, they were perplexed by what they encountered. "We went looking for fingerprints similar to what was on the D.N.C. computers, but we didn't find what we were looking for," Max told me. "We found something totally different—something unique." In the small town of Lititz, Pennsylvania, a domain linked to the Trump Organization (mail1.trump-email.com) seemed to be behaving in a peculiar way. The server that housed the domain belonged to a company called Listrak, which mostly helped deliver mass-marketing e-mails: blasts of messages advertising spa treatments, Las Vegas weekends, and other enticements. Some Trump Organization domains sent mass e-mail blasts, but the one that Max and his colleagues spotted appeared not to be sending anything. At

the same time, though, a very small group of companies seemed to be trying to communicate with it.

Examining records for the Trump domain, Max's group discovered D.N.S. lookups from a pair of servers owned by Alfa Bank, one of the largest banks in Russia. Alfa Bank's computers were looking up the address of the Trump server nearly every day. There were dozens of lookups on some days and far fewer on others, but the total number was notable: between May and September, Alfa Bank looked up the Trump Organization's domain more than two thousand times. "We were watching this happen in real time—it was like watching an airplane fly by," Max said. "And we thought, Why the hell is a Russian bank communicating with a server that belongs to the Trump Organization, and at such a rate?"

Only one other entity seemed to be reaching out to the Trump Organization's domain with any frequency: Spectrum Health, of Grand Rapids, Michigan. Spectrum Health is closely linked to the DeVos family; Richard DeVos, Jr., is the chairman of the board, and one of its hospitals is named after his mother. His wife, Betsy DeVos, was appointed Secretary of Education by Donald Trump. Her brother, Erik Prince, is a Trump associate who has attracted the scrutiny of Robert Mueller, the special counsel investigating Trump's ties to Russia. Mueller has been looking into Prince's meeting, following the election, with a Russian official in the Seychelles, at which he reportedly discussed setting up a back channel between Trump and the Russian President, Vladimir Putin. (Prince maintains that the meeting was "incidental.") In the summer of 2016, Max and the others weren't aware of any of this. "We didn't know who DeVos was," Max said.

The D.N.S. records raised vexing questions. Why was the Trump Organization's domain, set up to send mass-marketing e-mails, conducting such meagre activity? And why were computers at Alfa Bank and Spectrum Health trying to reach a server that didn't seem to be doing anything? After analyzing the data, Max said, "We decided this was a covert communication channel."

The Trump Organization, Alfa Bank, and Spectrum Health have repeatedly denied any contact. But the question of whether Max's conclusion was correct remains enormously consequential. Was this evidence of an illicit connection between Russia and the Trump campaign? Or was it merely a coincidence, cyber trash, that fed suspicions in a dark time?

In August, 2016, Max decided to reveal the data that he and his colleagues had assembled. "If the covert communications were real, this potential threat to our country needed to be known before the election," he said. After some discussion, he and his lawyer decided to hand over the findings to Eric Lichtblau, of the *Times*. Lichtblau met with Max, and began to look at the data.

Lichtblau had done breakthrough reporting on National Security Agency surveillance, and he knew that Max's findings would require sophisticated analysis. D.N.S. lookups are metadata—records that indicate computer interactions but don't necessarily demonstrate human communication. Lichtblau shared the data with three leading computer scientists, and, like Max, they were struck by the unusual traffic on the server. As Lichtblau talked to experts, he became increasingly convinced that the data suggested a substantive connection. "Not only is there clearly something there but there's clearly something that someone has gone to great lengths to conceal," he told me. Jean Camp, of Indiana University, had also vetted some of the data. "These people who should not be communicating are clearly communicating," she said. In order to encourage discussion among analysts, Camp posted a portion of the raw data on her Web site.

As Lichtblau wrote a draft of an article for the *Times*, Max's lawyer contacted the F.B.I. to alert agents that a story about Trump would be running in a national publication, and to pass along the data. A few days later, an F.B.I. official called Lichtblau and asked him to come to the Bureau's headquarters, in Washington, D.C.

At the meeting, in late September, 2016, a roomful of officials told Lichtblau that they were looking into potential Russian interference in the election. According to a source who was briefed on the investigation, the Bureau had intelligence from informants suggesting a possible connection between the Trump Organization and Russian banks, but no data. The information from Max's group could be a significant advance. "The F.B.I. was looking for people in the United States who were helping Russia to influence the election," the source said. "It was very important to the Bureau. It was urgent."

The F.B.I. officials asked Lichtblau to delay publishing his story, saying that releasing the news could jeopardize their investigation. As the story sat, Dean Baquet, the *Times*' executive editor, decided that it would not suffice to report the existence of computer contacts without knowing their purpose. Lichtblau disagreed, arguing that his story contained important news: that the F.B.I. had opened a counterintelligence investigation into Russian contacts with Trump's aides. "It was a really tense debate," Baquet told me. "If I were the reporter, I would have wanted to run it, too. It felt like there was something there." But, with the election looming, Baquet thought that he could not publish the story without being more confident in its conclusions.

