היערכות לעימות באירופה – רוסיה / אוקראינה / נאט"ו / ארה"ב וההשלכות של העימות במרחב הסייבר – עדכון מוצ"ש 12.2

מסמך זה נכתב לאור ההנחה שקיימת אפשרות שבימים הקרובים יתרחש עימות שבו תתקוף רוסיה את אוקראינה. ההערכה שלנו, לאור ניתוח תקיפות רוסיות קודמות היא שהתקיפה תלווה במתקפת סייבר רחבה. הרוסים למדו בכל הנראה מהשגיאות שלהם מעימותים קודמים (אסטוניה, גאורגיה, אוקראינה סבב א', ב', ארה"ב ואזורים אחרים שהם פעלו בהם) ולהערכתנו הם הבינו סט שלם של פעולות משולבות סייבר ותקיפה פיזית שאמורות לפגוע קשה ביכולת של האוקראינים להתמודד מולם **ולהביא להכרעה מהירה של המערכה**. הפעילות הרוסית עלולה לכלול בין השאר את הרכיבים הבאים :

1. **תקיפת מערכות הממשל והצבא האוקראיני** במספר וקטורים:
   a. הפצת נוזקות הרס במערכות המחשב של הממשל
   b. תקיפות מניעת שירות – DDOS
   c. פגיעה והשתלטות על אתרי האינטרנט של הממשלה,
   d. פגיעה במערכות הבספיות והלוגיסטיות של הממשלה והצבא
   e. פגיעה במחשבים ובמכשירי הסלולר של האישים המרכזיים בממשלה ובצבא
   f. השתלטות על חשבונות הממשלה ברשתות החברתיות או לפחות מניעת גישה אליהם על ידי שיבוש מערכות התקשורת במדינה.
2. **תקיפת ספקי התקשורת, הסלולר והאינטרנט של אוקראינה** כולל ניסיון לשבש את כלל מערכי התקשורת של המדינה תקיפה כזו תכלול כמעט בוודאות רכיב פיזי של פגיעה באתרי תקשורת, מרכזי מחשבים וסלולר במדינה) כולל אפשרות לניתוק פיזי של כבלים תת מימיים וכבלי תקשורת למדינה, שיבוש תקשורת לווינים
3. **תקיפת מערכות האנרגיה במדינה (תחנות חשמל ומערכות גיבוי חשמלי)** גם בתקיפה זו יופעלו נוזקות הרס יחד עם תקיפה פיזית של תחנות כח ומערכות הולכה. התקיפה הזו תשבש את אספקה החשמל של המדינה
4. **הפעלת מערך תעמולה /פייק ניוז** שמטרותיו הישירות הן :
   a. להסתיר ולמנוע דיווחים על המתרחש במדינה
   b. הסתרת הפעילות של הצבא הרוסי ויצירת ערפל קרב
   c. הפללת האוקראינים והמערב בפעולה
   d. יצירת דעת קהל עוינת לממשלת אוקראינה
   e. פנייה ישירה לאזרחים בקריאה לסוג של מרד אזרחי ויצירת הפרדה בינם לבין הממשל בעקבות העימות

תגובה אפשרית של האמריקאים לפעילות הרוסית, במרחב הסייבר:

1. סיוע שוטף של הצבא וזרועות המודיעין האמריקאיות לאוקראינים בחשיפת וסיכול הפעילות הרוסית בסייבר
2. רתימת חברות הטכנולוגיה האמריקאיות ובראשן מיקרוסופט לסייע לאוקראינים
3. חשיפת הנוזקות ומתווה הפעולה הרוסי בהתראות שיוצאו על ידי CISA וה FBI
4. ביצוע פעילות התקפית בסייבר מול הפעילות הרוסית לא רק במרחב האוקראיני
5. חסימת מערכות בספיות קריטיות לרוסים (Swift)
6. יצירת קמפיין תקשורתי נגדי מול הרוסים
7. שיבוש מערכות תקשורת צבאית רוסית

