Russia and the 2016 Election

# Timeline

## Earlier Russian Hacking

* 2008-2015 “The Dukes” activity earliest known Nov 2008 associated with Chechnya.[[1]](#footnote-1)
* 2010-14 Operation Pawn Storm (TrenMicro) targeting US officials, defense firms, and Russian dissidents with spear phishing, typo squatting, and Sofacy malware [APT-28/Fancy Bear/GRU] to move from “pawn” to high value targets, or to move through attack stages.[[2]](#footnote-2) And later (Feb 2015) discovered iOS X-Agent malware.[[3]](#footnote-3)
* Feb 2012 CozyDuke malware activity associated with MiniDuke and OnionDuke [2015 F-Secure].[[4]](#footnote-4) Targeting govt orgs. Oldest samples from 29 Dec 2011.
* Feb 2014 “One of the first American targets of kompromat was Victoria Nuland, who served as the top U. S. diplomat for Europe during Obama's second term. In February 2014, at the peak of the crisis in Ukraine, Nuland was surreptitiously recorded while speaking on the phone with the U. S. ambassador to Kiev. Frustrated with Europe's lackluster response to the Ukrainian crisis, Nuland said, "Fuck the EU." Shortly after, an aide to the Russian deputy prime minister tweeted a link to a recording of the intercepted phone call. The State Department called the leak "a new low in Russian tradecraft."”[[5]](#footnote-5)
* Fall 2014 Russian intrusion into White House unclas network in Oct.[[6]](#footnote-6) Russian intrusion into State Dept unclas network in Nov (USPS and NOAA breached by PRC)[[7]](#footnote-7). Kaspersky(!) links CozyDuke (CozyBear, CozyCar, OfficeMonkeys [runs a funny flash video while dropping an executable], APT-29), also targeting US, Germany, S Korea, Uzbek.[[8]](#footnote-8) [Called Duke because it reminded Kaspersky of Duqu]—MiniDuke interested in Ukraine NATO MAP in Feb 2013.[[9]](#footnote-9)
  + CozeDuke leverages OneDrive for C2[[10]](#footnote-10)
* April 2015 TV5Monde goes offline due to APT-28 (Fancy/GRU) attacks false-flagged as ISIS “Cyber Caliphate”[[11]](#footnote-11)
* May 2015 APT-28 targeting US banks.[[12]](#footnote-12)

## DNC penetrated in Summer 2015

* Summer 2015 APT-29 gets into DNC
* June 2015 NYT story on St Petersberg Troll factory.[[13]](#footnote-13)
* July 2015 Fireeye Hammertoss malware report describes APT-29 activity & tradecraft, communicating through autogenerated Twitter accounts (each day generate a new account, then check if it exists and follow link and decrypt key to a stock image on GitHub with encrypted commands hidden using basic steganography (after image EOF), anti-forensic techniques, usually in UTC+3 (Moscow,St. P). Discovered early 2015, operating since at least late 2014.[[14]](#footnote-14)
* July 2015 CloudDuke spearphishing campaign leverages OneDrive for C2.[[15]](#footnote-15)
* 25 July 2015 Russian (APT-29/FSB) intrusion into JCS NIPRNET affects 4k personnel; NIPR down for 2 weeks.[[16]](#footnote-16)
* Sep 2015 FBI SA Adrian Hawkins tells IT tech Yared Tamene at DNC (not a fulltime employee) that Dukes had compromised the network. He took no action since he thought the call was a prank. [a mile away!!].[[17]](#footnote-17)
* Oct-Nov 2015 SA Hawkins calls repeatedly by Tamene doesn’t return the calls. In Nov the FBi detects a DNC computer is phoning home. Only by March did Tamene think the FBI was real.[[18]](#footnote-18)
* 17 Dec 2015 Putin praises Trump as “absolute leader in the presidential race….He’s a very lively man, talented without doubt”[[19]](#footnote-19)
* Feb 2016 Announcement of Pentagon budget to increase European Reassurance Initiative[[20]](#footnote-20)April 2016 Leak of Panama Papers (Mossack Fonseca law firm) suggests $2B offshored by Putin’s close associates.[[21]](#footnote-21)
* 19 March 2016 John Podesta, chairman of the Clinton campaign, gets pwned by a spear-fishing email[[22]](#footnote-22) and campaign aide Charles Delavan writes “legitimate” instead of “illegitimate,” unlocking a decade/60k gmails for the Russians.[[23]](#footnote-23) This looked a lot like the Pawn Storm technique and also the bitly shortened links method.
* 22 March 2016 Billy Reinhart, Jr., regional field director in DNC, targeted with Fancy Bear spearphish. (DCLinks has a page for him—“The Rinehart example suggests an end-to-end operation where FANCY BEAR collection was most likely posted to DCLeaks for use as an influence operation.”).[[24]](#footnote-24)
* Mar-Apr 2016 Podesta emails enable (APT-29? CS says APT-28) hacking of Dem Congressional Campaign Committee (DCCC). This material would be released by Guccifer in Sep, targeting close House races in PA, NH, OH, IL, NM, NC.[[25]](#footnote-25)
* 19 April 2016 DCLeaks registered
* Oct15-May16 Threat Group 4127 [aka APT-28/Sofacy/Sednit/GRU] (reporting on 16 June 2016): “Between October 2015 and May 2016, CTU researchers analyzed 8,909 Bitly links that targeted 3,907 individual Gmail accounts and corporate and organizational email accounts that use Gmail as a service. In March 2016, CTU researchers identified a spearphishing campaign using Bitly accounts to shorten malicious URLs. The targets were similar to a 2015 TG-4127 campaign — individuals in Russia and the former Soviet states, current and former military and government personnel in the U.S. and Europe, individuals working in the defense and government supply chain, and authors and journalists — but also included email accounts linked to the November 2016 United States presidential election. Specific targets include staff working for or associated with Hillary Clinton's presidential campaign and the Democratic National Committee (DNC), including individuals managing Clinton's communications, travel, campaign finances, and advising her on policy.”[[26]](#footnote-26)

