The Intercept_

TOP-SECRET NSA REPORT DETAILS RUSSIAN HACKING EFFORT DAYS BEFORE 2016 ELECTION

Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim

June 5 2017, 3:44 p.m.

Photo Illustration: The Intercept

LEIA EM PORTUGUÊS ⟶

Russian military intelligence executed a cyberattack on at least one U.S. voting software supplier and sent spear-phishing emails to more than 100 local election officials just days before last November's presidential

election, according to a highly classified intelligence report obtained by The Intercept.

The top-secret National Security Agency document, which was provided anonymously to The Intercept and independently authenticated, analyzes intelligence very recently acquired by the agency about a months-long Russian intelligence cyber effort against elements of the U.S. election and voting infrastructure. The report, dated May 5, 2017, is the most detailed U.S. government account of Russian interference in the election that has yet come to light.

While the document provides a rare window into the NSA's understanding of the mechanics of Russian hacking, it does not show the underlying "raw" intelligence on which the analysis is based. A U.S. intelligence officer who declined to be identified cautioned against drawing too big a conclusion from the document because a single analysis is not necessarily definitive.


TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

[redacted] DIRNSA

National Security Agency

Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, [redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to

FVEY/FISA)

NSA Report on Russia Spearphishing
5 pages

on in this report is provided for intelligence purposes
on contained in this report, nor any information derived
therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any

The report indicates that Russian hacking may have penetrated further into U.S. voting systems than was previously understood. It states unequivocally in its summary statement that it was Russian military intelligence, specifically the Russian General Staff Main Intelligence Directorate, or GRU, that conducted the cyber attacks described in the document:

> Russian General Staff Main Intelligence Directorate actors … executed cyber espionage operations against a named U.S. company in August 2016, evidently to obtain information on elections-related software and hardware solutions. … The actors likely used data obtained from that operation to … launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations.

This NSA summary judgment is sharply at odds with Russian President Vladimir Putin's denial last week that Russia had interfered in foreign elections: "We never engaged in that on a state level, and have no intention of doing so." Putin, who had previously issued blanket denials that

any such Russian meddling occurred, for the first time floated the possibility that freelance Russian hackers with "patriotic leanings" may have been responsible. The NSA report, on the contrary, displays no doubt that the cyber assault was carried out by the GRU.

The NSA analysis does not draw conclusions about whether the interference had any effect on the election's outcome and concedes that much remains unknown about the extent of the hackers' accomplishments. However, the report raises the possibility that Russian hacking may have breached at least some elements of the voting system, with disconcertingly uncertain results.