השלכות אפשריות על ישראל

1. פגיעה בכבלי תקשורת של ישראל או בתשדורת הלוויינים בעקבות פגיעה בכבלי התקשורת באירופה – שיבוש הפעולה של חברות וארגונים בישראל מול לקוחות/ספקים בעולם
2. פגיעה במערכי מיקור החוץ של חברות ישראליות וסטרטאפים באוקראינה – פגיעה בפיתוח של יישומים או בתיקון תקלות תוכנה של חברות הנסמכות על פיתוח יישומים
3. זליגת תקיפות המיועדות לתקיפות באוקראינה / חברות באירופה ובארה"ב לישראל ופגיעה במערכי המחשוב של חברות בישראל
4. פגיעה כספית בחברות הטכנולוגיה בישראל – עליית מחירי דלק, ירידות חדות בשוק המניות העולמי, הקפאת רכישות של תוכנה מאירופה ומאזורים אחרים בעולם

נספח - תקיפות סייבר רוסיות קודמות

התקיפה הרוסית ב 2007 מול אסטוניה - ויקיפדיה

The **2007 cyberattacks on Estonia** (Estonian: *2007. aasta küberrünnakud Eesti vastu*) were a series of cyberattacks which began on 27 April 2007 and targeted websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters, amid the country's disagreement with Russia about the relocation of the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn.[1][2] Most of the attacks that had any influence on the general public were distributed denial of service type attacks ranging from single individuals using various methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements including that of the Estonian Reform Party website also occurred.[3] Research has also shown that large conflicts took place to edit the English-language version of the Bronze Soldier's Wikipedia page.[4]

Some observers reckoned that the onslaught on Estonia was of a sophistication not seen before. The case is studied intensively by many countries and military planners as, at the time it occurred, it may have been the second-largest instance of state-sponsored cyberwarfare, following Titan Rain.[5]

As of January 2008, one ethnic-Russian Estonian national has been charged and convicted.[6]

During a panel discussion on cyber warfare, Sergei Markov of the Russian State Duma has stated his unnamed aide was responsible in orchestrating the cyber attacks. Markov alleged the aide acted on his own while residing in an unrecognised republic of the former Soviet Union, possibly Transnistria.[7] On 10 March 2009 Konstantin Goloskokov, a "commissar" of the Kremlin-backed youth group Nashi, has claimed responsibility for the attack.[8] Experts are critical of these varying claims of responsibility.[9] The direct result of the cyberattacks was the creation of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.

הפעילות הרוסית ב 2008 מול גאורגיה - ויקיפדיה

On 20 July 2008, weeks before the Russian invasion of Georgia, "zombie" computers were already on the attack against Georgia.[2][3] The website of the Georgian president Mikheil Saakashvili was targeted, resulting in overloading the site. The traffic directed at the website included the phrase "win+love+in+Rusia". The site then was taken down for 24 hours.[4][5]

On 5 August 2008, the websites for OSInform News Agency and OSRadio were hacked. The OSinform website at osinform.ru kept its header and logo, but its content was replaced by the content of Alania TV website. Alania TV, a Georgian government supported television station aimed at audiences in South Ossetia, denied any involvement in the hacking of the rival news agency website. Dmitry Medoyev, the South Ossetian envoy to Moscow, claimed that Georgia was attempting to cover up the deaths of 29 Georgian servicemen during the flare-up on August 1 and 2.[6]

On 5 August, Baku–Tbilisi–Ceyhan pipeline was subject to a terrorist attack near Refahiye in Turkey, responsibility for which was originally taken by Kurdistan Workers' Party (PKK) but there is circumstantial evidence that it was instead a sophisticated computer attack on line's control and safety systems that led to increased pressure and explosion.[7]

According to Jart Armin, a researcher, many Georgian Internet servers were under external control since late 7 August 2008.[8] On 8 August, the DDoS attacks peaked and the defacements began.[9]

On 9 August 2008, key sections of Georgia's Internet traffic reportedly had been rerouted through servers based in Russia and Turkey, where the traffic was either blocked or diverted. The Russian and Turkish servers were allegedly controlled by the Russian hackers. Later on the same day, the network administrators in Germany were able to temporarily reroute some Georgian Internet traffic directly to servers run by Deutsche Telekom AG. However, within hours the traffic was again diverted to Moscow-based servers.[8][10]

On 10 August 2008, RIA Novosti news agency's website was disabled for several hours by a series of attacks. Maxim Kuznetsov, head of the agency's IT department said: "The DNS-servers and the site itself have been coming under severe attack."[11]

On 10 August, Jart Armin warned that Georgian sites that were online might have been fake. "Use caution with any Web sites that appear of a Georgia official source but are without any recent news [such as those dated Saturday, Aug. 9, or Sunday, Aug. 10], as these may be fraudulent," he said.[8][10]