## Public doxing starts Spring 2016

* 29 Apr 2016 APT-28 breach detected by DNC IT team, which alerts CEO Amy Dacey, who contacts Michael Sussmann, former DoJ cybercrime prosecutor, who knows not to alert the attackers.[[27]](#footnote-27)
* May 2016 DNC hires Crowdstrike within 24 hrs of detection (30 Apr), which deploys Falcon to monitor networks, and begins remediating damage. Discovered Cozy Bear (APT 29/FSB) present since summer 2015, and Fancy Bear (APT 28/GRU) present since late April targeting oppo. (CS attr of 28 to GRU more certain than 29 to FSB; other firms only go so far as “Russian intel”)[[28]](#footnote-28)
  + US intel (probably SIGINT) picks up: “a Russian military intelligence officer bragged to a colleague that his organization, known as the GRU, was getting ready to pay Clinton back for what President Vladimir Putin believed was an influence operation she had run against him five years earlier as Secretary of State. The GRU, he said, was going to cause chaos in the upcoming U.S. election. What the officer didn't know, senior intelligence officials tell TIME, was that U.S. spies were listening.”[[29]](#footnote-29)
* 4 May 2016 DJT becomes presumptive nominee after winning IN and Cruz drops
* 6 June 2016 HRC becomes presumptive nominee after winning NJ
* June 2016 FBI alerts Arizona officials of Russian hacking. Illinois also targeted.[[30]](#footnote-30)
* 14 June 2016 CrowdStrike report on DNC intrusion [updated 15 June][[31]](#footnote-31) [DNC decision to go public, trying to get ahead of the story, only to be checked by Guccifer2 the next day][[32]](#footnote-32)
  + Superb tradecraft, “living off the land” using native Windows tools to avoid detection, concealing RATs, loots of checks, swapping out tools actively, registering domains in advance.
  + APT-29/COZY BEAR/CozyDuke has infiltrated White House, State, JCS, numerous industries. Thought to be FSB (only because more involved in cyber than SVR) because of adversarial relations between Russian agencies (KGB split into FSB [Federal Security Bureau] for internal (most powerful), SVR [Foreign Intel Service] for external (runs illegals); GRU [Main Intel Directorate] is military (includes Spetznaz and ISR/EW))[[33]](#footnote-33)
  + APT-28/FANCY BEAR/Sofacy linked to GRU based on target profile matching Moscow’s strategic interests. Linked to German Bundestag and French TV5 Monde intrusions.
  + WXP (Ellen Nakashima) reports “Russian government hackers penetrated the computer network of the Democratic National Committee and gained access to the entire database of opposition research on GOP presidential candidate Donald Trump….Some of the hackers had access to the DNC network for about a year”[[34]](#footnote-34)
    - Russia denies: ““I completely rule out a possibility that the [Russian] government or the government bodies have been involved in this,” Dmitry Peskov, the Kremlin’s spokesman, told the Reuters news agency in Moscow.”
  + “Alperovitch told me he was thrilled that the DNC decided to publicize Russia's involvement. "Having a client give us the ability to tell the full story" was a "milestone in the industry," he says. "Not just highlighting a rogue nation-state's actions but explaining what was taken and how and when. These stories are almost never told."”[[35]](#footnote-35)
* 15 June 2016 Guccifer 2.0 claims credit for DNC hack and begins doxing internal campaign memos including Trump oppo.[[36]](#footnote-36) CS stands by its assessment that Russian intel is responsible.
  + Guccifer2 claims to be Romanian, but some docs include signatures in Russian (by Felix Dzerzhinsky, aka Iron Felix, founder of the Cheka), and Guccifer makes mistakes in colloquial Romanian.[[37]](#footnote-37)
    - “Matt Tait, a former GCHQ operator who tweets from the handle @pwnallthethings, was particularly prolific. Hours after the first Guccifer 2.0 dump, on the evening of June 15, Tait found something curious.”[[38]](#footnote-38)
  + Guccifer2 is probably not a technical operator, rather a propaganda official (or group) using a French-based VPN; plus several Russian artifacts support att to Russia.[[39]](#footnote-39)
* 20 June 2016 Fidelis (Threat Geek) corroborates CS assessment (useful meta-analysis of naming conventions for groups and malware).[[40]](#footnote-40) Mandiant also backs them up.[[41]](#footnote-41)
* 27 June 2016 Guccifer2 offers HRC emails to “The Smoking Gun” and refers to DCLeaks, described as Wikileaks subproject. Threatconnect assesses (Aug) Guccifer2 and DCLeaks are both Russian influence ops due to Guccifer2 knowledge of things before publicly available, APT28 TTP, DClinks registration artifacts linked to APT28.[[42]](#footnote-42)
* 1 July 2016 DCLeaks posts emails from Gen Philip Breedlove (NATO SACEUR) from 2014 to Colin Power discussing and complaining about Obama’s unwillingness to escalate.[[43]](#footnote-43)
* 5 July 2016 Comey clears Clinton on email server.[[44]](#footnote-44) “we did not find direct evidence that Secretary Clinton’s personal e-mail domain, in its various configurations since 2009, was successfully hacked….We do assess that hostile actors gained access to the private commercial e-mail accounts of people with whom Secretary Clinton was in regular contact from her personal account.”
* 6 July 2016 Guccifer2 dumps DNC battle plan and budget for countering GOP convention in 12 days.[[45]](#footnote-45)
* 6 July 2016 Sanders concedes
* 18-21 Jul 16 GOP convention—DJT nominated
* 22 July 2016 Wikileaks dumps 44k DNC emails + 17k attachments as of 13 Dec beginning on 22 Jul [an error in the NYT story implies they were all at once].[[46]](#footnote-46) The initial dump on 22 Jul is 19k emails and 8k attachments.[[47]](#footnote-47) The slow drip drip keeps them in the news, a lesson learned after Manning. Journos find disparaging emails about Sanders (use his religion against him in the South), infighting, media manipulation, etc.
