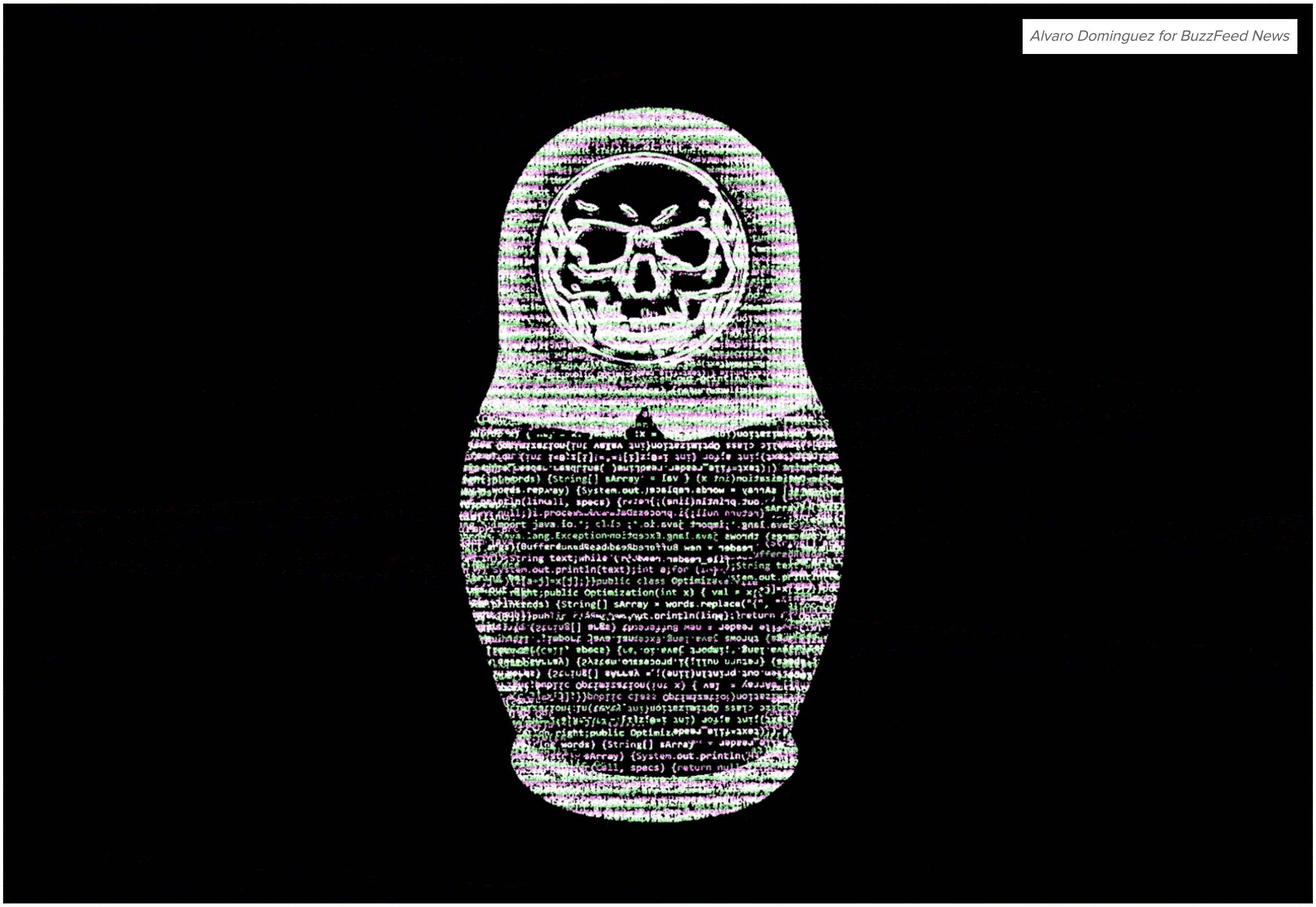


Alvaro Dominguez for BuzzFeed News

The New Handbook For Cyberwar Is Being Written By Russia

"It's not that the Russians are doing something others can't do," a US intelligence officer said. "It's that Russian hackers are willing to go there, to experiment and carry out attacks that others countries would back away from."