By 11 August 2008, the website of the Georgian president had been defaced and images comparing President Saakashvili to Adolf Hitler were posted. This was an example of cyber warfare combined with PSYOPs.[9] Georgian Parliament's site was also targeted.[9][8][12] Some Georgian commercial websites were also attacked.[10][8][12] On 11 August, Georgia accused Russia of waging cyber warfare on Georgian government websites simultaneously with a military offensive. The Foreign Ministry of Georgia said in a statement, "A cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including that of the Foreign Affairs Ministry." A Kremlin spokesman denied the accusation and said, "On the contrary, a number of internet sites belonging to the Russian media and official organizations have fallen victim to concerted hacker attacks."[13] The Ministry of Foreign Affairs set up a blog on Google's Blogger service as a temporary site. The Georgian President's site was moved to US servers.[9][12] The National Bank of Georgia's Web site had been defaced at one point and 20th-century dictators' images and an image of Georgian president Saakashvili were placed.[2] The Georgian Parliament website was defaced by the "South Ossetia Hack Crew" and the content was replaced with images comparing President Saakashvili to Hitler.[12]

Estonia offered hosting for Georgian governmental website and cyberdefense advisors.[14][3] However a spokesman from Estonia's Development Centre of State Information Systems said Georgia didn't request help. "This will be decided by the government," he said.[10] It was reported that the Russians bombed Georgia's telecommunications infrastructure, including cell towers.[14] Private United States companies also assisted the Georgian government to protect its non-war making information such as the government payroll during the conflict.[15]

Russian hackers also attacked the servers of the Azerbaijani Day.Az news agency. The reason was Day.Az position in covering the Russian-Georgian conflict.[16] ANS.az, one of the leading news websites in Azerbaijan, was also attacked.[17] Russian intelligence services had also disabled the information websites of Georgia during the war.[16] The Georgian news site Civil Georgia switched their operations to one of Google's Blogspot domains.[14] Despite the cyber-attacks, Georgian journalists managed to report on the war. Many media professionals and citizen journalists set up blogs to report or comment on the war.[18][19]

Barack Obama, the U.S. presidential candidate demanded Russia halt the internet attacks as well as complying with a ceasefire on the ground.[10] The President of Poland, Lech Kaczyński, said that Russia was blocking Georgian "internet portals" to supplement its military aggression. He offered his own website to Georgia to aid in the "dissemination of information".[12] Reporters Without Borders condemned the violations of online freedom of information since the outbreak of hostilities between Georgia and Russia. "The Internet has become a battleground in which information is the first victim," it said.[17]

The attacks involved Denial-of-service attacks.[2][12][17] The New York Times reported on 12 August that according to some experts, it was the first time in history a known cyberattack had coincided with a shooting war. On 12 August, the attacks continued, controlled by programs that were located in hosting centers controlled by a Russian telecommunications companies. A Russian-language site, stopgeorgia.ru, continued to operate and offer software for Denial-of-service attacks.[2]

On 14 August 2008, it was reported that although a ceasefire reached, major Georgian servers were still down, hindering communication in Georgia.[19]

תקיפת תחנות חשמל באוקראינה – 2015

The Ukraine power grid hack was a cyberattack on Ukraine's power grid on December 23, 2015, resulting in power outages for roughly 230,000 consumers in Ukraine for 1-6 hours. The attack took place during an ongoing Russian military intervention in Ukraine (2014–present) and is attributed to a Russian advanced persistent threat group known as "Sandworm".[1] It is the first publicly acknowledged successful cyberattack on a power grid.[2]

Description

On 23 December 2015, hackers remotely compromised information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to consumers. Most affected were consumers of "Prykarpattyaoblenergo" (Ukrainian: Прикарпаттяобленерго; servicing Ivano-Frankivsk Oblast): 30 substations (7 110kv substations and 23 35kv substations) were switched off, and about 230,000 people were without electricity for a period from 1 to 6 hours.[3]

At the same time, consumers of two other energy distribution companies, "Chernivtsioblenergo" (Ukrainian: Чернівціобленерго; servicing Chernivtsi Oblast) and "Kyivoblenergo" (Ukrainian: Київобленерго; servicing Kyiv Oblast) were also affected by a cyberattack, but at a smaller scale. According to representatives of one of the companies, attacks were conducted from computers with IP addresses allocated to the Russian Federation.[4]

Vulnerabillity[edit]