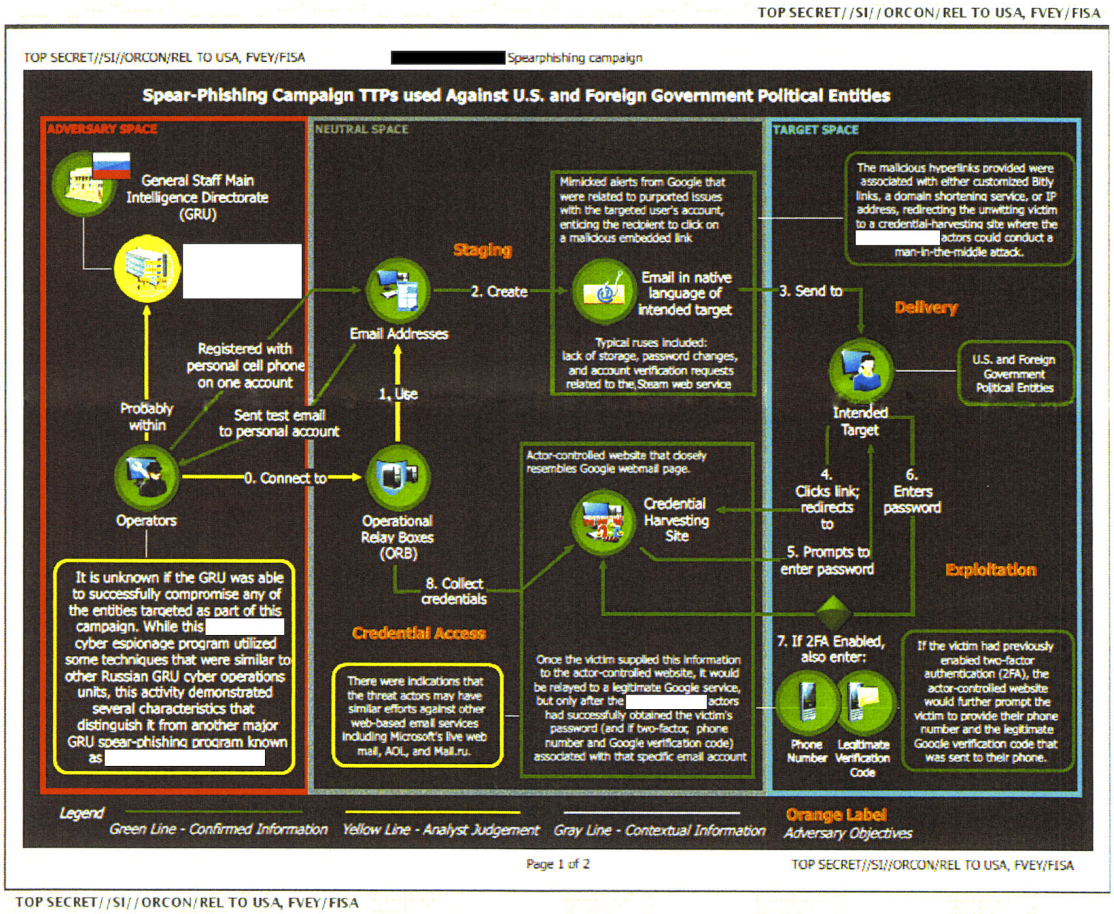
The NSA and the Office of the Director of National Intelligence were both contacted for this article. Officials requested that we not publish or report on the top secret document and declined to comment on it. When informed that we intended to go ahead with this story, the NSA requested a number of redactions. The Intercept agreed to some of the redaction requests after determining that the disclosure of that material was not clearly in the public interest.

The report adds significant new detail to the picture that emerged from the unclassified intelligence assessment about Russian election meddling released by the Obama administration in January. The January assessment presented the U.S. intelligence community's conclusions but omitted many specifics, citing concerns about disclosing sensitive sources and methods. The assessment concluded with high confidence that the Kremlin ordered an extensive, multi-pronged propaganda effort "to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency."

That review did not attempt to assess what effect the Russian efforts had on the election, despite the fact that "Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards." According to the Department of Homeland Security, the assess-

ment reported reassuringly, "the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying."

The NSA has now learned, however, that Russian government hackers, part of a team with a "cyber espionage mandate specifically directed at U.S. and foreign elections," focused on parts of the system directly connected to the voter registration process, including a private sector manufacturer of devices that maintain and verify the voter rolls. Some of the company's devices are advertised as having wireless internet and Bluetooth connectivity, which could have provided an ideal staging point for further malicious actions.



Attached to the secret NSA report is an overview chart detailing the Russian government's spear-phishing operation, apparently missing a second page that was not provided to The Intercept. Graphic: NSA

The Spear-Phishing Attack

As described by the classified NSA report, the Russian plan was simple: pose as an e-voting vendor and trick local government employees into opening Microsoft Word documents invisibly tainted with potent malware that could give hackers full control over the infected computers.

But in order to dupe the local officials, the hackers needed access to an election software vendor's internal systems to put together a convincing disguise. So on August 24, 2016, the Russian hackers sent spoofed emails purporting to be from Google to employees of an unnamed U.S. election software company, according to the NSA report. Although the document does not directly identify the company in question, it contains references to a product made by VR Systems, a Florida-based vendor of electronic voting services and equipment whose products are used in eight states.