Over time, the F.B.I.'s interest in the possibility of an Alfa Bank connection seemed to wane. An agency official told Lichtblau that there could be an innocuous explanation for the computer traffic. Then, on October 30th, Senate Minority Leader Harry Reid wrote a letter to James Comey, the director of the F.B.I., charging that the Bureau was withholding information about "close ties and coordination" between the Trump campaign and Russia. "We had a window," Lichtblau said. His story about Alfa Bank ran the next day. But it bore only a modest resemblance to what he had filed. The headline— "INVESTIGATING DONALD TRUMP, F.B.I. SEES NO CLEAR LINK TO RUSSIA"—seemed to exonerate the Trump campaign. And, though the article mentioned the server, it omitted any reference to the computer scientists who had told Lichtblau that the Trump Organization and

Alfa Bank might have been communicating. “We were saying that the investigation was basically over—and it was just beginning,” Lichtblau told me.

That same day, Slate ran a story, by Franklin Foer, that made a detailed case for the possibility of a covert link between Alfa Bank and Trump. Foer’s report was based largely on information from a colleague of Max’s who called himself Tea Leaves. Foer quoted several outside experts; most said that there appeared to be no other plausible explanation for the data.

One remarkable aspect of Foer’s story involved the way that the Trump domain had stopped working. On September 21st, he wrote, the *Times* had delivered potential evidence of communications to B.G.R., a Washington lobbying firm that worked for Alfa Bank. Two days later, the Trump domain vanished from the Internet. (Technically, its “A record,” which translates the domain name to an I.P. address, was deleted. If the D.N.S. is a phone book, the domain name was effectively decoupled from its number.) For four days, the servers at Alfa Bank kept trying to look up the Trump domain. Then, ten minutes after the last attempt, one of them looked up another domain, which had been configured to lead to the same Trump Organization server.

Max’s group was surprised. The Trump domain had been shut down after the *Times* contacted Alfa Bank’s representatives—but before the newspaper contacted Trump. “That shows a human interaction,” Max concluded. “Certain actions leave fingerprints.” He reasoned that someone representing Alfa Bank had alerted the Trump Organization, which shut down the domain, set up another one, and then informed Alfa Bank of the new address.

A week after the *Times* story appeared, Trump won the election. On Inauguration Day, Liz Spayd, the *Times*' ombudsman, published a column criticizing the paper's handling of stories related to Trump and Russia, including the Alfa Bank connection. "The Times was too timid in its decisions not to publish the material it had," she wrote. Spayd's article did not sit well with Baquet. "It was a bad column," he told the Washington *Post*. Spayd argued that Slate had acted correctly by publishing a more aggressive story, which Baquet dismissed as a "fairly ridiculous conclusion." That June, Spayd's job was eliminated, as the paper's publisher said that the position of ombudsman had become outdated in the digital age. When I talked to Baquet recently, he still felt that he had been right to resist discussing the server in greater depth, but he acknowledged that the *Times* had been too quick to disclaim the possibility of Trump's connections to Russia. "The story was written too knowingly," he said. "The headline was flawed. We didn't know then what we know now."

In April, 2017, Lichtblau left the *Times*, after fifteen years—in part, he said, because of the way that the Alfa Bank story was handled. He went to work for CNN, but resigned less than two months later, amid controversy over another story that he had worked on, about the Trump aide Anthony Scaramucci. This April, Lichtblau returned to the *Times* newsroom for a celebration: he had been part of a team of *Times* reporters that was awarded a Pulitzer Prize for its work on other aspects of the Trump campaign. "It was quite a year," he said.
Meanwhile, the Trump-Alfa Bank story seemed to fade. The Trump campaign dismissed any connection, saying, "The only covert server is the one Hillary Clinton recklessly established in her basement." Bloggers and tech journalists assailed the Slate piece online. The cybersecurity researcher Robert Graham called the analysis "nonsense," and complained, "This is why we can't have nice things on the Internet." He pointed out several problems. For instance, Foer's sources had found that the Trump domain was blocking incoming e-mail, and argued that this was evidence that Trump and Alfa Bank were maintaining a private communications network; in fact, Listrak routinely configured its

marketing servers to send e-mail but not to receive it. Graham also noted that the domain was administered not by Trump but by Cendyn, a company in Boca Raton that handled his company's marketing e-mail.

Alfa Bank hired two cybersecurity firms, Mandiant and Stroz Friedberg, to review the data. Both firms reported that they had found no evidence of communications with the Trump Organization. The bank also began trying to uncover the anonymous sources in the Slate piece. Attorneys representing Alfa contacted Jean Camp, telling her that they were considering legal action and asking her to identify the researchers who had assembled the data. She declined to reveal their names. "This is what tenure is for," she told me.