In 2019, it was argued that Ukraine was a special case, comprising unusually dilapidated infrastructure, a high level of corruption, the ongoing Russo-Ukrainian War, and exceptional possibilities for Russian infiltration due to the historical links between the two countries.[5] The Ukrainian power grid was built when it was part of the Soviet Union, has been upgraded with Russian parts and (as of 2022), still not been fixed. Russian attackers are as familiar with the software as operators. Furthermore, the timing of the attack during the holiday season guaranteed only a skeleton crew of Ukrainian operators were working (as shown in videos). [6]

Method

The cyberattack was complex and consisted of the following steps:[4]

- prior compromise of corporate networks using spear-phishing emails with BlackEnergy malware
- seizing SCADA under control, remotely switching substations off

- disabling/destroying IT infrastructure components (uninterruptible power supplies, modems, RTUs, commutators)
- destruction of files stored on servers and workstations with the KillDisk malware
- denial-of-service attack on call-center to deny consumers up-to-date information on the blackout.

At last the emergency power at the utility company's operations center was switched off.[6] In total, up to 73 MWh of electricity was not supplied (or 0.015% of daily electricity consumption in Ukraine).[4]

Russian election interference in Ukraine - 2014

The May 2014 Ukrainian presidential election was disrupted by cyberattacks over several days, including the release of hacked emails, attempted alteration of vote tallies, and distributed denial-of-service attacks to delay the final result. They were found to have been launched by pro-Russian hackers.[10][11] Malware that would have displayed a graphic declaring far-right candidate Dmytro Yarosh the electoral winner was removed from Ukraine's Central Election Commission less than an hour before polls closed. Despite this, Channel One Russia falsely reported that Yarosh had won, fabricating a fake graphic from the election commission's website.[10][12] Political scientist Peter Ordeshook said in 2017, "These faked results were geared for a specific audience in order to feed the Russian narrative that has claimed from the start that ultra-nationalists and Nazis were behind the revolution in Ukraine."[10] The same Sofacy malware used in the Central Election Commission hack was later found on the servers of the Democratic National Committee (DNC).[12] Around the same time as Russia's attempt to hack the 2014 elections, the Obama administration received a report suggesting that the Kremlin was building a disinformation program which could be used to interfere in Western politics.[11]

Social media and Internet trolls

Further information: Internet Research Agency

According to the special counsel investigation's Mueller Report (officially named "Report on the Investigation into Russian Interference in the 2016 Presidential Election"),[40] the first method of Russian interference used the Internet Research Agency (IRA), a Kremlin-linked troll farm, to wage "a social media campaign that favored presidential candidate Donald J. Trump and disparaged presidential candidate Hillary Clinton".[41] The Internet Research Agency also sought to "provoke and amplify political and social discord in the United States".[42]

By February 2016, internal IRA documents showed an order to support the candidacies of Donald Trump and Bernie Sanders, while IRA members were to "use any opportunity to criticize" Hillary Clinton and the rest of the candidates.[43] From June 2016, the IRA organized election rallies in the U.S. "often promoting" Trump's campaign while "opposing" Clinton's campaign.[44] The IRA posed as Americans, hiding their Russian background, while asking Trump campaign members for campaign buttons, flyers, and posters for the rallies.[45]

Initially in 2016 Facebook CEO Mark Zuckerberg said, "I think the idea that fake news on Facebook influenced the election in any way, I think is a pretty crazy idea."[46]

Russian use of social media to disseminate propaganda content was very broad. Facebook and Twitter were used, but also Reddit, Tumblr, Pinterest, Medium, YouTube, Vine, and Google+ (among other sites). Instagram was by far the most used platform, and one that largely remained out of the public eye until late 2018.[47][48] The Mueller report lists IRA-created groups on Facebook including "purported conservative groups" (e.g. 'Tea Party News'), "purported Black social justice groups" (e.g. 'Blacktivist') "LGBTQ groups" ('LGBT United'), and "religious groups" ('United Muslims of America').[45] The IRA Twitter accounts included @TEN_GOP (claiming to be related to the Tennessee Republican Party), @jenn_abrams and @Pamela_Moore13; both claimed to be Trump supporters and both had 70,000 followers.[49]

Several Trump campaign members (Donald J. Trump Jr., Eric Trump, Kellyanne Conway, Brad Parscale and Michael T. Flynn) linked or reposted material from the IRA's @TEN_GOP Twitter account listed above. Other people who responded to IRA social media accounts include Michael McFaul, Sean Hannity, Roger Stone and Michael Flynn Jr.[50]