  + Easier to search than the Guccifer stuff, which people feared was infected
* 24 July 2016 DNC Chairperson Debbie Wasserman Schultz (R-D FL) resigns. HRC campaign manager Robby Mook accuses Russian hackers of trying to elect DJT (on CNN State of the Union)
* 25-28 Jul 2016 Democratic convention—HRC is nominated
* 27 July 2016 DJT: “Russia, if you’re listening, I hope you’re able to find the 30,000 emails that are missing,” Mr. Trump said during a news conference here in an apparent reference to Mrs. Clinton’s deleted emails. “I think you will probably be rewarded mightily by our press.”[[48]](#footnote-48)
* 30 July 2016 FSB Press release about sophisticated cyber espionage found in 20 Russian organizations.[[49]](#footnote-49)
  + “data provided by Microsoft [Dukes use of CloudDrive] also helped America's elite digital spies identify the DNC intruders "with confidence" as Russian”[[50]](#footnote-50) Rid further speculates that 15 Aug ShadowBrokers dump is FSB retaliation for NSA retaliation.
* 12 Aug 2016 Guccifer2 dumps a lot of personal information on Democratic staffers and the Dem Congressional Campaign Committee.[[51]](#footnote-51)
  + The GOP would end up using this material in attack ads
  + “The Russians began to act like a PR agency, providing access to reporters at Politico, The Intercept, and BuzzFeed. Journalists were eager to help.”[[52]](#footnote-52)
* 15 Aug 2016 Guccifer2 follows up with more DCCC docs on Florida, a very competitive race.[[53]](#footnote-53)
* 15 Aug 2016 ShadowBrokers publishes NSA toolkit.[[54]](#footnote-54) Probably the TAO accidentally left the goods on an exposed C2 server that was hacked.[[55]](#footnote-55) Or a human spy walked out with a USB key.[[56]](#footnote-56) Lots of neat things to explore.[[57]](#footnote-57) Not from the Snowden trove.[[58]](#footnote-58) Probably a Russian operation.[[59]](#footnote-59) Is this a warning to the USG not to retaliate?
* 22 Aug 2016 Direct interaction between Guccifer2 and a GOP lobbyist.[[60]](#footnote-60)
* 2 Sep 2016 Putin denies Russian hacking but says that it is for the public good. “It doesn’t really matter who hacked this data from Mrs. Clinton’s campaign headquarters,” Putin said, referring to Democratic presidential nominee Hillary Clinton. “The important thing is the content was given to the public.”[[61]](#footnote-61)
* 4-5 Sep 2016 G20 meeting in Hangzhou, Obama warns Putin not to meddle in the election.[[62]](#footnote-62)
  + 5 Sep 2016 Obama to reporters, a declaratory statement to Russia? “But I will tell you that we have had problems with cyber intrusions from Russia in the past, from other countries in the past,” he added. “And look, we’re moving into a new era here where a number of countries have significant capacities. And frankly we’ve got more capacity than anybody, both offensively and defensively.”[[63]](#footnote-63)
  + 5 Sep 2016 Public reports of IC investigating Russian active measures, but no accusations.[[64]](#footnote-64)
* 22 Sep 2016 Michelle Obama’s passport shows up on DCLeaks.[[65]](#footnote-65)
* Late Sep 2016 “In late September, DC Leaks published hundreds of emails from the account of a twenty-two-year-old freelancer for the Clinton campaign. Lachlan Markay, a reporter for The Washington Free Beacon, found an audio clip buried deep in the cache. In the recording, which was made at a fundraiser in Virginia, Hillary Clinton could be heard describing Sanders supporters as "children of the Great Recession" who "are living in their parents' basement."”[[66]](#footnote-66)
* 26 Sep 2016 DJT in debate: “As far as the cyber, I agree to parts of what Secretary Clinton said. We should be better than anybody else, and perhaps we're not. I don't think anybody knows it was Russia that broke into the DNC. She's saying Russia, Russia, Russia, but I don't — maybe it was. I mean, it could be Russia, but it could also be China. It could also be lots of other people. It also could be somebody sitting on their bed that weighs 400 pounds, okay?”[[67]](#footnote-67)
* 2 Oct 2016 Roger Stone with Trump campaign tweets that “Wednesday @HilaryClinton is done #Wikileaks” implying advance knowledge that Podesta emails would be released
* 3 Oct 2016 Russia suspends participation in Plutonium Management and Disposition Agreement[[68]](#footnote-68)
* 7 Oct 2016 Joint DNI-DHS statement: “The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.”[[69]](#footnote-69)
  + 7 Oct 2016 Vulgar Access Hollywood tape emerges via WXP
  + 7 Oct 2016 Podesta email leaks from Wikileaks begin one hour after AH tape[[70]](#footnote-70) [Check date—7 or 9 Oct?[[71]](#footnote-71)]
* 10 Oct 2016 DJT at a rally in PA: “I love Wikileaks”[[72]](#footnote-72)
* 15 Oct 2016 VP Biden on NBC Meet the Press: “We’re sending a message…We have the capacity to do it…He’ll know it…And it will be at the time of our choosing. And under the circumstances that have the greatest impact.” Biden not concerned that Russia could “fundamentally alter the election.” Would public know if message was sent? Biden: “Hope not”[[73]](#footnote-73)
* 28 Oct 2016 Comey writes an open letter to Congress that he is reopening email investigation.[[74]](#footnote-74)
* 31 Oct 2016 FBI investigation has turned up no direct links between Trump campaign and Russia, and FBI believes the hacking was to disrupt the election not to help Trump.[[75]](#footnote-75)
* 31 Oct 2016 Obama may have used cyber “red line” to warn Putin not to meddle in the election.[[76]](#footnote-76)