Alfa Bank was founded by Mikhail Fridman, in the last years of the Soviet Union. Fridman was born in western Ukraine and studied metallurgy in college. Like many others of his generation, he was introduced to the market economy through hustle. He sold theatre tickets, washed windows, and ran a student discothèque. After the Soviet Union collapsed, in 1991, Fridman joined the scramble to befriend members of the new government and amass a fortune with help from the state. Along with an economist named Petr Aven, who had previously served as the country's minister for foreign economic relations, Fridman built Alfa Bank into one of the most successful businesses in the new Russia. Its parent company, Alfa Group, now controls the country's largest private bank, along with financial institutions in several European nations.

Fridman and Aven acquired reputations as brilliant, relentless businessmen. Describing the lawless post-Soviet years to the journalist Chrystia Freeland, who is now the foreign minister of Canada, Fridman said, "We were absolute savages." In a notorious episode in 2008, a group of Russian companies, including Alfa Group, tried to gain control of a joint venture they'd formed with British Petroleum. The power struggle was so fierce that the C.E.O. of the joint venture, Robert Dudley, felt compelled to leave Russia. The oligarchs kept pushing for

control of the BP venture until it was sold to a state-owned petroleum company, for fifty-five billion dollars; Alfa Group's cut was almost fourteen billion.

Alfa Bank prospered during the Yeltsin years and has continued to do so under Putin. Though Fridman and Aven are not part of Putin's innermost circle, they have managed to avoid the fate of some other oligarchs, who have had assets seized and, in a few cases, been imprisoned, after falling out of favor. Michael McFaul, a former U.S. Ambassador to Russia, told me he was impressed that Fridman and Aven had "navigated the very difficult world of maintaining their private business interests and not crossing the Kremlin."

One reason the server story alarmed Alfa Bank was that it threatened the bank's standing in Washington. Members of Russia's government and many of its businessmen have been under American economic sanctions since 2014, when Russia annexed Crimea, but Alfa's principals and representatives have enjoyed access to U.S. politicians at the highest levels. Fridman and Aven met several times with officials at the Obama White House, discussing such issues as Russia's effort to gain entrance to the World Trade Organization. (Alfa Bank maintains that it has "never advocated for political or trade issues on behalf of the Russian government.") "Fridman and Aven were seen as people that Washington could talk to about U.S.-Russia, because they checked two boxes—they were 'polite company' oligarchs, and they could shed light on Putin's intentions and perspective," a senior official in the Obama Administration told me. "They got meetings at State and on the Hill and at the White House. And they were understood to be operating with the consent and guidance of Vladimir Putin."

Alfa is still closely tied to the Russian system, but Fridman and Aven live much of the time in the United Kingdom. If there was a communications link with the Trump Organization, it might have been created without their knowledge. According to experts I spoke to, large Russian companies typically have a member of the intelligence services, either active or retired, working at a senior level. If a company's services are required in some way, the officer—called a

kurator—coördinates them. “A company couldn’t say no,” a Washington-based Russia expert told me. (When asked about this, an Alfa Bank spokesperson said, “To our knowledge there are no senior intelligence officials at senior levels at Alfa Bank.”)

This past May, I saw Petr Aven in New York, at the Four Seasons Hotel. He had just come from a dinner in Washington, at which he had met a group of prominent Americans, including officials from the White House, to discuss Russia’s economic situation. Aven seemed worried about surveillance; before we sat down, he brought his phone to the other side of the lobby and hid it behind a plant. He wouldn’t say much for the record, but he told me that his bank didn’t have “any connection at all with Trump—nothing.”

Aven and Fridman have visited Washington less often since Trump took office. But Trump’s victory appeared to elevate Alfa Bank’s connections there—at least by association. Don McGahn, the White House counsel, came from Jones Day, one of the law firms that represent Alfa Bank in the United States. McGahn brought five Jones Day lawyers with him into the White House; six more were appointed to senior posts in the Administration. Jones Day has done work for businesses belonging to a long list of Russian oligarchs, including Oleg Deripaska, Viktor Vekselberg, and Alexander Mashkevich. The firm has also represented the Trump campaign in its dealings with Robert Mueller. For this reason, McGahn secured an ethics waiver that allows him to talk to his old firm when its clients have business before the U.S. government.

In June, 2017, Trump nominated Brian Benczkowski, a lawyer who had overseen the Stroz Friedberg report for Alfa Bank, to lead the criminal division of the Justice Department. At his confirmation hearing, Benczkowski said emphatically that Stroz Friedberg, like Mandiant, had rejected the possibility of complicity. The investigation, he said, found that “there was no communications link between the Trump Organization and Alfa Bank.”