Sheera Frenkel
BuzzFeed News Reporter

posted on Mar. 19, 2017, at 5:15 p.m.

SAN FRANCISCO — It was just before midnight on Dec. 17, 2016, when most of the Ukrainian capital, Kiev, went dark.

A transmission station, a type of power station that transmits high voltage electricity across large areas, had gone down. Vsevolod Kovalchuk, the head of Ukrainian state power grid operator Ukrenergo, explained on his Facebook page that the station had come under an "external attack" lasting roughly 30 minutes.

It was, cybersecurity experts said, the most recent maneuver in Russia's increasingly aggressive and overt efforts to push the boundaries of modern-day warfare using everything from old-fashioned kompromat, the Russian term for publishing (real or fake) compromising material designed to smear opponents, to malware that blacks out cities.

"The Russians use cyberweapons like they butter bread in the morning. It's a critical, fundamental component of their global hybrid warfare strategy. They are pushing the envelope on how they use it every day," said Malcolm Nance, a former counterterrorism and intelligence officer for the US military, intelligence agencies, and the Department of Homeland Security. "Ukraine is just one of many test beds."

If the world is currently entering a new era of cyberwarfare, Russian hackers are the pirates of those yet-uncharted seas. Nearly every week brings a new cyberattack, as Russia tests the vulnerabilities of countries around the world. From hacking into the emails of senior members of the Democratic Party to defacing the websites of Eastern European political candidates, Russia is being named as the perpetrator of the most audacious cyberattacks in recent years. In some cases, those attacks are acts of espionage, looking to sweep up as much intelligence as possible. In others, Russia is toying with psychological operations, teasing out their geopolitical goals. Just this week, the Department of Justice (DOJ) announced that a 2014 breach of Yahoo, which exposed more than 500 million email accounts, had actually been the work of Russian Federal Security Service (FSB) agents working with cybercriminals — one of the largest email breaches in history, targeting, the DOJ said, the email accounts of a small group of journalists, dissidents, and US government officials.

For years, the world's top military leadership has been saying that cyberwarfare is simply warfare fought in today's world. In pushing forward, Russia is testing the limits of what other countries will tolerate as acts of war and setting an example for countries around the world as to what can be accomplished with a military budget roughly one-tenth the size of the United States.

The attack that blanketed Kiev in darkness took place almost a year to the day after the first known attack on an electrical system. In a cyberattack widely attributed to Russian state-sponsored hackers, dozens of power substations in the Ivano-Frankivsk region of Ukraine were disabled, shutting off power to nearly a quarter of a million people. Cybersecurity experts had long theorized that such an attack was possible, but assumed that few countries would be willing to launch such a blatant act of cyberwar for fear of retribution. Now, those same experts are studying the second such attack in 12 months, as it becomes increasingly clear that Russia is using its hackers to achieve key strategic goals — and push its adversaries around with impunity.

Russia's involvement in the most brazen attack on the US, the email breach of senior Democratic Party members, resulted in only minor sanctions on Russian officials and the expelling of 35 Russian diplomats (though the US claims that they are retaliating in other, unseen ways). "Look, we're moving into a new era here where a number of countries have significant capacities," Barack Obama, then president, said during a September 2016 appearance at the annual G20 summit in China, just after he had ordered US intelligence agencies to review foreign interference in the US election. Obama added that he had been in discussions with China, as well as Russia, on creating rules for cyberwarfare. "Our goal is not to suddenly, in the cyber arena, duplicate a cycle of escalation that we saw when it comes to other arms races in the past."

One US intelligence officer currently involved in cyber ops said, "It's not that the Russians are doing something others can't do. It's not as though, say, the US wouldn't have the technical skill level to carry out those types of attacks. It's that Russian hackers are willing to go there, to experiment and carry out attacks that other countries would back away from," said the officer, who asked not to be quoted by name due to the sensitivity of the subject. "It's audacious, and reckless. They are testing things out in the field and refining them, and a lot of it is very, very messy and some is very smart."