Advertisements bought by Russian operatives for the Facebook social media site are estimated to have reached 10 million users. But many more Facebook users were contacted by accounts created by Russian actors. 470 Facebook accounts are known to have been created by Russians during the 2016 campaign. Of those accounts six generated content that was shared at least 340 million times, according to research done by Jonathan Albright, research director for Columbia University's Tow Center for Digital Journalism.[51] The most strident Internet promoters of Trump were paid Russian propagandists/trolls, who were estimated by *The Guardian* to number several thousand.[52] (By 2017 the U.S. news media was focusing on the Russian operations on Facebook and Twitter and Russian operatives moved on to Instagram.)[48] The Mueller Report found the IRA spent $100,000 for more than 3,500 Facebook advertisements from June 2015 to May 2017,[53] which included anti-Clinton and pro-Trump advertisements.[45] In comparison, Clinton and Trump campaigns spent $81 million on Facebook ads.[54][55]

Fabricated articles and disinformation[56] were spread from Russian government-controlled outlets, RT and Sputnik to be popularized on pro-Russian accounts on Twitter and other social media.[56] Researchers have compared Russian tactics during the 2016 U.S. election to the "active measures" of the Soviet Union during the Cold War,[56] but made easier by the use of social media.[56][57]

Monitoring 7,000 pro-Trump social media accounts over a 2+½-year period, researchers J. M. Berger, Andrew Weisburd and Clint Watts[58] found the accounts denigrated critics of Russian activities in Syria and propagated falsehoods about Clinton's health.[59] Watts found Russian propaganda to be aimed at fomenting "dissent or conspiracies against the U.S. government and its institutions",[60] and by autumn of

2016 amplifying attacks on Clinton and support for Trump, via social media, Internet trolls, botnets, and websites.[56]

Former site of the Internet Research Agency in Saint Petersburg, Russia

Wikisource has original text related to this article:
Internet Research Agency Indictment

Monitoring news on Twitter directed at one state (Michigan) prior to the election, Philip N. Howard found about half of it fabricated or untrue; the other half came from real news sources.[61] In continued analysis after the election, Howard and other researchers found the most prominent methods of misinformation were ostensibly "organic posting, not advertisements", and influence operation activity increased after the 2016 and was not limited to the election.[62]

Facebook originally denied that fake news on their platform had influenced the election and had insisted it was unaware of any Russian-financed advertisements but later admitted that about 126 million Americans may have seen posts published by Russia-based operatives.[63][64][65] Criticized for failing to stop fake news from spreading on its platform during the 2016 election,[66] Facebook originally thought that the fake-news problem could be solved by engineering, but in May 2017 it announced plans to hire 3,000 content reviewers.[67][*failed verification*]

According to an analysis by Buzzfeed, the "20 top-performing false election stories from hoax sites and hyperpartisan blogs generated 8,711,000 shares, reactions, and comments on Facebook."[68] In September 2017, Facebook told congressional investigators it had discovered that hundreds of fake accounts linked to a Russian troll farm had bought $100,000 in advertisements targeting the 2016 U.S. election audience.[64] The ads, which ran between June 2015 and May 2017, primarily focused on divisive social issues; roughly 25% were geographically targeted.[69][70] Facebook has also turned over information about the Russian-related ad buys to Special Counsel Robert Mueller.[71] Approximately 3,000 adverts were involved, and these were viewed by between four and five million Facebook users prior to the election.[72] On November 1, 2017, the House Intelligence Committee released a sample of Facebook ads and pages that had been financially linked to the Internet Research Agency.[73] A 2019 analysis by *The Washington Post*'s "Outlook" reviewed a number of troll accounts active in 2016 and 2018, and found that many resembled organic users. Rather than wholly negative and obvious, many confirmed troll accounts deployed humor and were "astute in exploiting questions of culture and identity and are frequently among the first to push new divisive conversations" even "picked up by mainstream print media."[74]

Cyberattack on Democrats

Hillary Clinton at the 2016 Democratic National Convention

According to the Mueller Report, the second method of Russian interference saw the Russian intelligence service, the GRU, hacking into email accounts owned by volunteers and employees of the Clinton presidential campaign, including that of campaign chairman John Podesta, and also hacking into "the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC)". As a result, the GRU obtained hundreds of thousands of hacked documents, and the GRU proceeded by arranging releases of damaging hacked material via the WikiLeaks organization and also GRU's personas "DCLeaks" and "Guccifer 2.0".[75][76][77]