Democratic senators expressed concern that Benczkowski had taken on work for Alfa Bank; he had been a senior member of Trump's transition team and had good reason to expect that he would be appointed to a job in the Administration. "The client was a Russian bank that is under suspicion of having a direct connection with the Trump campaign," Senator Richard Durbin said, during the hearing.

He and the other Democratic senators were especially troubled that Benczkowski would not commit to recusing himself from dealing with Mueller's investigation, even though he had worked for two of Russia's leading oligarchs. "Why did you refuse to recuse yourself?" Senator Dianne Feinstein asked.

"I don't know what's in Special Prosecutor Mueller's investigation," Benczkowski said. "I'm a lawyer in private practice. I have no idea what he's up to, other than what I read in the papers."

Despite these questions, the Republican-led committee approved Benczkowski. This past July, the Senate confirmed him.

While Republicans in Congress have rejected the possibility of collusion, with some joining Trump in calling the Mueller inquiry a politically motivated "witch hunt," a few Democrats have continued to pursue the matter. After Trump's Inauguration, two Democratic senators who had reviewed the data assembled by Max's group—Mark Warner and a colleague who requested anonymity—asked the F.B.I. for an assessment of any potential contacts between Alfa Bank and the Trump Organization. The material was also brought to the attention of the C.I.A., which found it substantial enough to suggest that the F.B.I. investigate. In March, 2017, a Pennsylvania news outlet called Lancaster Online reported that F.B.I. agents had visited the offices of Listrak, the company that housed the Trump server. Ross Kramer, Listrak's C.E.O., told me, "I gave them everything they asked for."

Around the same time, the second Democratic senator approached a former Senate staffer named Daniel Jones and asked him to give the data a closer look. Jones had served as a counterterrorism investigator for the F.B.I. and then spent ten years working for the Senate Intelligence Committee, where he led the inquiry into the use of torture under the George W. Bush Administration. Now he was running an investigations firm, the Penn Quarter Group, and a nonprofit initiative called the Democracy Integrity Project, which was intended to help keep elections free from foreign interference.

To assess the Alfa Bank data, Jones assembled a team of computer scientists, divided into two groups, one on each coast. (They also consulted with Jean Camp, who agreed to coöperate despite the possibility that Alfa Bank might take legal action.) All these experts have national reputations in the field. Some have held senior cybersecurity jobs in the Pentagon, the White House, and the intelligence services, as well as in leading American technology companies. In order to encourage an unbiased outcome, Jones never introduced the East Coast group to the West Coast group.

I met several times with the two members of the East Coast group and spoke with them repeatedly. They used pseudonyms, Paul and Leto, in part because they had been alarmed by encounters with Russia while they were working at high levels of government. Leto said that, in 2016, as he was investigating cyber intrusions that seemed to originate in Russia, he became convinced that he was being followed. Both he and Paul believed that their phones had been hacked. These incursions coincided with a period of intense Russian activity in the U.S., including the hacking of the D.N.C., a pro-Trump social-media blitz, and the arrival of Maria Butina, who is accused of being a Russian agent sent to ingratiate herself with American conservative leaders. (Butina has denied the accusations.)

As Paul and Leto began working, they needed to verify that Max's data presented an accurate picture of the traffic. After the Slate story appeared, skeptics pointed out that no one has a comprehensive view of the Domain Name System. They

speculated that other entities, besides Alfa Bank and Spectrum Health, had looked up the Trump domain, and that Max had failed to see them. The D.N.S. company Dyn told a reporter that it had seen lookups from other computers around the world. But Dyn turned out to have registered only two additional lookups, both from the same address in the Netherlands.

Max and his colleagues maintain that they are able to see nearly all the D.N.S. lookups on a given domain; the senior Capitol Hill aide I spoke to affirmed that Max's group is widely understood to have this capability. Paul Vixie, one of the original architects of the D.N.S. network, examined the data and told me, "If this is a forgery, it's better than any forgery I've seen." Jones's team also ran analyses and real-time tests to check Max's access to D.N.S. records. "It's completely implausible that he could have fooled us," Paul said.

Max had provided the Jones team with thirty-seven million D.N.S. records, enough to fill thousands of screens with time stamps and I.P. addresses—long strings of numbers and letters in green type. Over the course of several months, Paul and Leto examined the data for patterns and anomalies. "We stared at a lot of green screens," Paul said. They regarded their inquiry as a statistical enterprise, capturing each Alfa Bank D.N.S. query from the ocean of data that they had been given and plotting it over a four-month period. Both said that they began their work as skeptics. "I started from an assumption that this is a bunch of nonsense," Leto told me.