Cybersecurity experts generally agree that the countries with the largest and most sophisticated cyberwarfare capabilities are the United States, China, and Russia. Nance, who recently wrote *The Plot to Hack America*, a book examining Russia's alleged interference in the 2016 election, compared US cyber operations to a precision bullet, handcrafted, repeatedly tested, and produced in duplicate before one is ever used in the field. The US, for example, targeted the centrifuges in an Iranian nuclear facility via Stuxnet, a virus likely built in conjunction with Israel, rather than use cyberattacks that attacked financial institutions or infrastructure that would have had widespread impacts on average Iranian citizens. China, while in some ways every bit as audacious and aggressive in its cyber ops as Russia, has thus far remained focused on economic gain, corporate cyber espionage, or the general type of intelligence gathering most countries take part in.

"Russia is using cyber weapons to try and achieve geopolitical goals," said Nance. "And it is working."

"Russia is using cyber weapons to try and achieve geopolitical goals," said Nance. "And it is working."

The December 2015 attack on the Ivano-Frankivsk region of Western Ukraine cut power to some regions for as long as six hours. The December 2016 one cast much of Kiev in darkness for roughly 75 minutes. Neither is known to have caused injuries or deaths, yet the attacks are still being studied by cybersecurity experts and government bodies across the world.

There are few cyberattacks that inspire as much fear among the general public, as much panic among lawmakers, as those on a country's source of electricity. Hospitals suddenly left without the power to operate incubators for babies or life-support machines, airports blinded as pilots struggle to land, and major metropolises thrown into a literal pitch blackness are some of the doomsday scenarios that cybersecurity experts have painted if a coordinated attack were to one day be launched on a country's source of electricity.

"The US is terrified of it," said Robert M. Lee, a former cyberwarfare operations officer for the US Air Force and co-founder of Dragos Security, a security company that specializes in critical infrastructure. Lee was part of a team that investigated and produced a report on the 2015 attack on Ukraine's power grid. "Although a lot of people don't actually understand what an attack on a power grid means, or what can actually be achieved. There is a huge disconnect between what DC thinks can be done with a power grid and what can actually be done. The effects are more psychological than anything else."

Even a sophisticated cyberattack would likely only take power out for a half hour to an hour, say cybersecurity experts, and many institutions, such as hospitals or airports, have backup generators and emergency plans in place were they to suddenly lose power.

Russia, say current US intelligence officers, knew the psychological impact even a short-term outage of Ukraine's power grid would have on officials in the US and Europe, who know they are vulnerable to similar attacks. Four active US intelligence officers who agreed to speak to BuzzFeed News on condition of anonymity regarding the 2015 and 2016 attacks on Ukraine all used the term "game changer."

> "The effects are more psychological than anything else."

"It's not that the US can't defend against it. It's just that from our point of view, a foreign state being able to take down your power grid — even for 10 minutes — that's a game changer," said one of the officers, who like others asked for anonymity because they didn't have permission to speak publicly about the topic. "That's why we are studying what happened in Ukraine and trying to learn from it."

The 2015 cyberattack on Ukraine was achieved by attacking a number of power substations, said Lee.

“About 70 substations were disconnected from the power grid. All of the attacks except one were malware-enabled,” said Lee, whose report details the steps taken by hackers in bringing down the power station. In all but one substation, hackers used spear-phishing emails (emails that appear innocent but include malicious links or malware) as an initial point of entry. It’s a method favored by Russian hackers, say cybersecurity researchers, who say spear-phishing emails were also used to get into the email accounts of senior members of the Democratic Party. In Ukraine, the hackers used the spear-phishing emails to trick computer users at the power stations into downloading a virus called BlackEnergy3.

It was the last substation, however, that was the most interesting, and the most frightening.

In that power station, which Ukrainian officials and cybersecurity researchers declined to name, hackers decided to test a much more complex method. They built a mirror image of the supervisory control and data acquisition system (SCADA), which is used to monitor and control equipment at facilities like power plants. Then, having created a perfect replica of the system being used at the station, they sent through commands that the system accepted as its own.