Starting in March 2016, the Russian military intelligence agency GRU sent "spearphishing" emails targeted more than 300 individuals affiliated with the Democratic Party or the Clinton campaign, according to the Special Counsel's July 13, 2018 Indictment. Using malware to explore the computer networks of the DNC and DCCC,[78] they harvested tens of thousands of emails and attachments and deleted computer logs and files to obscure evidence of their activities.[79] These were saved and released in stages to the public during the three months before the 2016 election.[80] Some were released strategically to distract the public from media events that were either beneficial to the Clinton campaign or harmful to Trump's.

The first tranche of 19,000 emails and 8,000 attachments was released on July 22, 2016, three days before the Democratic convention. The resulting news coverage created the impression that the Democratic National Committee was biased against Clinton's Democratic primary challenger Bernie Sanders (who received 43% of votes cast in the Democratic presidential primaries) and forced DNC Chairwoman Debbie Wasserman Schultz to resign, disrupting the plans of the Clinton campaign.[68][81] A second tranche was released on October 7, a few hours after the Obama Administration released a statement by the Department of Homeland Security and the director of National Intelligence accusing the Russian government of interfering in the election through hacking, and just 29 minutes after *The Washington Post* reported on the Access Hollywood videotape where Trump boasted about grabbing women "by the pussy". The stolen documents effectively distracted media and voter attention from both stories.[68][80][82]

Stolen emails and documents were given both to platforms created by hackers—a website called DCLeaks and a persona called Guccifer 2.0 claiming to be a lone hacker—and to an unidentified organization believed to be WikiLeaks.[81] (The Russians registered the domain dcleaks.com,[83] using principally Bitcoin to pay for the domain and the hosting.)[83]

Podesta hack

Main article: Podesta emails

John Podesta, Chairman of Hillary Clinton's presidential campaign, received a phishing email on March 19, 2016, sent by Russian operatives purporting to alert him of a "compromise in the system", and urging him to change his password "immediately" by clicking on a link.[84] This allowed Russian hackers to access around 60,000 emails from Podesta's private account.[85]

John Podesta, later told *Meet the Press* that the FBI spoke to him only once regarding his hacked emails and that he had not been sure what had been taken until a month before the election on October 7 "when [WikiLeaks' Julian] Assange ... started dumping them out and said they would all dump out, that's when I knew that they had the contents of my email account."[86]

The WikiLeaks October 7 dump started less than an hour after *The Washington Post* released the Donald Trump and Billy Bush recording *Access Hollywood* tape, WikiLeaks announced on Twitter that it was in possession of 50,000 of Podesta's emails, and a few hours after the Obama Administration released a statement by the Department of Homeland Security and the director of National Intelligence stating "The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations."[87]

It initially released 2,050 of these.[88] The cache included emails containing transcripts of Clinton's paid speeches to Wall Street banks, controversial comments from staffers about Catholic voters, infighting among employees of the Clinton campaign, as well as potential Vice-Presidential picks for Clinton.[89][90] The Clinton campaign did not confirm or deny the authenticity of the emails but emphasized they were stolen and distributed by parties hostile to Clinton and that "top national security officials" had stated "that documents can be faked as part of a sophisticated Russian misinformation campaign."[91]

Podesta's e-mails, once released by WikiLeaks, formed the basis for Pizzagate, a debunked conspiracy theory that falsely posited that Podesta and other Democratic Party officials were involved in a child trafficking ring based out of pizzerias in Washington, D.C.[92][93]

DNC hack

Main articles: Democratic National Committee cyber attacks and 2016 Democratic National Committee email leak

Debbie Wasserman Schultz resigned her position as chairperson of the DNC.[94]

The United States Intelligence Community concluded by January 2017 that the GRU (using the names Cozy Bear and Fancy Bear) had gained access to the computer network of the Democratic National Committee (DNC)—the formal governing body of the Democratic Party—in July 2015 and maintained it until at least June 2016,[95][96] when they began leaking the stolen information via the Guccifer 2.0 online persona, DCLeaks.com and Wikileaks.[97] Debbie Wasserman Schultz resigned as DNC chairwoman following

the release of e-mails by WikiLeaks that showed DNC officials discussing Bernie Sanders and his presidential campaign in a derisive and derogatory manner.[98] Emails leaked included personal information about Democratic Party donors, with credit card and Social Security numbers,[99][100] emails by Wasserman Schultz calling a Sanders campaign official a "damn liar".[101]