Much of the information that was publicly available might well have supported that assumption. Foer's article in Slate had prompted online discussions, in which commentators offered explanations ranging from the benign to the sinister. The timing of the lookups, which came in the summer just before the election, invited speculation. Foer claimed that the biggest flurries of traffic coincided with major campaign events, including the party conventions. Paul and Leto were dubious. If anything, the traffic coincided with Paul Manafort's time as Trump's campaign

manager—but the D.N.S. queries continued after Manafort stepped down. “A lot of people are seeing faces in clouds,” Leto said.

The Trump Organization had done little to clarify the matter. In October, 2016, it released a statement denying interactions with Alfa Bank “or any Russian entity.” Instead, it offered a peculiar explanation for the D.N.S. traffic: it had been triggered when “an existing banking customer of Cendyn”—the marketing firm—had used the company’s systems to send communications to Alfa Bank. Such a scenario would be highly irregular; it was as if Gmail had allowed a user to send e-mail from another user’s account. “It makes no sense,” Paul told me.

Trump’s advocates claimed that the investigations sponsored by Alfa Bank had proved that Alfa and the Trump Organization were not communicating. In fact, they sidestepped the question. Mandiant, one of the cybersecurity firms, said that it was unable to inspect the bank’s D.N.S. logs from 2016, because Alfa retained such records for only twenty-four hours. The other firm, Stroz Friedberg, gave the same explanation for why it, too, was “unable to verify” the data.

As Jones’s team vetted the data, they examined various possible explanations. One was malware, which had played a role in the hack of the D.N.C.’s computers. Most malware has “distinctive patterns of behavior,” Camp told me. It is typically sent out in a blast, aimed simultaneously at multiple domains. There is a “payload”—a mechanism that activates the malicious activity—and a “recruitment mechanism,” which enables the malware to take over parts of a vulnerable computer. None of the experts whom Jones assembled found any evidence of this behavior on the Trump server. “Malware doesn’t keep banging on the door like that,” Paul said.

A second possibility was marketing e-mail. After the Slate article appeared, some commentators suggested that Trump’s server had innocently sent promotional e-mails to Alfa Bank, and that a computer there had responded with queries designed to verify the identity of the sender. This became a catchall answer for

anyone who couldn't explain what had happened. "Either this is something innocuous, like spam," Rachel Cohen, a press secretary for Senator Warner, told me, "or it's completely nefarious."

Alfa Bank had received Trump marketing e-mails in the past. But Cendyn had told CNN that it stopped sending e-mails for the Trump Organization in March, 2016, before the peculiar activity began; Trump had transferred his online marketing to another company, called Serenata. Jones's team investigated, and found additional evidence that the server wasn't sending marketing e-mails at the time. One indicator was the unusually limited traffic. Kramer, of Listrak, told me that a typical client sends "tens of thousands of e-mails a day" to huge numbers of recipients. If the Trump server was following that pattern, it would have generated significant D.N.S. traffic. To establish a kind of control group, Jones's team asked Max to capture the D.N.S. logs for the Denihan Hospitality Group—a hotel chain, similar in size to Trump's, which was using Cendyn and Listrak to send marketing e-mails. In a sample spanning August and September, 2016, a Denihan domain received more than twenty thousand D.N.S. queries, from more than a thousand I.P. addresses. In the same period, the Trump domain had twenty-five hundred lookups, nearly all of them from Alfa Bank and Spectrum Health.
The timing and the frequency of the D.N.S. lookups also did not suggest spam, Paul and Leto believed. Mass-marketing e-mails are typically sent by an automated process, one after another, in an unbroken rhythm. The Alfa queries seemed to fall into two categories. Some came in a steady pulse, while others arrived irregularly—sometimes many in a day, sometimes a few. "The timing of the communication was not random, and it wasn't regular-periodic," Paul said. "It was a better match for human activity."

But, if the Trump server wasn't sending or receiving e-mail, what could explain the traffic? There was the possibility of "spoofing"—essentially, faking an identity. Did someone try to make it appear, falsely, that Alfa Bank was reaching out to the Trump Organization? Jones's team concluded that such an attack would

have been unlikely to produce thousands of D.N.S. lookups, over such a long time. “Maybe for a few days, but not four months,” Leto said. There was also a question of motive. In the spring of 2016, very few people knew that Max and his colleagues were able to monitor D.N.S. traffic so comprehensively, so any spoofers would have been impersonating Alfa Bank with little expectation of being detected. News stories investigating the links between Trump and Russia were months away. “Why would someone do that?” Steven Bellovin, of Columbia, said. “And why would they pick those organizations?”

When I saw Petr Aven at the Four Seasons, he argued that the connections with the Trump Organization had been fabricated in order to frame his company. “This is a conspiracy against us,” he told me. “It is really much bigger than the computers.” Aven did not elaborate, but Jeffrey Birnbaum, a spokesperson for Alfa Bank, supplied more detail. The bank, he said, suspected that “we are victims of classic Russian *kompromat*—a well-known scam in which Russian competitors pay analysts to write false reports to damage reputations.” Birnbaum described the press inquiries into the matter as an extended affliction. “This has been a terrible ordeal for Alfa Bank, like living through a Kafka novel,” he said. (Max rejected the idea that his group had fabricated data. “If we were going to lie, then we would have made up a much better story than this!” he said.)