“Building their own SCADA environment is a complex and time-consuming endeavor,” Lee said. “We highlighted this, when we spoke to national level leaders, to say, ‘Look, this is a test. There is no operational reason to go through that much trouble, to conduct that level of espionage, to just do one substation this way.” The hackers, it appeared, were testing a type of cyberattack that signaled that they not only had the technical expertise to replicate an entire SCADA system, but had conducted the type of cyber espionage on Ukraine where they could piece together the detailed plans of a single power station. “From a cybersecurity perspective, from an industrial control system, that singular attack scared more people than all the other substations that went offline.”

One year later, the 2016 attack that targeted Kiev showed all the fingerprints of being a similar type of SCADA attack.

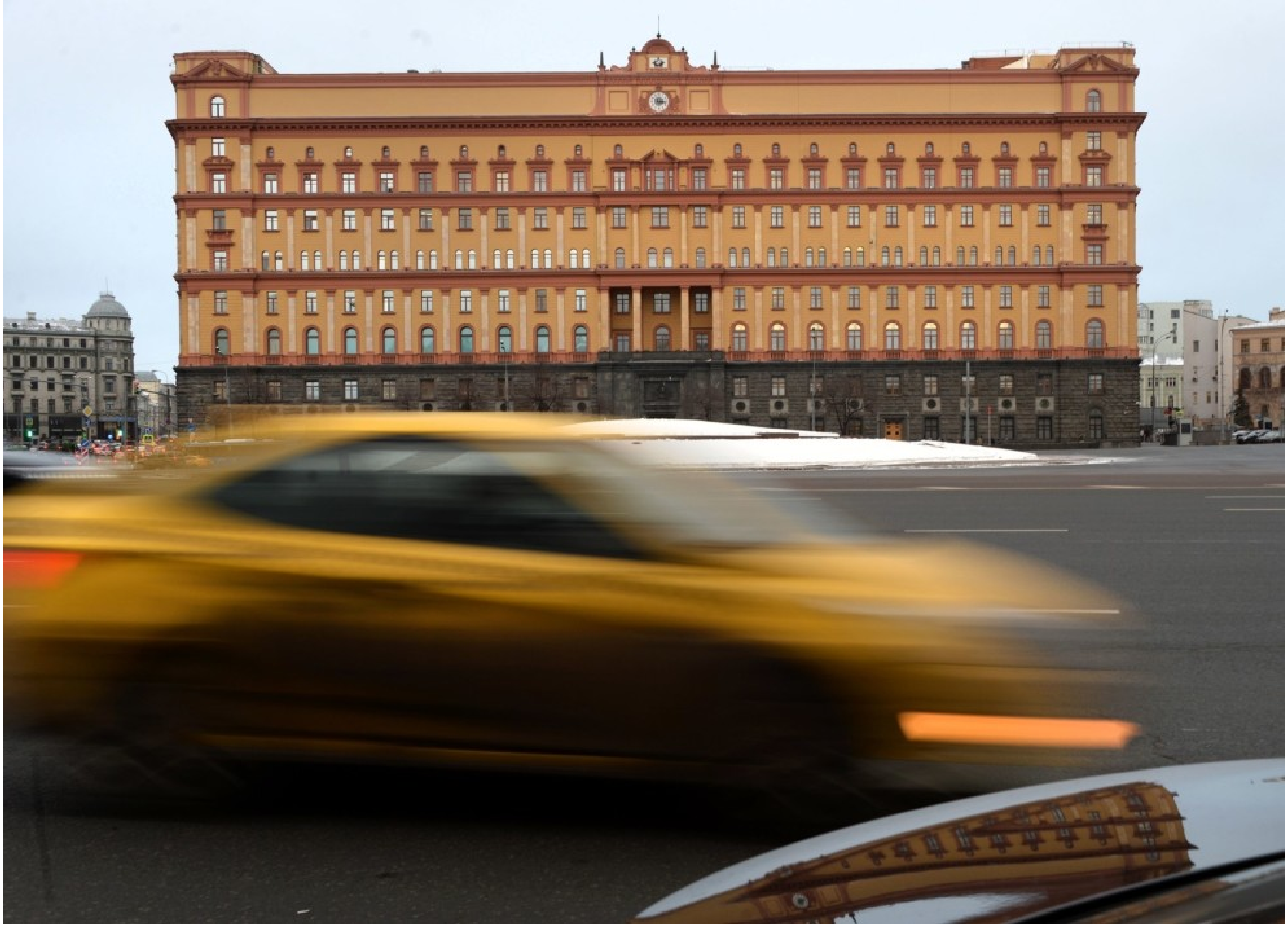
“This is definitely a higher level — it’s a transmission-level substation, not distribution-level substation,” Lee said. Attacks on transmission stations, he added, “are the kind of thing we worry about in the US.”