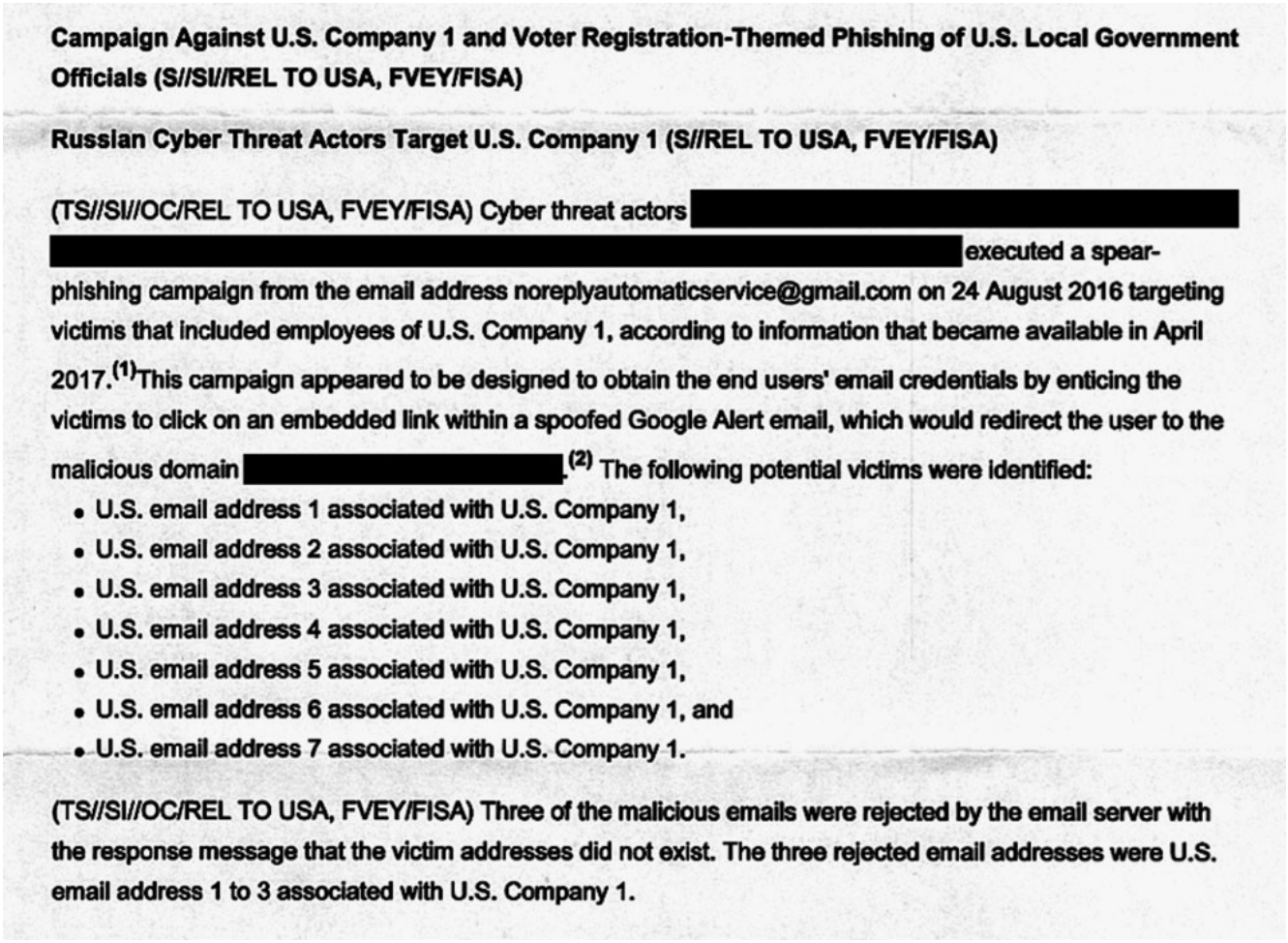
The spear-phishing email contained a link directing the employees to a malicious, faux-Google website that would request their login credentials and then hand them over to the hackers. The NSA identified seven "potential victims" at the company. While malicious emails targeting three of the potential victims were rejected by an email server, at least one of the employee accounts was likely compromised, the agency concluded. The NSA notes in its report that it is "unknown whether the aforementioned spear-phishing deployment successfully compromised all the intended victims, and what potential data from the victim could have been exfiltrated."

VR Systems declined to respond to a request for comment on the specific hacking operation outlined in the NSA document. Chief Operating Officer Ben Martin replied by email to The Intercept's request for comment with the following statement:

> Phishing and spear-phishing are not uncommon in our industry. We regularly participate in cyber alliances with state officials and members of the law enforcement community in an effort to ad-

> dress these types of threats. We have policies and procedures in effect to protect our customers and our company.