Because Alfa Bank did not retain its D.N.S. logs (many large companies don’t), its assessments of what produced the lookups in early 2016 are necessarily speculative. “We are as mystified as anybody about these false allegations,”

Birnbaum told me this September. In a series of exchanges over three weeks, he offered a range of possibilities. He suggested that the data had been faked, but also that they had been stolen from the bank's logs. He attributed the traffic to *kompromat*, but also expounded a scenario in which it had been caused by a technical glitch: Trump e-mails "hidden" in the system were intermittently processed by the bank's security software, an application called Trend Micro Deep Discovery Inspector. In this explanation, Trump marketing e-mails from before March, 2016, had made it through the spam filter and been stored in a permanent archive, where the bank backs up all its e-mail. Periodically, the bank re-scanned that archive, as updates to the security software provided new information about which senders might be unsafe. During scans, the system performed D.N.S. lookups for every domain name contained in every e-mail. In the course of several months, the bank said, this could account for the traffic.

The experts I spoke to confirmed that this was a technically plausible, if highly inefficient, way to configure security software. But the explanation raised questions of its own. Alfa Bank said that its scans ran for two days after each update. But Max's data don't show a consistent pattern of two-day spikes. Another concern lay in the chronology. The bank had received e-mails from the Trump domain in late 2015 and early 2016, which should have triggered lookups. But, according to the data, the lookups didn't begin until May, 2016. In response to a question about this discrepancy, Birnbaum said that the Trend Micro software had not been "fully integrated" until March—but that wouldn't account for the time between March and May.

A third problem was that, if Alfa Bank wasn't receiving new e-mails from the Trump Organization after March, 2016, then the number of Trump e-mails in the archive—and thus the number of lookups—should have remained steady through the summer. But Max's data showed a different pattern: no lookups in the spring, a small number in May, and then a slow increase starting in June, with spikes that lasted until the system went offline. When asked about the increase, Birnbaum

offered another refinement of the explanation. The bank had previously said that the software had performed checks of old e-mails "multiple times over the six-month period." Now he said that a security update "around August" had caused old e-mails to be re-scanned.

In any case, for an explanation of this kind to work, it would require the servers at Spectrum Health to be simultaneously experiencing the same glitch, or another one with similar effects. (Spectrum declined to answer questions about its computer systems.) Trend Micro has thousands of users, most of them businesses, but in the sample that Max and his colleagues could see, only Alfa Bank and Spectrum Health exhibited this peculiar behavior.

For some, the most baffling part of the puzzle was the way that the lookups stopped. The Trump domain vanished from the Web on the morning of Friday, September 23rd, two days after the *Times* presented its data to B.G.R., Alfa Bank's lobbyists in Washington, but before it called Trump or Cendyn. In Max's view, this was evidence of direct contact between Alfa Bank and Trump. One researcher whom Foer interviewed put it vividly: "The knee was hit in Moscow, the leg kicked in New York." There is, however, at least one possibility that doesn't involve Moscow: the lobbyists in Washington could have passed along a warning to Trump, as a courtesy. But B.G.R. denies doing this, calling the idea "ridiculous on its face."

Whatever the reason that the Trump domain vanished, Alfa Bank's servers continued trying to look it up: Max's group observed fifteen failed attempts that Friday, twenty-eight on Saturday, none on Sunday, ninety on Monday, twenty on Tuesday. Spectrum Health's machine kept trying, too, in a weeklong spasm of activity that entailed thousands of seemingly automated lookups. Spectrum never succeeded in relocating the Trump server—but Alfa did. On the night of Tuesday, September 27th, ten minutes after the bank made its last failed attempt, it looked up the domain name trump1.contact-client.com—which was, it turned out, another route to the same Trump server.

The alternative domain name does not appear to have been previously active; no one has produced an e-mail sent from it. So how did Alfa find it? The easiest method would have been by consulting a PTR record, which shows what domain names are associated with a given I.P. address. But the PTR record for the Trump address did not include the alternative name.

Birnbaum said that Alfa Bank's researchers, investigating the traffic, found the new name in other public records and then performed a test lookup. Vixie said that such a lookup would be unusual, and questioned why the bank would feel that it was necessary: "Why did Alfa look up either name? And especially the second name?"