"A foreign state being able to take down your power grid — even for 10 minutes — that’s a game changer."

Ihor Huz, a member of the foreign affairs committee in Ukraine’s parliament, told BuzzFeed News there was no doubt that Russia was behind the most recent attack on the power grid. Russia has a long history of meddling in Ukraine, ranging from cutting off gas supplies to Ukraine to moving ground troops into the peninsula of Crimea. The attacks, Huz said, “will last as long as Russia will have the opportunity to support such interference.”

In the three months that have passed since the Kiev attack, cybersecurity experts have studied the methods that were used. Lee said there are few defenses against an opponent who dedicates that amount of time and effort to completely replicate a system. It represents the ideal type of attack for a country like Russia, as it requires very little overhead — other than the time involved in studying the target under attack and replicating it — and achieves maximum impact.

“The best you can do is get it back up quickly,” Lee said. “A power grid is one of the most complex systems ever designed. Attacking it absolutely helps hone your skills. ... The message that was sent by taking down power grids was definitely heard in DC and in the White House.”



Headquarters of the FSB in Moscow. *Vasily Maximov / AFP / Getty Images*

Earlier this year, a US cyber intelligence officer was taking part in a routine intelligence-sharing meeting with European lawmakers when things took an unusual turn and an assistant to one of the lawmakers pulled him outside into the hallway.

“She opened her phone to show me a spear-phishing email someone had recently sent her boss,” the US officer said, speaking on condition that neither he nor the lawmakers be named.

“He didn’t want to bring it up in the room — he was embarrassed. He had clicked on the damn thing and didn’t know what to do,” the officer said. “I felt so bad for the guy, but I just told [his assistant] it happens to everyone.”

The assistant then asked the officer to write down a series of protocols and worst-case scenarios to try and appease the panicked lawmaker.

“I just shook my head. I was like, ‘Worst case is you get to read your emails on WikiLeaks in a couple of months,’” he said, in reference to the thousands of emails of senior Democratic Party members. “Worst-case scenario is what happened here in the US.”

One of the first known targets of a Russia-led cyberattack was Estonia, which found its websites coming under a coordinated DDoS, or denial of service, attack in 2007. Toomas Hendrik Ilves, the former president of Estonia, has been documenting and researching Russia’s cyberwarfare tactics in the years since. This week he testified before the US Senate Judiciary Subcommittee on Crime and Terrorism to deliver a warning about the tools Russia uses to undermine democracies.

“The Russians are very aggressive everywhere, across Europe, and this is a problem that each country is struggling with on its own,” Ilves told BuzzFeed News.

Russia has spent over a decade investing in the cyber division of its military. An investigation last year by the independent Russian news site *Meduza* revealed a system in which Russia’s top political leadership was tasked with recruiting hackers and blackmailing criminals to do their bidding. Last month, Russia Defense Minister Sergey Shoigu told Russian lawmakers that Russia’s cyber army was waging a propaganda war and that “they are expected to be a far more effective tool than all we used before for counter-propaganda purposes.”

Within the next few months, France and Germany are holding national elections, while the Netherlands voted in the liberal party earlier this week. A number of Eastern European states will hold crucial votes later this year. All have publicly stated that they are concerned about Russian meddling in the vote.