Although the NSA report indicates that VR Systems was targeted only with login-stealing trickery, rather than computer-controlling malware, this isn't necessarily a reassuring sign. Jake Williams, founder of computer security firm Rendition Infosec and formerly of the NSA's Tailored Access Operations hacking team, said stolen logins can be even more dangerous than an infected computer. "I'll take credentials most days over malware," he said, since an employee's login information can be used to penetrate "corporate VPNs, email, or cloud services," allowing access to internal corporate data. The risk is particularly heightened given how common it is to use the same password for multiple services. Phishing, as the name implies, doesn't require everyone to take the bait in order to be a success — though Williams stressed that hackers "never want just one" set of stolen credentials.



Campaign Against U.S. Company 1 and Voter Registration-Themed Phishing of U.S. Local Government Officials (S//SI//REL TO USA, FVEY/FISA)

Russian Cyber Threat Actors Target U.S. Company 1 (S//REL TO USA, FVEY/FISA)

(TS//SI//OC/REL TO USA, FVEY/FISA) Cyber threat actors [redacted] executed a spear-phishing campaign from the email address noreplyautomaticservice@gmail.com on 24 August 2016 targeting victims that included employees of U.S. Company 1, according to information that became available in April 2017.(1) This campaign appeared to be designed to obtain the end users' email credentials by enticing the victims to click on an embedded link within a spoofed Google Alert email, which would redirect the user to the malicious domain [redacted].(2) The following potential victims were identified:

- U.S. email address 1 associated with U.S. Company 1,
- U.S. email address 2 associated with U.S. Company 1,
- U.S. email address 3 associated with U.S. Company 1,
- U.S. email address 4 associated with U.S. Company 1,
- U.S. email address 5 associated with U.S. Company 1,
- U.S. email address 6 associated with U.S. Company 1, and
- U.S. email address 7 associated with U.S. Company 1.

(TS//SI//OC/REL TO USA, FVEY/FISA) Three of the malicious emails were rejected by the email server with the response message that the victim addresses did not exist. The three rejected email addresses were U.S. email address 1 to 3 associated with U.S. Company 1.

A detail from a top-secret NSA report on a Russian military intelligence operation targeting the U.S. election infrastructure. Image: NSA

In any event, the hackers apparently got what they needed. Two months later, on October 27, they set up an "operational" Gmail account designed to appear as if it belonged to an employee at VR Systems, and used documents obtained from the previous operation to launch a second spear-phishing operation "targeting U.S. local government organizations." These emails contained a Microsoft Word document that had been "trojanized" so that when it was opened it would send out a beacon to the "malicious infrastructure" set up by the hackers.

The NSA assessed that this phase of the spear-fishing operation was likely launched on either October 31 or November 1 and sent spear-fishing emails to 122 email addresses "associated with named local government organizations," probably to officials "involved in the management of

voter registration systems." The emails contained Microsoft Word attachments purporting to be benign documentation for VR Systems' EViD voter database product line, but which were in reality maliciously embedded with automated software commands that are triggered instantly and invisibly when the user opens the document. These particular weaponized files used PowerShell, a Microsoft scripting language designed for system administrators and installed by default on Windows computers, allowing vast control over a system's settings and functions. If opened, the files "very likely" would have instructed the infected computer to begin downloading in the background a second package of malware from a remote server also controlled by the hackers, which the secret report says could have provided attackers with "persistent access" to the computer or the ability to "survey the victims for items of interest." Essentially, the weaponized Word document quietly unlocks and opens a target's back door, allowing virtually any cocktail of malware to be subsequently delivered automatically.

According to Williams, if this type of attack were successful, the perpetrator would possess "unlimited" capacity for siphoning away items of interest. "Once the user opens up that email [attachment]," Williams explained, "the attacker has all the same capabilities that the user does." Vikram Thakur, a senior research manager at Symantec's Security Response Team, told The Intercept that in cases like this the "quantity of exfiltrated data is only limited by the controls put in place by network administrators." Data theft of this variety is typically encrypted, meaning anyone observing an infected network wouldn't be able to see what exactly was being removed but should certainly be able to tell something was afoot, Williams added. Overall, the method is one of "medium sophistication," Williams said, one that "practically any hacker can pull off."

The NSA, however, is uncertain about the results of the attack, according to the report. "It is unknown," the NSA notes, "whether the afore-

mentioned spear-phishing deployment successfully compromised the intended victims, and what potential data could have been accessed by the cyber actor."

The FBI would not comment about whether it is pursuing a criminal investigation into the cyber attack on VR Systems.