According to Max's data, Alfa Bank looked up the new domain name only once. In the following months, he and his group stopped collecting data on the Trump Organization domains. After the Slate story came out, curious readers looked up the address thousands of times, and the D.N.S. traffic devolved into statistical noise. The Trump Organization now controls the original domain; in March, 2017, Cendyn told CNN that it had been "transferred back." Records show that Cendyn handed over the domain only a few days before the CNN story ran—a year after the last e-mail was sent from it. Jones's team believed that Cendyn had continued its relationship with the Trump Organization in 2016. "There were thousands of e-mails between Trump and Cendyn through the entire period that Alfa Bank was looking up the Trump server," Max told me. Cendyn said that this was "regular business correspondence," related to transferring back the domain. When I called the company's C.E.O., Richard Deyo, to ask more broadly about the situation, he said, "This is old news—that's just Internet traffic," and then hung up. A spokesperson for Serenata, which took over Trump's hotel marketing, told me that the company had nothing to say. "Don't call again," she said.

As Jones's team sifted through explanations for the traffic, they began constructing their own theory. "What you have here is a minimally viable

technical footprint of a small number of people who are using what I suspect is an ad-hoc system to communicate," Paul said. "Anytime the F.B.I. or anyone else pulls apart a cyber-crime organization, there is always some communication structure that's used for command and control. That's where the high-value communications happen." (Max and his colleagues did not see any D.N.S. evidence that the Trump Organization was attempting to access the server; they speculated that the organization was using a virtual private network, or V.P.N., a common security measure that obscures users' digital footprints.)

If this was a communications mechanism, it appeared to have been relatively simple, suggesting that it had been set up spontaneously and refined over time. Because the Trump Organization did not have administrative control of the server, Paul and Leto theorized that any such system would have incorporated software that one of the parties was already using. "The likely scenario is not that the people using the server were incredibly sophisticated networking geniuses doing something obscure and special," Max said. "The likely scenario is that they adapted a server and vender already available to them, which they felt was away from prying eyes." Leto told me that he envisioned "something like a bulletin-board system." Or it could have been an instant-messaging system that was part of software already in use on the server.

Kramer, of Listrak, insisted that his company's servers were used exclusively for mass marketing. "We only do one thing here," he told me. But Listrak's services can be integrated with numerous Cendyn software packages, some of which allow instant messaging. One possibility is Metron, used to manage events at hotels. In fact, the Trump Organization's October, 2016, statement, blaming the unusual traffic on a "banking customer" of Cendyn, suggested that the communications had gone through Metron, which supports both messaging and e-mail.

The parties might also have been using Webmail—e-mail that leaves few digital traces, other than D.N.S. lookups. Or, Paul and Leto said, they could have been communicating through software used to compose marketing e-mails. They might

have used a method called foldering, in which messages are written but not sent; instead, they are saved in a drafts folder, where an accomplice who also has access to the account can read them. “This is a very common way for people to communicate with each other who don’t want to be detected,” Leto told me. David Petraeus, when he was the director of the C.I.A., used this method to exchange intimacies—and to share classified information—with his lover, Paula Broadwell. In June, an attorney for the Mueller investigation accused Paul Manafort of using foldering to facilitate secret communications.

Given the limitations of D.N.S. data, none of the independent experts I spoke to could be certain of what Alfa Bank and the Trump Organization were doing. Some of them cautioned that it was impossible even to guess at every way that an e-mail system might malfunction. A senior analyst at a D.N.S.-service provider said, “Things can get messed up in unexpected ways.” But Paul and Leto maintained that they had considered and rejected every scenario that they had encountered in decades of cybersecurity work. “Is it possible there is an innocuous explanation for all this?” Paul said. “Yes, of course. And it’s also possible that space aliens did this. It’s possible—just not very likely.”

Paul and Leto periodically went back to Max in the course of their research, interrogating his assumptions and asking for more information. In one tranche of data that he gave them, they noticed that a third entity, in addition to Alfa Bank and Spectrum Health, had been looking up the Trump domain: Heartland Payment Systems, a payments processor based in Princeton. Of the thirty-five hundred D.N.S. queries seen for the Trump domain, Heartland made only seventy-six—but no other visible entity made more than two. Heartland had a link to Alfa Bank, but a tenuous one. It had recently been acquired by Global Payments, which, in 2009, had paid seventy-five million dollars for United Card Services, Russia’s leading credit-card-processing company; two years later, United Card Services bought Alfa Bank’s credit-card-processing unit. (A spokesperson for Global Payments said that her company had never had any relationship with the Trump

Organization or with Alfa Bank, and that its U.S. and Russia operations functioned entirely independently.)

Spectrum Health has a similarly indirect business tie to Alfa Bank. Richard DeVos' father co-founded Amway, and his brother, Doug, has served as the company's president since 2002. In 2014, Amway joined with Alfa Bank to create an "Alfa-Amway" loyalty-card program in Russia. But such connections are circumstantial at best; the DeVos family seems far more clearly linked to Trump than to Russia.