“What happened in the US was a reality check for Europeans. We didn’t observe what was happening earlier, and then it was too late,” said Stefan Meister, a Russia-watcher at the German Council on Foreign Relations. While Eastern European states like Ukraine and Georgia long complained of Russian tampering, Western Europe assumed it was largely immune from the hacks, cyber espionage, and disinformation campaigns that have been attributed to Russia. “Germany and France, they were really latecomers to taking it seriously. It was only after what happened in the US that they realized their systems were vulnerable as well."

The interference follows certain patterns. The most common of these are disinformation campaigns, in which online figures and outlets, largely believed to be working on behalf of the Russian state, spread a story online with a political agenda. Last year, Germany saw the spread of a viral news story involving Lisa F, a 13-year-old girl reportedly from a Russian immigrant family who disappeared for 30 hours only to resurface with claims that she had been kidnapped and raped by "Arab" men. She later admitted her story was a lie, but that didn't stop a frenzied media campaign on pro-Russian websites that blamed German Chancellor Angela Merkel's open-door policy towards refugees for the brutal attacks on Lisa F.

"None of this is expensive or difficult," said Meister, who believes Russia's efforts to meddle in other countries — both through cyber and traditional warfare — started in earnest following the 2012 vote in Russia, when Putin won re-election. "Russia understood that to influence the information spear is equally as important as a classical conventional arms race… They combined different elements of their own cyberattacks with WikiLeaks, with foreign media — you take something and spread disinformation and use social networks to reach the broadest possible audience. It really uses the structure of our democratic societies, of our lives online, against us."

In the Balkan state of Montenegro, there are claims that Russia's meddling was far more brazen. Last November during parliamentary elections, Montenegro's incumbent candidate nearly lost to a pro-Russian coalition, amid accusations that Russia not only funneled money to the opposition candidates, but set up media outlets to try and promote those candidates. Even after the incumbent candidate, Prime Minister Milo Dukanovic, won the vote, top officials allege that Russia schemed to launch his overthrow, using the cover of anti-government protests to storm the prime minister's office, where fake police would be planted to arrest or kill him. The Montenegrin special prosecutor for organized crime confirmed that two Russian nationals are being sought as key organizers of the coup plot.

"Russia, it seems, is going through a system of trial and error right now. They are testing methods in Ukraine, in Georgia, in other countries," said Meister. "This costs very little for Russia. These cyberattacks are cheap to launch and very difficult to prove."

Meister added that Russia was simply adopting what others had done, but bending it to today's online world.

"This is the war of the 21st century. The US and countries in Europe do it now, but what Russia does is just more aggressive. They are using the instruments of cyber to attack much bigger and much richer countries… This makes sense," said Meister. "Many other countries will be learning from this."

Toomas Hendrik Ilves, the former president of Estonia. *Alex Wong / Getty Images*

Last month, cybersecurity researchers noticed something odd about malware they had detected trying to attack Polish financial institutions. Within the malware code were several Russian words, though they appeared to make little sense when read by native Russian speakers.

“In some cases, the inaccurate translations have transformed the meaning of the words entirely. This strongly implies that that authors of this attack are not native Russian speakers and, as such, the use of Russian words appears to be a ‘false flag,’” wrote cybersecurity researchers from the BAE Systems research firm. Rather than being deployed by Russian cybercriminals, BAE believed the malware had been used by a group known as Lazarus, prolific hackers linked to North Korea thought to be responsible for the 2014 attacks against Sony Pictures, as well as a $81 million cyber heist from Bangladesh’s Central Bank in 2016.