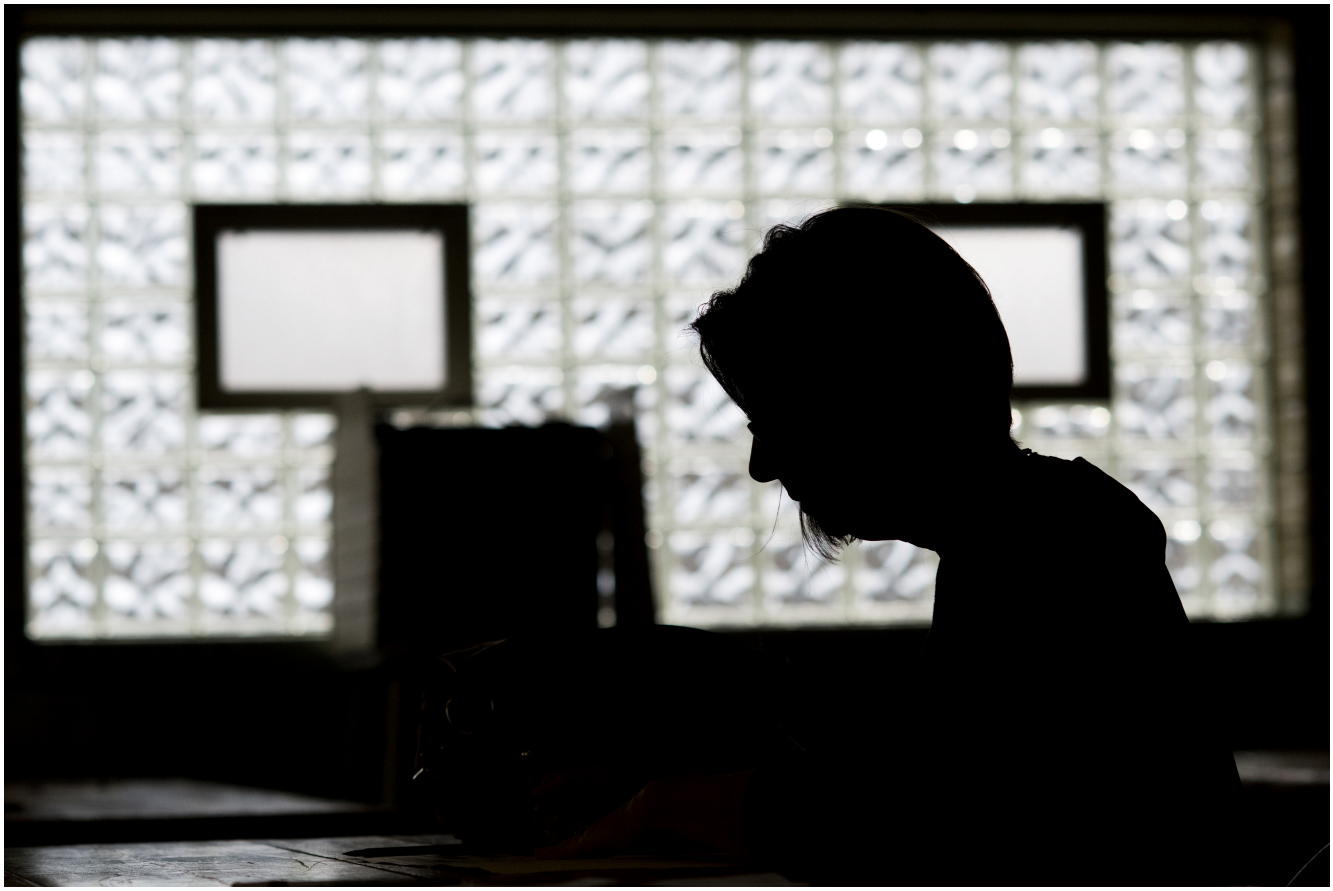
At a December press conference, President Obama said that he told Russian President Vladimir Putin in September not to hack the U.S. election infrastructure. "What I was concerned about in particular was making sure [the DNC hack] wasn't compounded by potential hacking that could hamper vote counting, affect the actual election process itself," Obama said. "So in early September, when I saw President Putin in China, I felt that the most effective way to ensure that that didn't happen was to talk to him directly and tell him to cut it out and there were going to be serious consequences if he didn't. And in fact we did not see further tampering of the election process."