Following the July 22 publication of a large number of hacked emails by WikiLeaks, the FBI announced that it would investigate the theft of DNC emails.[102][103]

Intelligence analysis of attack

In June and July 2016, cybersecurity experts and firms, including CrowdStrike,[104] Fidelis, FireEye,[105] Mandiant, SecureWorks,[106] Symantec[105] and ThreatConnect, stated the DNC email leaks were part of a series of cyberattacks on the DNC committed by two Russian intelligence groups, called Fancy Bear and Cozy Bear,[107][108] also known respectively as APT28 and APT29 / The Dukes.[109][110][104][111] ThreatConnect also noted possible links between the DC Leaks project and Russian intelligence operations because of a similarity with Fancy Bear attack patterns.[112] SecureWorks added that the actor group was operating from Russia on behalf of the Russian government.[113][114] *de Volkskrant* later reported that Dutch intelligence agency AIVD had penetrated the Russian hacking group Cozy Bear in 2014, and observed them in 2015 hack the State Department in real time, while capturing pictures of the hackers via a security camera in their workspace.[115][116] American, British, and Dutch intelligence services had also observed stolen DNC emails on Russian military intelligence networks.[117]

Intelligence reaction and indictment

On October 7, 2016, Secretary Johnson and Director Clapper issued a joint statement that the intelligence community is confident the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations, and that the disclosures of hacked e-mails on sites like DCLeaks.com and WikiLeaks are consistent with the Russian-directed efforts.[118]

In the July 2018 indictment by the Justice Department of twelve Russian GRU intelligence officials posing as "a Guccifer 2.0 persona" for conspiring to interfere in the 2016 elections[119][120] was for hacking into computers of the Clinton campaign, the Democratic National Committee, state election boards, and secretaries of several states. The indictment describes "a sprawling and sustained cyberattack on at least three hundred people connected to the Democratic Party and the Clinton campaign". The leaked stolen files were released "in stages," a tactic wreaking "havoc on the Democratic Party throughout much of the election season."[120][80]

One collection of data that hackers obtained and that may have become a "devastating weapon" against the Clinton campaign was the campaign's data analytics and voter-turnout models,[121] extremely useful in targeting messages to "key constituencies" that Clinton needed to mobilize.[80] These voters were later bombarded by Russian operatives with negative information about Clinton on social media.[80]

WikiLeaks

WikiLeaks founder Julian Assange

In April 2017, CIA Director Mike Pompeo said WikiLeaks was a hostile intelligence agency aided by foreign states including Russia, and that the U.S. Intelligence Community concluded that Russia's "propaganda outlet," RT, had conspired with WikiLeaks.[122]

WikiLeaks[123] and its founder Julian Assange[124][125] have made a number of statements denying that the Russian government was the source of the material. However, an anonymous CIA official said that Russian officials transferred the hacked e-mails to WikiLeaks using "a circuitous route" from Russia's military intelligence services (GRU) to WikiLeaks via third parties.[126]

In a leaked private message on Twitter, Assange wrote that in the 2016 election "it would be much better for GOP to win," and that Hillary Clinton was a "sadistic sociopath".[127][128]

Hacking of Congressional candidates

Hillary Clinton was not the only Democrat attacked. Caches of Democratic Congressional Campaign Committee documents stolen by "Guccifer 2.0" were also released to reporters and bloggers around the U.S. As one Democratic candidate put it, "Our entire internal strategy plan was made public, and suddenly all this material was out there and could be used against me." The New York Times noted, "The seats that Guccifer 2.0 targeted in the document dumps were hardly random: They were some of the most competitive House races in the country."[129]

Hacking of Republicans

On January 10, 2017, FBI Director James Comey told the Senate Intelligence Committee that Russia succeeded in "collecting some information from Republican-affiliated targets but did not leak it to the public".[130] In earlier statements, an FBI official stated Russian attempts to access the RNC server were unsuccessful,[131] or had reportedly told the RNC chair that their servers were secure,[132] but that email accounts of individual Republicans (including Colin Powell) were breached. (Over 200 emails from Colin Powell were posted on the website DC Leaks.)[131][133][132][134] One state Republican Party (Illinois) may have had some of its email accounts hacked.[135]