If Trump and Alfa Bank—as well as Spectrum Health and Heartland Payment Systems—were communicating, what might they have been talking about? Max and some of the other scientists I spoke to theorized that they may have been using the system to signal one another about events or tasks that had to be performed: money to be transferred, for instance, or data to be copied. "My guess is that, whenever someone wanted to talk, they would do a D.N.S. lookup and then route the traffic somewhere else," Richard Clayton, of the University of Cambridge, said. Camp also speculated that the system may have been used to coördinate the movement of data. She noted that Cambridge Analytica, which was working for the Trump campaign, took millions of personal records from Facebook. In Camp's scenario, these could have been transferred to the Russian government, to help guide its targeting of American voters before the election.

The researchers I spoke with were careful to point out that the limits of D.N.S. data prevent them from going beyond speculation. If employees of the companies were talking, the traffic reveals nothing about who they were or what they were saying; it is difficult to rule out something as banal as a protracted game of video poker. "If I'm a cop, I'm not going to take this to the D.A. and say we're ready to prosecute," Leto said. "I'm going to say we have enough to ask for a search warrant." More complete information could be difficult to obtain. This March, after Republicans on the House Intelligence Committee announced that it had

found no evidence of collusion between the Trump campaign and Russia, the committee's Democrats filed a dissent, arguing that there were many matters still to be investigated, including the Trump Organization's connections to Alfa Bank. The Democrats implored the majority to force Cendyn to turn over computer data that would help determine what had happened. Those records could show who in the Trump Organization used the server. There would probably also be a record of who shut down the Trump domain after the *Times* contacted Alfa Bank. Cendyn might have records of any outgoing communications sent by the Trump Organization. But the request for further investigation is unlikely to proceed as long as Republicans hold the majority. "We've all looked at the data, and it doesn't look right," a congressional staffer told me. "But how do you get to the truth?"

The enigma, for now, remains an enigma. The only people likely to finally resolve the question of Alfa Bank and the Trump Organization are federal investigators. Max told me that no one in his group had been contacted. But, he said, it wasn't necessary for anyone in the F.B.I. to talk to him, if the agents gathered the right information from other sources, like Listrak and Cendyn. "I hope Mueller has all of it," he said. ♦

Published in the print edition of the October 15, 2018, issue, with the headline "Enigma Machines."

Dexter Filkins is a staff writer at The New Yorker and the author of "The Forever War," which won a National Book Critics Circle Award.

More: Cybersecurity Hacking 2016 Election Elections Democratic National Committee Russia Trump Organization Collusion Donald Trump

Read More

News Desk

Trump and Putin: A Love Story

The attraction is mutual, but history shows who's really using whom.

By David Remnick

Annals of Diplomacy

Trump, Putin, and the New Cold War

What lay behind Russia's interference in the 2016 election—and what lies ahead?

By Evan Osnos,David Remnick, and Joshua Yaffa

A Reporter at Large

Deutsche Bank's $10-Billion Scandal

How a scheme to help Russians secretly funnel money offshore unravelled.

By Ed Caesar

Annals of Justice

Why Corrupt Bankers Avoid Jail

Prosecution of white-collar crime is at a twenty-year low.

By Patrick Radden Keefe

Currency

Wells Fargo and a New Age of Banking Scandals

By Sheelah Kolhatkar

Q. & A.

What Could Happen if the U.S. Abandons Europe

Donald Trump's disdain for NATO will reshape the domestic politics—and military posture—of some of America's closest allies.

By Isaac Chotiner

The New Yorker Radio Hour

Richard Brody Presents the 2025 Brody Awards

Oscar who? The film critic, a true believer in the art of cinema, picks the winners of the most coveted award of all: the Brodys.

The New Yorker Radio Hour

John Fetterman on Trump's "Raw Sewage," and What the Democrats Get Wrong

The Pennsylvania senator says the Administration is dumping "three feet of raw sewage" on America, "and we have a Dixie cup" to bail it out. But Democrats have to work with Trump.

Humor

Daily Cartoon: Friday, February 21st

"No, Mr. Bond, I expect you to star in a series of increasingly bland spinoffs and TV shows that have significant viewership decline after the first episode."

By Ellis Rosen

Fault Lines

A Profoundly Empathetic Book on Homelessness in the Bay Area

Kevin Fagan's new work moves beyond predictable policy critique to offer a powerful reminder of the moral side of the crisis.

By Jay Caspian Kang

Crossword

The Mini Crossword: Friday, February 21, 2025

Meerkat who sings “Hakuna Matata” with Pumbaa, in “The Lion King”: five letters.

By Kate Chin Park

On Television

“The White Lotus” Overstays Its Welcome

In the third season of Mike White’s HBO satire of the rich and terrible, a now familiar formula yields diminishing returns.

By Inkoo Kang