## President Elect Trump vs. IC

* 8 Nov 2016 Election day—DJT wins
  + According to Comey (10 Jan SSCI hearing) Russian intel celebrated this win.
  + CozyBear initiates spear phishing against think tanks in DC.[[77]](#footnote-77) And academics.[[78]](#footnote-78)
* 9 Dec 2016 Public reports that CIA assesses Russian motive was to help DJT.[[79]](#footnote-79)
  + NYT points out that GOP was also targeted by Russia but GOP has not been doxed.[[80]](#footnote-80) This is circumstantial evidence that the Russians intended to help Trump.
* “early Dec” Russia arrests FSB officer, Kaspersky scientist, and hacker for treason.[[81]](#footnote-81)
* 11 Dec 2016 DJT denies that Russia helped him to win.[[82]](#footnote-82)
* 13 Dec 2016 NYT breaks backstory on the hack.[[83]](#footnote-83) ADM Rogers: “This was a conscious effort by a nation-state to attempt to achieve a specific effect.” Obama reticent to do anything for fear of escalation with Russia, losing cooperation on Syria, or being accused of electioneering. “Any retaliatory measures were seen through the prism of what would happen in Election Day” said participant in classified planning meeting. Focus shifted from retaliation to protecting voting machines to preclude Trumps “rigged” scenario.
* 16 Dec 2016 FBI agrees that Russian motive was to help DJT.[[84]](#footnote-84)
* 23 Dec 2016 Putin in Moscow: The Democrats “are losing on all fronts and looking elsewhere for things to blame,” he told the nearly 1,400 journalists packed into a Moscow convention hall for the nearly four-hour event. “In my view, this, how shall I say it, degrades their own dignity. You have to know how to lose with dignity.”[[85]](#footnote-85)
* 26 Dec 2016 Former FSB General and current chief of staff for state owned oil firm Rosneft (run by Igor Sechin) found dead in Moscow—potentially one of Steele’s sources.
  + “Gen. Oleg Erovinkin, had been found dead, by his driver, in the back seat of his corporate Lexus which had been parked in a downtown alley in Moscow’s China Town district. Erovinkin, 61, was a KGB/FSB general, who had been head of the Department for Protection of State Secrets at the Kremlin under Yeltsin, and later under the early Putin. In 2008, Putin (then a fresh Prime Minister) appointed him Chief of Staff of his deputy PM Igor Sechin. When Sechin was promoted to President of the state-owned oil giant Rosneft in 2012, Erovinkin followed him into the ominous-sounding, if fuzzily-defined position of “Chief of Special Supervision of the President’s Apparatus.” Insiders have described Erovinkin to me alternately as “Sechin’s treasurer” and “the go-between between Putin and Sechin”. One thing that everyone seems to agree – both in public and private sources – is that Erovinkin was Sechin’s closest associate.”[[86]](#footnote-86)
* 29 Dec 2016 Obama announces expulsion of 35 Russian operatives, closing of US dachas in MD and NY, and new sanctions on individuals responsible for hacking.[[87]](#footnote-87)
  + “I cannot say now what the response will be, although, as we know, there is no alternative here to the principle of reciprocity,” Russian presidential spokesman Dmitry Peskov said in a statement late Thursday evening carried by the Interfax news service. [[88]](#footnote-88)
  + Tass reports “Foreign Minister Sergey Lavrov has called US accusations against Russia of interference in elections groundless… Russia set to declare 35 US diplomats persona non grata”[[89]](#footnote-89) [This will be reversed by Putin] Followed by tweets from “Russia in USA” promising retaliation
  + Simultaneous release of Joint FBI-DHS Grizzly Steppe report.[[90]](#footnote-90) Not very coherent—vague overview and a random list of names and code.
  + The same day, Mike Flynn speaks to Russian ambassador Sergey Kislyak on his vacation in DomRep (apparently Kislyak called him) and suggests Trump will relieve sanctions. US intel (NSA?) monitors the call.[[91]](#footnote-91)
* 30 Dec 2016 ‘Putin said he would wait to see how U.S.-Russian relations develop under the new Trump administration before planning “any further steps” on the issue.’… “We will not create any problems for U.S. diplomats,” Putin said in a statement late Friday afternoon. “We will not expel anyone. We will not prevent their families and children from using their traditional leisure sites during the New Year’s holidays.”[[92]](#footnote-92)
  + “Great move on delay (by V. Putin),” Trump tweeted Friday afternoon. “I always knew he was very smart!”[[93]](#footnote-93)
* 6 Jan 2017 DNI-CIA-NSA-FBI report on Russian interference.[[94]](#footnote-94) Top line assessment but not evidence declassified. NSA and CIA have “high confidence” while NSA has “moderate confidence.” Report details a wide effort, with cyber just one component.
  + Trump is briefed before the public release. During the brief the IC informed Trump about the allegations of Kompromat (CNN reports on 10 Jan).[[95]](#footnote-95)
* 9 Jan 2017 Official Russian denial.[[96]](#footnote-96) Kremlin spokesman: “Groundless accusations which are not supported by anything are being rehearsed in an amateurish, unprofessional way. We don't know what information they are actually relying on.”
* 10 Jan 2017 SSCI open hearing on Russian intel activities with FBI and DNI.[[97]](#footnote-97)
  + “There was evidence that there was hacking directed at state-level organizations and the RNC, but old domains of the RNC, that is, email domains they were no longer using,” Comey told the Senate committee. “Information was harvested from there, but it was old stuff. None of that was released.”[[98]](#footnote-98)
* 10 Jan 2017 CNN goes public with the report that Trump was briefed on the Kompromat allegations, and Buzzfeed opts to release the dossier[[99]](#footnote-99) compiled by Christopher Steele, former MI6 agent now with private firm Orbis hired to do opps during GOP primary then for Dems, then on his own.[[100]](#footnote-100) When Steele felt the FBI was dragging its feet, he went to McCain.[[101]](#footnote-101)
  + Steele later goes into hiding when he is outed.
  + 19 Oct report (via “trusted compatriot” of “close associate,” perhaps the doomed Gen Erovinkin) links Carter Page and Michael Cohen to sanctions relief for 19% Rosneft stake deal allegedly on 7 or 8 July.[[102]](#footnote-102) And, announced on 7 Dec, a 19.5% share of Rosneft was indeed sold to parties unknown.[[103]](#footnote-103)
* 11 Jan 2017 Chaotic press session where Trump admits that Russia was responsible for the hack, denies any blackmail, disparages CNN as fake news, compares the intel community to Nazis.[[104]](#footnote-104)
* 12 Jan 2017 Guccifer2 resurfaces and denies links to Russia.[[105]](#footnote-105)
  + Shadow Brokers says farewell but drops 61 Windows binaries that appear to be NSA tools.[[106]](#footnote-106)
  + Wapo reports that Kislyak phoned Flynn several times on 29 Dec.[[107]](#footnote-107)
* 13 Jan 2017 Spicer denies that Flynn and Kislyak discussed sanctions—it “centered on logistics…plain and simple”
* 14 Jan 2017 “Vice President-elect Mike Pence and Flynn have a conversation, in which Pence says Flynn assured him that “the conversations that took place at that time were not in any way related to the new U.S. sanctions against Russia or the expulsion of diplomats,” according to an account Pence later gave “Fox News Sunday.””[[108]](#footnote-108)
* 15 Jan 2017 Pence on CBS “Face the Nation” and Priebus on NBC “Meet the Press” deny Flynn talked about sanctions.[[109]](#footnote-109)
* 19 Jan 2017 NYT reports that FBI, CIA, NSA, and Treasury are investigating communications and financial data for potential links between Russia and Trump campaign.[[110]](#footnote-110)