Yet the NSA has now found that the tampering continued. "The fact that this is occurring in October is troubling," said one senior law enforcement official with significant cyber expertise. "In August 2016 warnings went out from the FBI and DHS to those agencies. This was not a surprise. This was not hard to defend against. But you needed a commitment of budget and attention."

The NSA document briefly describes two other election-related Russian hacking operations. In one, Russian military hackers created an email account pretending to be another U.S. election company, referred to in the document as U.S. company 2, from which they sent fake test emails offering "election-related products and services." The agency was unable to determine whether there was any targeting using this account.

In a third Russian operation, the same group of hackers sent test emails to addresses at the American Samoa Election Office, presumably to de-

termine whether those accounts existed before launching another phishing attack. It is unclear what the effort achieved, but the NSA assessed that the Russians appeared intent on "mimicking a legitimate absentee ballot-related service provider." The report does not indicate why the Russians targeted the tiny Pacific islands, a U.S. territory with no electoral votes to contribute to the election.



A voter casts her ballot on Nov. 8, 2016 in Ohio. Photo: Ty Wright/Getty Images

An Alluring Target

Getting attention and a budget commitment to election security requires solving a political riddle. "The problem we have is that voting security doesn't matter until something happens, and then after something happens, there's a group of people who don't want the security, because whatever happened, happened in their favor," said Bruce

Schneier, a cybersecurity expert at Harvard's Berkman Center who has written frequently about the security vulnerabilities of U.S. election systems. "That makes it a very hard security problem, unlike your bank account."

Schneier said the attack, as described by the NSA, is standard hacking procedure. "Credential-stealing, spear-phishing — this is how it's done," he said. "Once you get a beachhead, then you try to figure out how to go elsewhere."

All of this means that it is critical to understand just how integral VR Systems is to our election system, and what exactly the implications of this breach are for the integrity of the result.

VR Systems doesn't sell the actual touchscreen machines used to cast a vote, but rather the software and devices that verify and catalogue who's permitted to vote when they show up on Election Day or for early voting. Companies like VR are "very important" because "a functioning registration system is central to American elections," explained Lawrence Norden, deputy director of the Brennan Center for Justice at the NYU School of Law. Vendors like VR are also particularly sensitive, according to Norden, because local election offices "are often unlikely to have many or even any IT staff," meaning "a vendor like this will also provide most of the IT assistance, including the work related to programming and cyber security" — not the kind of people you want unwittingly compromised by a hostile nation state.

According to its website, VR Systems has contracts in eight states: California, Florida, Illinois, Indiana, New York, North Carolina, Virginia, and West Virginia.

Pamela Smith, president of election integrity watchdog Verified Voting, agreed that even if VR Systems doesn't facilitate the actual casting of

votes, it could make an alluring target for anyone hoping to disrupt the vote.

"If someone has access to a state voter database, they can take malicious action by modifying or removing information," she said. "This could affect whether someone has the ability to cast a regular ballot, or be required to cast a 'provisional' ballot — which would mean it has to be checked for their eligibility before it is included in the vote, and it may mean the voter has to jump through certain hoops such as proving their information to the election official before their eligibility is affirmed."