Attribution — the process by which cybersecurity researchers and governments try to determine which country or group of hackers is responsible for an attack — is becoming harder each year. False flags, in which hackers purposefully plant misleading clues, are just the tip of the iceberg. Cybersecurity researchers also say Russia is deploying a number of other tactics, such as inventing public figures who take responsibility for, and help disseminate information about, cyberattacks. When the emails of senior members of the Democratic Party were first made public, a figure appeared online calling himself Guccifer2.0, a clear allusion to a well-known Romanian hacker known as Guccifer. In email exchanges with journalists, Guccifer2.0 claimed to be a hacker-activist, and of Romanian origin — though those claims were largely proven false (and cybersecurity researchers say grammatical mistakes and syntax strongly point the finger at a Russian speaker running the account), his initial claims helped cast doubt over Russia's role in the hack.

Russia's use of cybercriminals, as seen through the DOJ indictment published this week, highlights the murky line between hackers working on behalf of the Russian state and cybercriminals seeking financial gain. According to the DOJ, two Russian FSB agents recruited two well-known hackers to help them breach Yahoo and access more than 500 million email accounts. For legal experts and government officials seeking to attribute cyberattacks to a nation-state, the use of cybercriminals poses an added complication.

"Russia has laid out the playbook."

It's becoming easier and easier to mask an identity online, cybersecurity experts say, while the code used in malware, once it hits the open market, can be bought and repurposed by hackers and nation-states across the world.

Take the Stuxnet virus, which the US developed to target and damage Iran's nuclear weapons program and which is largely believed to one of the most sophisticated cyberattacks ever launched. Parts of the code that makes up Stuxnet has resurfaced in cyberattacks ranging from Asia to Latin America. And, perhaps making lemonade out of lemons, Iran is believed to have repurposed parts of the Stuxnet virus to create "Shamoon," a virus used in 2012 to infect and damage 30,000 computers of the Saudi-American oil company ARAMCO.

"When these tools get out it proliferates among those who want to attack. They will be taken and modified and used by others who want to attack," said Eric O'Neill, a former counterintelligence officer for the FBI who now works for the cybersecurity firm Carbon Black. He spoke to BuzzFeed News last week in the wake of WikiLeaks publishing a new cache of 8,761 documents that detail the malware and exploits the CIA uses to hack into devices ranging from phones and laptops to smart TVs.

Those documents show that even the CIA is in the habit of repurposing code. One series of documents details a CIA group called UMBRAGE, which recycles snippets of code developed by other groups, in what appears to be an effort to save themselves time.

"Everyone borrows from everyone. What is different about Russia is that they use it more aggressively. They set the example for how to do these things with a small budget, and how to make a big impact," said Meister, who noted that a number of small countries in Latin America, Africa, and Asia could easily model their behavior on how Russia has conducted its cyberwarfare operations.

Ilves, the former Estonian president, agreed. Russia, he said, is "very aggressive everywhere."

“What they do is asymmetric — what they do to us we cannot do them. This applies to all authoritarian regimes. Liberal democracies with a free press and free and fair elections are at an asymmetric disadvantage because they can be interfered with — the tools of their democratic and free speech can be used against them,” said Ilves.

The hack on the DNC, which US intelligence agencies have widely attributed to Russia, could be replicated by dozens of countries around the world, according to Robert Knake, a former director of cybersecurity policy in the Obama administration.

“Russia has laid out the playbook. What Russia did was relatively unsophisticated and something that probably about 60 countries around the world have the capability of doing — which is to target third parties, to steal documents and emails, and to selectively release them to create unfavorable conditions for that party,” Knake told the BBC’s *Today*. “It’s unsubtle interference. And it’s a violation of national sovereignty and customary law.”

Meister said that in cyberwarfare, the advantage could often go to smaller countries, especially those that do not have open, democratic media systems.

“In an authoritarian state which is closed off, it is hard to have much of an effect. But if you are that authoritarian state, you can use instruments of cyber to attack bigger societies who value their online debate and speech,” said Meister.

Russia, he added, is teaching the world that while its conventional military has its limits, it can induce panic and fear using cyberwarfare.

“They have scared us, and that is what they wanted to show. Now, every attack, someone says immediately, ‘This is Russia,’” said Meister. “That is a form of winning too.”

Other perspectives on this story

1 A lot of people feel as though this is a war and one we're losing.

2 Chess grandmaster and chairman of the Human Rights Foundation Garry Kasparov emphasizes the difficulty of deterrin cyber attacks.