## The Trump Administration

* 20 Jan 2017 Donald J. Trump sworn in as 45th POTUS
* 27 Jan 2017 NYT reports (1) “one current and one former United States official, speaking about the classified recruitments on condition of anonymity, confirmed that human sources in Russia did play a crucial role in proving who was responsible for the hacking….the agencies were initially reluctant to disclose their certainty about the Russian role for fear of setting off a mole hunt in Moscow.” ; (2) “Two Russian intelligence officers who worked on cyberoperations and a Russian computer security expert have been arrested and charged with treason for providing information to the United States, according to multiple Russian news reports.”[[111]](#footnote-111)
  + “The arrests, according to reports by the Russian newspaper Kommersant and Novaya Gazeta, among others, were made in early December and amounted to a purge of the cyberwing of the F.S.B., the main Russian intelligence and security agency.”
  + “Sergei Mikhailov, a deputy director of the Center for Information Security, the agency’s computer security arm, and Ruslan Stoyanov, a senior researcher at a prominent Russian computer security company, Kaspersky Lab….a third suspect, Dmitry Dokuchayev…a former hacker…agreed to work for the F.S.B. to avoid prosecution for credit card fraud”
  + “Novaya Gazeta said the F.S.B. began the internal investigation after news media reports that a United States cybersecurity company, ThreatConnect, had linked the election hacking to a Siberian server company…King Servers [on 2 Sept[[112]](#footnote-112)]…the investigation led to Mr. Mikhailov”
  + Interesting that “multiple” Russian sources are advertising treason arrests. Possible interpretations: (1) punishing operators for getting caught; (2) tightening internal discipline in intel agency squabbling; (3) signal to Trump that Russia has more data about hacking; (4) offer an olive branch to Trump by punishing hackers; (5) advertise Moscow’s cyber potency to the world
  + There was apparently a fourth arrest and four other accomplices, and Moscow Times reports they were working for the CIA.[[113]](#footnote-113)
* 28 Jan 2017 Trump speaks to Putin. Speculation before hand that sanction relief is forthcoming. Details of the conversation leaked.[[114]](#footnote-114)
* 9 Feb 2017 Flynn backing away from denials of conversations with Russian ambassador, but denying it was about promising sanctions relief.[[115]](#footnote-115)
* 10 Feb 2017 CNN reports IC corroborates parts of Steele dossier on campaign contacts with foreign nationals.[[116]](#footnote-116)
* 24 Feb 2017 WaPo reports that WH is trying to get Congress and IC members to tamp down Russia stories.[[117]](#footnote-117)
* 20 Mar 2017 In HPSCI testimony, Comey confirms FBI CI investigation into Trump campaign ties to Russia.[[118]](#footnote-118)
  + Previous reports (19 Jan) were not so specific.[[119]](#footnote-119)
* 22 Mar 2017 Devin Nunes (r), HPSCI chair, says in presser “on numerous occasions the Intelligence Community incidentally collected information about U.S. citizens involved in the Trump transition.” Much is unclear here.[[120]](#footnote-120)
* 23 June 2017 Wapo expo on Obama handling of confirmation of Russian active measures[[121]](#footnote-121)
  + “In political terms, Russia’s interference was the crime of the century”
  + “In many ways . . . we dealt with this as a cyberthreat and focused on protecting our cyber infrastructure,” Rhodes said in an interview. “Meanwhile, the Russians were playing this much bigger game, which included elements like released hacked materials, political propaganda and propagating fake news, which they’d pursued in other countries.” “We weren’t able to put all of those pieces together in real time,” Rhodes said, “and in many ways that complete picture is still being filled in.”
  + This is a two level game vs. Russia and the GOP.
  + Using cyber to signal: a cyber operation that was designed to be detected by Moscow but not cause significant damage, officials said. The operation, which entailed implanting computer code in sensitive computer systems that Russia was bound to find, served only as a reminder to Moscow of the United States’ cyber reach….The cyber operation is still in its early stages and involves deploying “implants” in Russian networks deemed “important to the adversary and that would cause them pain and discomfort if they were disrupted,” a former U.S. official said.

# Knowledge Gaps

* Precise timeline of releases by Guccifer2, Wikileaks
* Marginal effect (pro-DJT) of releases
* Marginal effect (pro-HRC) of indignation about Russia
* Effects on down ballot races
* APT-28 v 29 attribution to particular agencies, cases, coordination, motivation
* Russian activity vs. Germany, France, other states
* Russian decision making
* Intel released directly to Trump campaign, not public
* Intel released directly to other GOP campaigns, not public
* Degree of awareness/collaboration by DJT and close advisors with Russia
* Origin of DJT public sympathy for Russia/Putin
* Use of Kompromat against DJT & usefulness if so
* How FBI detected Dukes in DNC
* Details of FBI investigation of Trump-Russia leaks
* Evidence used by US IC for (a) attrib to Russia, (b) to Putin, (c) motive to help Trump
* Why CIA/FBI are “high confidence” while NSA is “moderate confidence”
* When Obama became aware of a-c
* Impact of Orbis reports on IC assessment
* Reliability of Orbis reports (if sources are fabricating, why? Russian long game?)
* The Vermont power grid hack
* State election board
* Reaction of GOP leaders to Russia news
* Ongoing APT activity in DNC after CS mitigation
* Degree of APT penetration of GOP
* APT attacks against USG agencies during election
* US active responses in cyber (or other covert action)
* Voting machine integrity
* Technical details of APT exploitation of DNC
* Shadow Brokers affiliation and timing
* Assange—useful idiot or Russian tool?
* Russian timing alongside primary voting
* Timeline of Russian decision making & evolution of objectives
* Role of Russian criminal/private hackers vs. GRU/FSB
* Why Obama decided to release intel assessment

# Thematic coverage

* Politico timeline of the broader Trump-Russia nexus.[[122]](#footnote-122) And the American Interest on Trump-Russia connections.[[123]](#footnote-123)
  + Manafort had worked to advance Putin interests.[[124]](#footnote-124) And was involved in money laundering for Yanukovych.[[125]](#footnote-125)
* Rid has the best account of the entire episode in Esquire (Oct).[[126]](#footnote-126) The NYT story has some more details (Dec).[[127]](#footnote-127)
* Good summary of the attribution case here.[[128]](#footnote-128) Perhaps better.[[129]](#footnote-129) Rid made a good early summary in Motherboard.[[130]](#footnote-130) Of course it is logically possible that someone else is just acting Russian [but unlikely!].[[131]](#footnote-131)
* Russian noncontact doctrine.[[132]](#footnote-132) Russian hybrid war and the Baltics.[[133]](#footnote-133) Russian IO in Ukraine.[[134]](#footnote-134)
* Background on Russian intelligence agencies.[[135]](#footnote-135) Nexus of Russian intel with criminal hackers.[[136]](#footnote-136) Background on APT-28/Fancy Bear (GRU).[[137]](#footnote-137) “The Dukes” timeline and background.[[138]](#footnote-138)
  + More APT-28 activity called “Iron Twilight”[[139]](#footnote-139)
* Background on Russian propaganda.[[140]](#footnote-140) Dezinformatzia in Sweden, Ukraine as an attack on truth itself.[[141]](#footnote-141) Russian support for fake news in the election.[[142]](#footnote-142)
* Fake news from sources other than Russia. From the right[[143]](#footnote-143) and from pranksters trolling the left.[[144]](#footnote-144)
* The Steele Dossier[[145]](#footnote-145)
* Trump seeking real estate deals in Russia.[[146]](#footnote-146)
* Background on Crowdstrike’s role, focus on Alperovitch.[[147]](#footnote-147)
  + “In 2014, Sony called in CrowdStrike to investigate a breach of its network. The company needed just two hours to identify North Korea as the adversary. Executives at Sony asked Alperovitch to go public with the information immediately, but it took the FBI another three weeks before it confirmed the attribution.”
* Democratic party in disarray[[148]](#footnote-148)
* Russian officials are showing up dead. Former Putin press minister and Gazprom-Media CEO killed in November 2016 in DC.[[149]](#footnote-149)
* Attrib of one white hat: “Matt Tait, a former GCHQ operator who tweets from the handle @pwnallthethings, was particularly prolific.”[[150]](#footnote-150)

# Hypotheses

Much work needed to clarify, consolidate, infer implications, and evaluate.