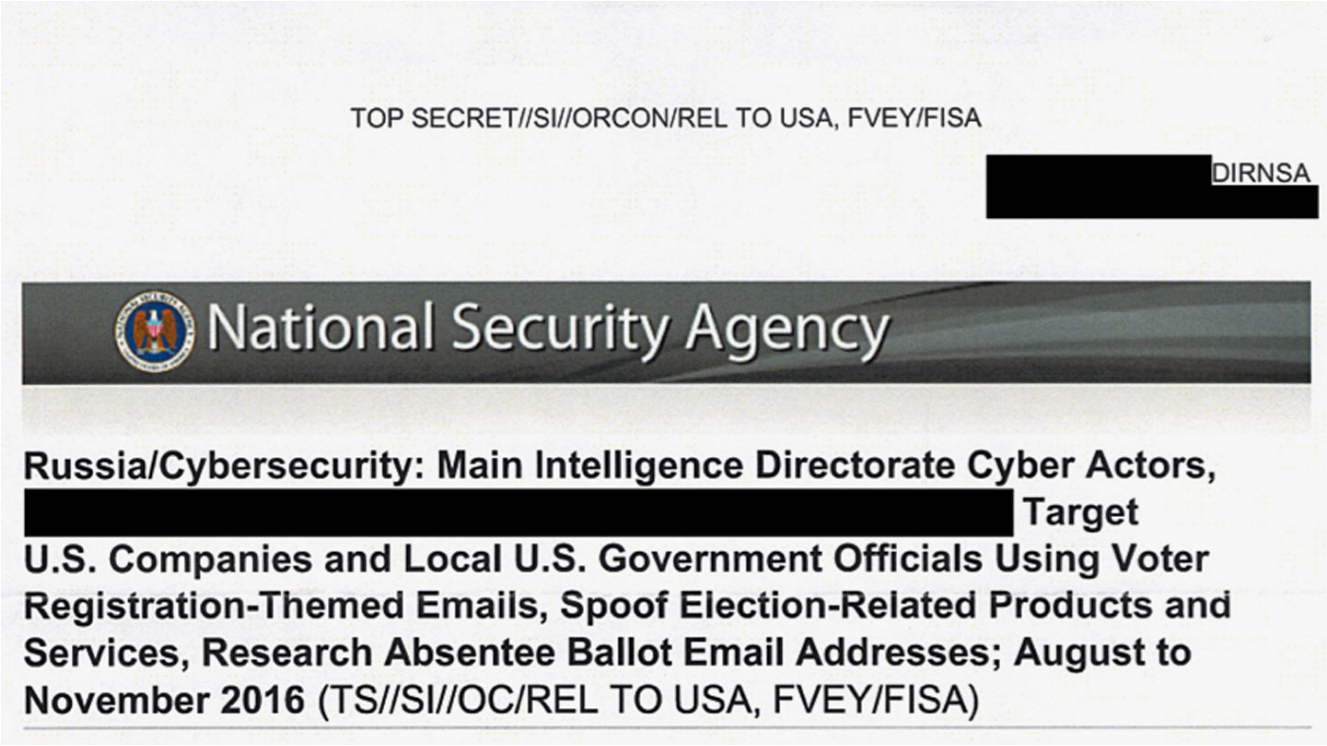
Mark Graff, a digital security consultant and former chief cybersecurity officer at Lawrence Livermore National Lab, described such a hypothetical tactic as "effectively a denial of service attack" against would-be voters. But a more worrying prospect, according to Graff, is that hackers would target a company like VR Systems to get closer to the actual tabulation of the vote. An attempt to directly break into or alter the actual voting machines would be more conspicuous and considerably riskier than compromising an adjacent, less visible part of the voting system, like voter registration databases, in the hope that one is networked to the other. Sure enough, VR Systems advertises the fact that its EViD computer polling station equipment line is connected to the internet, and that on Election Day "a voter's voting history is transmitted immediately to the county database" on a continuous basis. A computer attack can thus spread quickly and invisibly through networked components of a system like germs through a handshake.

According to Alex Halderman, director of the University of Michigan Center for Computer Security and Society and an electronic voting expert, one of the main concerns in the scenario described by the NSA document is the likelihood that the officials setting up the electronic poll books are the same people doing the pre-programming of the voting machines. The actual voting machines aren't going to be networked

to something like VR Systems' EViD, but they do receive manual updates and configuration from people at the local or state level who could be responsible for both. If those were the people targeted by the GRU malware, the implications are troubling.

"Usually at the county level there's going to be some company that does the pre-election programming of the voting machines," Halderman told The Intercept. "I would worry about whether an attacker who could compromise the poll book vendor might be able to use software updates that the vendor distributes to also infect the election management system that programs the voting machines themselves," he added. "Once you do that, you can cause the voting machine to create fraudulent counts."

According to Schneier, a major prize in breaching VR Systems would be the ability to gather enough information to effectively execute spoof attacks against election officials themselves. Coming with the imprimatur of the election board's main contractor, a fake email looks that much more authentic.



TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

[redacted] DIRNSA

National Security Agency

Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, [redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)

A detail from a top-secret NSA report on a Russian military intelligence operation targeting the U.S. election infrastructure. Image: NSA

Such a breach could also serve as its own base from which to launch disruptions. One U.S. intelligence official conceded that the Russian operation outlined by the NSA — targeting voter registration software — could potentially have disrupted voting in the locations where VR Systems' products were being used. And a compromised election poll book system can do more than cause chaos on Election Day, said Halderman. "You could even do that preferentially in areas for voters that are likely to vote for a certain candidate and thereby have a partisan effect."