3 Many people think it's time to get used to cyberwarfare and attempted electoral interference.

4 Some people worry that America is losing too much ground to Russia in cyber tactics.

5 A Twitter user thinks America's hackers are too busy having fun online to help adequately defend the U.S. from cyber at

6 Some people dismiss concerns about Russian cyberwarfare as Cold War-era paranoia.

Outside Your Bubble is a BuzzFeed News effort to bring you a diversity of thought and opinion from around the internet. If you don't see your viewpoint represented, contact the curator at bubble@buzzfeed.com. Click here for more on Outside Your Bubble.

Sheera Frenkel is a cybersecurity correspondent for BuzzFeed News based in San Francisco. She has reported from Israel, Egypt, Jordan and across the Middle East. Her secure PGP fingerprint is 4A53 A35C 06BE 5339 E9B6 D54E 73A6 0F6A E252 A50F
Contact Sheera Frenkel at Sheera.Frenkel@buzzfeed.com.

Got a confidential tip? Submit it here.

More ▾

NEXT ON NEWS›

9 Gross Firsts That Happen In Every Relationship

Tagged:russia, cyber attacks, cyberwar, cyberwarfare, fsb, hacking, russia hack, ukraine

Tell Us What You Know.

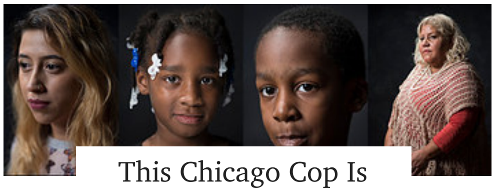
Submit A News Tip ›

BuzzFeed NEWS

In The News Today

- Jared Kushner secretly met with Muslim leaders before Trump took office, but relations between activists and the administration quickly turned toxic.
- The Trump White House blamed a suspected chemical attack in Syria on President Obama, saying it was a "result of the past administration's weakness."
- A former campaign adviser for Donald Trump met with and passed documents to a Russian spy in New York City in 2013.

- The NCAA will again hold college championship games in North Carolina now that the anti-LGBT bathroom law has been partially repealed.



This Chicago Cop Is Accused Of Framing At Least 51 People For Murder

by Melissa Segura

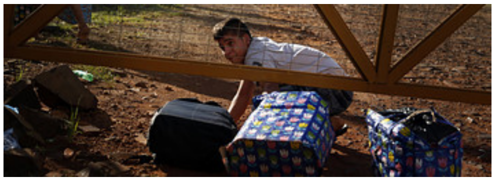
More News

Trump's Critics Are Letting The Bigger Russia Story Slide

A Murder In Berkeley Gave The Far-Right Its Perfect Perp

The Man Who Taught Donald Trump To Pit Gay People Against Immigrants

The Softening Of Kellyanne Conway



A Wall Divides Latin America — But Not The One You're Thinking Of

The Far Right's Most Common Memes Explained For Normal People

This Student's Secret Abortion Shows Why Thousands Of Irish Women Will Strike Next Week

Nashville's Last Taboo? Country Music Stars Are Tiptoeing Around Trump

Here's What Parental Leave Is Really Like Around The World

Egypt’s Feared Spy Agency Has Hired Some DC Lobbyists To Clean Up Its Image

Now Buzzing

Here’s How The White House Is Legitimizing The Pro-Trump Media

17 Nurses Reveal The Worst Things People Got Stuck Up Their Penises, Vaginas, And Butts

The Trump Administration Lay The Blame For Suspected Syria Gas Attack At Obama’s Feet

People Are Demanding McDonald’s Bring Back Szechuan Sauce Thanks To “Rick And Morty”

Zac Efron Riding Camels Shirtless In The Desert Is A Once-In-A-Lifetime Thirst Moment

Fans Of "13 Reasons Why" Are Shipping These Two Actors And I'm Here For It

More Buzz ›

Advertise Jobs Mobile Newsletter Shop US Edition

About Press RSS Privacy User Terms Ad Choices Help Contact