## Attribution of responsibility (Putin or Others?)

* RIO [Russian Intel Ops] directed by the Kremlin (by Putin personally) [IC]
* GRU and FSB were both directed by the Kremlin but not cooperating
* This was conducted by a rogue Russian agency, without Kremlin direction
* RIS [Russian Intel Services] worked through criminal cutouts
* This was a false flag operation, not Russia

## Russian Intentions (Strategic or Lucky?)

* Coordinated multi-pronged campaign to influence the election (vs. opportunistic efforts) [IC]
* Discredit democratic process and undermine American reputation [IC]
* Discredit HRC during and after election, never expecting DJT to win [IC]
* Help DJT win by discrediting HRC [IC] in order to (a) avoid HRC, (b) create chaos, (c) have a friendly agent
* Help DJT win and then destroy DJT in order to throw US into chaos

## Outcome of the election (Did it Matter?)

* The RIO effect was expressed through some unpredictable, unrepeatable, chaotic feedback interaction. Run this history through a hundred counterfactuals and it wouldn’t happen again.
* RIO somehow prompted investigation of Weiner. Nate Silver argues that Comey’s announcement of this 11 days before the election has a statistically significant effect.
* RIO had an effect on down-ballot races but not the general election. Some suggestion that Guccifer2 was in contact with GOP campaign managers.
* The doxing had no effect, but the blackmailing (or other control) of DJT did have some kind of effect in the messages, themes, etc., the candidate took up.
* RIO had no effect. This is an instance of pure correlation without causation.
* RIO had a negative marginal effect against DJT (attribution of Russia🡪indignation)
* RIO changed voter turnout
* RIO changed the minds of voters
* RIO was necessary for a DJT win (could not have won without it, but might have needed other things to win)
* RIO was sufficient for a DJT win (could have won without it, but didn’t need other things to win)

### Ecological changes correlated with RIO but distinct from it

* Globalization and automation (the information age) create the economic displacement and rural-urban inequality that becomes Trump’s base
* Social media echo chambers polarize the electorate
* Fake news and conspiracy theories from many sources
* The rise of opposition research
* The ease of deconstructing fact claims
* Leaks in politics and organizations to enable leaking
* Twitter as a bully pulpit
* Reality TV and a culture of celebrity
* The rise of cybersecurity firms, operations, agencies

### Particular factors other than RIO

* Dems in office for two terms—GOP as the change party
* The global erosion of liberalism and rise of authoritarians
* Clinton mistakes in the battleground
* Clinton decision to use private email server
* FBI director reversal on investigation 11 days before election
* Clinton perception as establishment candidate
* Cheating by DNC to undermine Sanders
* Sanders lefties not mobilized
* Right wing talk radio, Fox News, and conspiracy theories
* Bad DNC security procedures
* Historical opportunity for GOP
* The idiosyncrasy of the idiot: narcissism, celebrity, charisma, ignorance, inexperience, wealth
* Fear of Mexican immigration, Black crime, Muslim terrorism, Asian capitalists
* Gen X and Millennials don’t have the anti-Russian allergic reaction of Cold Warriors

## Trump relationship to Russia (Nitwit or Traitor?)

* Useful idiot (will destroy American and/or NATO on his own recognizance)
* Sympathetic character with compatible interests (an American oligarch)
* Indirect control through agents in his campaign/staff
* Knowing conspiracy during the election to (a) accept intelligence, (b) active measures vs HRC
* Direct control via blackmail for (a) sex acts, (b) bribes, (c) criminal connection, (d) conspiracy with RIS, (e) something that reveals DJT to be a poor, stupid failure
* Direct control via bribes
* Long term relationship/conspiracy/agent

## Trumps’s Russia-Friendly statements (Idiot or Intention?)

* Contrarianism with establishment (change candidacy)
* Controversy & belligerence as attention ploy (narcissistic psychology)
* Putin bromance
* Genuine DJT policy preferences, independent of Russia (policy of restraint)
* Under Russian control

## Obama’s Public Release of Intel Assessment

* If Trump is a Russian agent or was aided by Russia significantly, he would not continue the investigation, so put pressure on him, and Congress, to follow through
* Make it harder for Trump to continue to work for Moscow’s interests by alerting the press, all of Congress, the public to potential collusion
* Get the 1st draft of history closer to the truth
* Signal/response to Russia: we know all, you can’t get away with it
* Signal to allies: beware, or, we are compromised
* Get the FBI back in line
* Bait Trump into overreacting
* Smear Trump, delegitimize election, hobble Trump administration, help Dems
* Salve Obama’s legacy: make it harder for Trump to undo everything by casting suspicion on him and delegitimizing his presidency; show that Obama’s legacy was changed for the worse only because others did not play by the rules.
* Begin Obama’s transition to an activist in the public sphere
* Begin preparations for a coup if the Russians are taking over: encourage professionals in the security agencies to consider hindering or disobeying orders they feel are not in American interests

## The Steele Dossier (Credible or Not?)

* All true
* Reported in good faith by agents with access, with some errors in memory/interpretation
* Some agents are fabricating or exaggerating some things for personal reasons
* Some (all) agents are active disinformation measures run by the Kremlin—Steele is an unwitting tool (worse, witting double agent)
* Fabricated by Steele or his associates—there are no agents
* Corroborated/Undermined by other IC sources
* Suppressed/Ignored/Actioned by the FBI