Using this method to target a U.S. presidential election, the Russian approach faces a challenge in the decentralized federal election system, where processes differ not merely state to state but often county to county. And meanwhile, the Electoral College makes it difficult to predict where efforts should be concentrated.

"Hacking an election is hard, not because of technology — that's surprisingly easy — but it's hard to know what's going to be effective," said Schneier. "If you look at the last few elections, 2000 was decided in Florida, 2004 in Ohio, the most recent election in a couple counties in Michigan and Pennsylvania, so deciding exactly where to hack is really hard to know."

But the system's decentralization is also a vulnerability. There is no strong central government oversight of the election process or the acquisition of voting hardware or software. Likewise, voter registration, maintenance of voter rolls, and vote counting lack any effective national oversight. There is no single authority with the responsibility for safeguarding elections. Christian Hilland, a spokesperson for the FEC, told The Intercept that "the Federal Election Commission does not have jurisdiction over voting matters as well as software and hardware in con-

nection with casting votes. You may want to check with the Election Assistance Commission."

Checking with the EAC is also less than confidence inspiring. The commission was created in 2002 as the congressional reaction to the vote-counting debacle of 2000. The EAC notes online that it "is charged with serving as a national clearinghouse of information on election administration. EAC also accredits testing laboratories and certifies voting systems," but it is a backwater commission with no real authority. Click on the link about certifying voting systems and it leads you to a dead page.

If there were a central U.S. election authority, it might have launched an investigation into what happened in Durham, North Carolina, on Election Day. The registration system malfunctioned at a number of polling locations, causing chaos and long lines, which triggered election officials to switch to paper ballots and extend voting later into the evening.

Durham's voter rolls were run by VR Systems — the same firm that was compromised by the Russian hack, according to the NSA document.

Local officials said that a hack was not the cause of the disruption. "The N.C. State Board of Elections did not experience any suspicious activity during the 2016 election outside of what this agency experiences at other times. Any potential risks or vulnerabilities are being monitored, and this agency works with the Department of Homeland Security and the N.C. Department of Information Technology to help mitigate any potential risks," said Patrick Gannon, a spokesperson for the North Carolina board of elections.

George McCue, deputy director of the Durham County board of elections, also said that VR Systems' software was not the issue. "There was some investigation there, essentially no evidence came out of it indicating there was any problem with the product," he said. "It appears to be

user errors at different points in the process, between the setup of the computers and the poll workers using them."

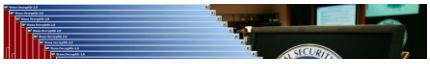
All of this taken together ratchets up the stakes of the ongoing investigations into collusion between the Trump campaign and Russian operatives, which promises to soak up more national attention this week as fired FBI Director James Comey appears before Congress to testify. If collusion can ultimately be demonstrated — a big if at this point — then the assistance on Russia's part went beyond allegedly hacking email to serve a propaganda campaign, and bled into an attack on U.S. election infrastructure itself.

Whatever the investigation into the Trump campaign concludes, however, it pales in comparison to the threat posed to the legitimacy of U.S. elections if the infrastructure itself can't be secured. The NSA conclusion "demonstrates that countries are looking at specific tactics for election manipulation, and we need to be vigilant in defense," said Schneier. "Elections do two things: one choose the winner, and two, they convince the loser. To the extent the elections are vulnerable to hacking, we risk the legitimacy of the voting process, even if there is no actual hacking at the time."

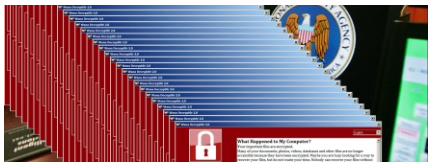
Throughout history, the transfer of power has been the moment of greatest weakness for societies, leading to untold bloodshed. The peaceful transfer of power is one of the greatest innovations of democracy.

"It's not just that [an election] has to be fair, it has to be demonstrably fair, so that the loser says, 'Yep, I lost fair and square.' If you can't do that, you're screwed," said Schneier. "They'll tear themselves apart if they're convinced it's not accurate."

RELATED



Leaked NSA Malware Is Helping Hijack Computers Around the World



Sen. Ron Wyden Talks Trump-Russia, "Warrantless Backdoor Queries" and Hacking of U.S. Phone System