1. https://www.f-secure.com/documents/996508/1030745/dukes\_whitepaper.pdf [↑](#footnote-ref-1)
2. https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf [↑](#footnote-ref-2)
3. http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/?linkId=12146208 [↑](#footnote-ref-3)
4. https://www.f-secure.com/documents/996508/1030745/CozyDuke [↑](#footnote-ref-4)
5. http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/ [↑](#footnote-ref-5)
6. https://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251\_print.html [↑](#footnote-ref-6)
7. https://www.nytimes.com/2014/11/17/us/politics/state-department-targeted-by-hackers-in-4th-agency-computer-breach.html?pagewanted=all&\_r=0 [↑](#footnote-ref-7)
8. https://securelist.com/blog/research/69731/the-cozyduke-apt/ [↑](#footnote-ref-8)
9. https://securelist.com/blog/incidents/31112/the-miniduke-mystery-pdf-0-day-government-spy-assembler-0x29a-micro-backdoor/ [↑](#footnote-ref-9)
10. https://securelist.com/blog/research/69731/the-cozyduke-apt/ [↑](#footnote-ref-10)
11. http://www.bbc.com/news/technology-37590375 [↑](#footnote-ref-11)
12. http://www.mediafire.com/file/bdr77piwp0ij0qz/FSOFACY.pdf [↑](#footnote-ref-12)
13. https://www.nytimes.com/2015/06/07/magazine/the-agency.html?\_r=0 [↑](#footnote-ref-13)
14. This is really cool tradecraft! <https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf> [↑](#footnote-ref-14)
15. https://www.f-secure.com/documents/996508/1030745/dukes\_whitepaper.pdf [↑](#footnote-ref-15)
16. http://www.cnbc.com/2015/08/06/russia-hacks-pentagon-computers-nbc-citing-sources.html [↑](#footnote-ref-16)
17. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [↑](#footnote-ref-17)
18. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [↑](#footnote-ref-18)
19. https://www.washingtonpost.com/world/putin-no-major-gaps-with-washington-over-efforts-to-end-syria-conflict/2015/12/17/a178255e-a431-11e5-8318-bd8caed8c588\_story.html?tid=a\_inl&utm\_term=.737a5df0f780 [↑](#footnote-ref-19)
20. https://www.washingtonpost.com/news/checkpoint/wp/2016/02/01/pentagon-unveils-budget-priorities-for-next-fiscal-year-countering-russia-and-china/?tid=a\_inl&utm\_term=.2871f8f06c6c [↑](#footnote-ref-20)
21. https://www.theguardian.com/news/2016/apr/03/panama-papers-money-hidden-offshore [↑](#footnote-ref-21)
22. https://wikileaks.org/podesta-emails/emailid/34899 [↑](#footnote-ref-22)
23. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [↑](#footnote-ref-23)
24. https://www.threatconnect.com/blog/does-a-bear-leak-in-the-woods/ [↑](#footnote-ref-24)
25. https://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html?\_r=0 [↑](#footnote-ref-25)
26. <https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign> [↑](#footnote-ref-26)
27. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [↑](#footnote-ref-27)
28. See also CS report 15Jun16. https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0\_story.html?utm\_term=.825158229247 [↑](#footnote-ref-28)
29. http://time.com/4783932/inside-russia-social-media-war-america/ [↑](#footnote-ref-29)
30. https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e\_story.html?tid=a\_inl&utm\_term=.45f6d675a9e3 [↑](#footnote-ref-30)
31. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ [↑](#footnote-ref-31)
32. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [↑](#footnote-ref-32)
33. This is really good background on these services and their activities, including crime ties (good for money laundering) and active measures: http://www.ecfr.eu/publications/summary/putins\_hydra\_inside\_russias\_intelligence\_services [↑](#footnote-ref-33)
34. https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0\_story.html?utm\_term=.825158229247 [↑](#footnote-ref-34)
35. http://www.esquire.com/news-politics/a49902/the-russian-emigre-leading-the-fight-to-protect-america/ [↑](#footnote-ref-35)
36. https://guccifer2.wordpress.com/2016/06/15/dnc/ [↑](#footnote-ref-36)
37. http://arstechnica.com/security/2016/06/guccifer-leak-of-dnc-trump-research-has-a-russians-fingerprints-on-it/ [↑](#footnote-ref-37)
38. http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/ [↑](#footnote-ref-38)
39. https://www.threatconnect.com/blog/guccifer-2-all-roads-lead-russia/ [↑](#footnote-ref-39)
40. http://www.threatgeek.com/2016/06/dnc\_update.html [↑](#footnote-ref-40)
41. https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3\_story.html?utm\_term=.90aedaa27e38 [↑](#footnote-ref-41)
42. <http://thesmokinggun.com/documents/investigation/tracking-russian-hackers-638295?_ga=1.46010852.1558185730.1484426665> See also <https://www.threatconnect.com/blog/does-a-bear-leak-in-the-woods/> [↑](#footnote-ref-42)
43. https://theintercept.com/2016/07/01/nato-general-emails/?\_ga=1.46010852.1558185730.1484426665 [↑](#footnote-ref-43)
44. https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system [↑](#footnote-ref-44)
45. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [↑](#footnote-ref-45)
46. https://wikileaks.org/dnc-emails/ [↑](#footnote-ref-46)
47. https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm\_term=.b92739b09efa [↑](#footnote-ref-47)
48. https://www.nytimes.com/2016/07/28/us/politics/donald-trump-russia-clinton-emails.html [↑](#footnote-ref-48)
49. http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10437870%40fsbMessage.html [↑](#footnote-ref-49)
50. http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/ [↑](#footnote-ref-50)
51. http://arstechnica.com/tech-policy/2016/08/guccifer-2-0-doxes-hundreds-of-house-democrats-with-massive-document-dump/ [↑](#footnote-ref-51)
52. http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/ [↑](#footnote-ref-52)
53. https://twitter.com/GUCCIFER\_2/status/765246466956886020 [↑](#footnote-ref-53)
54. http://arstechnica.com/security/2016/08/group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof/ [↑](#footnote-ref-54)
55. https://medium.com/@thegrugq/shadow-broker-breakdown-b05099eb2f4a#.j7tnd0r76 [↑](#footnote-ref-55)
56. https://cybersecpolitics.blogspot.ca/2016/08/why-eqgrp-leak-is-russia.html [↑](#footnote-ref-56)
57. https://musalbas.com/2016/08/16/equation-group-firewall-operations-catalogue.html [↑](#footnote-ref-57)
58. https://www.lawfareblog.com/very-bad-monday-nsa-0 [↑](#footnote-ref-58)
59. https://www.ft.com/content/d63c5b3a-65ff-11e6-a08a-c7ac04ef00aa [↑](#footnote-ref-59)
60. https://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html?\_r=0 [↑](#footnote-ref-60)
61. https://www.washingtonpost.com/world/putin-denies-that-russia-hacked-the-dnc-but-says-it-was-for-the-public-good/2016/09/02/d507a335-baa8-40e1-9805-dfda5d354692\_story.html?utm\_term=.ec4f846c1156 [↑](#footnote-ref-61)
62. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [↑](#footnote-ref-62)
63. http://www.politico.com/story/2016/09/obama-russia-cyber-arms-race-227732 [↑](#footnote-ref-63)
64. https://www.washingtonpost.com/world/national-security/intelligence-community-investigating-covert-russian-influence-operations-in-the-united-states/2016/09/04/aec27fa0-7156-11e6-8533-6b0b0ded0253\_story.html?utm\_term=.c1b614e7af4a [↑](#footnote-ref-64)
65. http://www.reuters.com/article/us-usa-cyber-idUSKCN11S2G3 [↑](#footnote-ref-65)
66. http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/ [↑](#footnote-ref-66)
67. https://www.washingtonpost.com/news/the-fix/wp/2016/09/27/the-answer-that-best-exemplifies-how-badly-donald-trump-was-out-of-his-depth-in-the-debate/?utm\_term=.2cd846bca161 [↑](#footnote-ref-67)
68. http://fissilematerials.org/library/2016/10/decree\_by\_the\_president\_o.html [↑](#footnote-ref-68)
69. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national [↑](#footnote-ref-69)
70. http://www.politifact.com/truth-o-meter/statements/2016/dec/18/john-podesta/its-true-wikileaks-dumped-podesta-emails-hour-afte/ [↑](#footnote-ref-70)
71. http://motherboard.vice.com/read/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts [↑](#footnote-ref-71)
72. https://www.youtube.com/watch?v=mUtT0b0EnSw [↑](#footnote-ref-72)
73. https://www.nytimes.com/2016/10/16/us/politics/biden-hints-at-us-response-to-cyberattacks-blamed-on-russia.html [↑](#footnote-ref-73)
74. http://www.nytimes.com/interactive/2016/10/28/us/politics/fbi-letter.html?\_r=0 [↑](#footnote-ref-74)
75. https://www.nytimes.com/2016/11/01/us/politics/fbi-russia-election-donald-trump.html [↑](#footnote-ref-75)
76. https://sputniknews.com/us/201612201048770210-obama-putin-us-election-armed-conflict/ [↑](#footnote-ref-76)
77. http://www.reuters.com/article/us-usa-election-cyber-russia-idUSKBN1352P9 [↑](#footnote-ref-77)
78. https://techcrunch.com/2016/11/14/russian-hacking-team-the-dukes-targeting-ngos-and-think-tanks-after-trump-victory/ [↑](#footnote-ref-78)
79. https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c\_story.html?tid=a\_inl&utm\_term=.2551eea8314b [↑](#footnote-ref-79)
80. https://www.nytimes.com/2016/12/10/us/politics/trump-mocking-claim-that-russia-hacked-election-at-odds-with-gop.html?\_r=0 [↑](#footnote-ref-80)
81. https://mobile.nytimes.com/2017/01/27/world/europe/russia-hacking-us-election.html [↑](#footnote-ref-81)
82. https://www.washingtonpost.com/news/powerpost/wp/2016/12/11/trump-denies-cia-report-russia-intervened-to-help-him-win-election/?utm\_term=.4af25739b225 [↑](#footnote-ref-82)
83. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [↑](#footnote-ref-83)
84. https://www.washingtonpost.com/politics/clinton-blames-putins-personal-grudge-against-her-for-election-interference/2016/12/16/12f36250-c3be-11e6-8422-eac61c0ef74d\_story.html?utm\_term=.b2cb12b745e5 [↑](#footnote-ref-84)
85. https://www.washingtonpost.com/world/europe/trump-syria-hacking-and-terrorism-in-play-as-russias-putin-meets-the-press/2016/12/23/28ead25a-c878-11e6-acda-59924caa2450\_story.html?tid=a\_inl&utm\_term=.662f8c33c8fe [↑](#footnote-ref-85)
86. https://cgrozev.wordpress.com/2017/01/14/tower-of-cards-part-1/ [↑](#footnote-ref-86)
87. Graphic includes details: https://www.washingtonpost.com/world/national-security/obama-administration-announces-measures-to-punish-russia-for-2016-election-interference/2016/12/29/311db9d6-cdde-11e6-a87f-b917067331bb\_story.html?tid=a\_inl&utm\_term=.549a0035dc0b [↑](#footnote-ref-87)
88. Graphic includes details: https://www.washingtonpost.com/world/national-security/obama-administration-announces-measures-to-punish-russia-for-2016-election-interference/2016/12/29/311db9d6-cdde-11e6-a87f-b917067331bb\_story.html?tid=a\_inl&utm\_term=.549a0035dc0b [↑](#footnote-ref-88)
89. http://tass.com/politics/923449 [↑](#footnote-ref-89)
90. https://www.us-cert.gov/sites/default/files/publications/JAR\_16-20296A\_GRIZZLY%20STEPPE-2016-1229.pdf [↑](#footnote-ref-90)
91. https://www.washingtonpost.com/world/national-security/flynns-swift-downfall-from-a-phone-call-in-the-dominican-republic-to-a-forced-resignation-at-the-white-house/2017/02/14/17b0d8e6-f2f2-11e6-b9c9-e83fce42fb61\_story.html [↑](#footnote-ref-91)
92. Original statement: <http://en.kremlin.ru/events/president/news/53678>. Reported in: https://www.washingtonpost.com/world/russia-plans-retaliation-and-serious-discomfortoverus-hacking-sanctions/2016/12/30/4efd3650-ce12-11e6-85cd-e66532e35a44\_story.html [↑](#footnote-ref-92)
93. https://www.washingtonpost.com/news/powerpost/wp/2016/12/30/trump-praises-putins-response-to-sanctions-calls-russian-leader-very-smart/?utm\_term=.87a796b887d2 [↑](#footnote-ref-93)
94. https://www.dni.gov/files/documents/ICA\_2017\_01.pdf [↑](#footnote-ref-94)
95. http://www.cnn.com/2017/01/10/politics/donald-trump-intelligence-report-russia/index.html [↑](#footnote-ref-95)
96. http://www.independent.co.uk/news/world/americas/putin-us-intelligence-report-russian-election-hacking-witch-hunt-president-amateur-unprofessional-a7517636.html [↑](#footnote-ref-96)
97. https://www.intelligence.senate.gov/hearings/open-hearing-russian-intelligence-activities [↑](#footnote-ref-97)
98. https://www.wired.com/2017/01/russia-hacked-older-republican-emails-fbi-director-says [↑](#footnote-ref-98)
99. https://www.documentcloud.org/documents/3259984-Trump-Intelligence-Allegations.html [↑](#footnote-ref-99)
100. https://www.nytimes.com/2017/01/10/us/politics/donald-trump-russia-intelligence.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=a-lede-package-region&region=top-news&WT.nav=top-news&\_r=0 [↑](#footnote-ref-100)
101. https://www.theguardian.com/us-news/2017/jan/11/trump-russia-report-opposition-research-john-mccain [↑](#footnote-ref-101)
102. https://cgrozev.wordpress.com/2017/01/14/tower-of-cards-part-1/ [↑](#footnote-ref-102)
103. http://www.reuters.com/article/us-russia-rosneft-privatisation-insight-idUSKBN1582OH [↑](#footnote-ref-103)
104. https://www.nytimes.com/2017/01/11/us/politics/trumps-press-conference-highlights-russia.html [↑](#footnote-ref-104)
105. https://guccifer2.wordpress.com/2017/01/12/fake-evidence/ [↑](#footnote-ref-105)
106. http://arstechnica.com/security/2017/01/nsa-leaking-shadow-brokers-lob-molotov-cocktail-before-exiting-world-stage/ [↑](#footnote-ref-106)
107. https://www.washingtonpost.com/opinions/why-did-obama-dawdle-on-russias-hacking/2017/01/12/75f878a0-d90c-11e6-9a36-1d296534b31e\_story.html [↑](#footnote-ref-107)
108. https://www.washingtonpost.com/news/fact-checker/wp/2017/02/15/the-firing-of-michael-flynn-a-timeline/?utm\_term=.c511e2afe2db [↑](#footnote-ref-108)
109. https://www.washingtonpost.com/news/fact-checker/wp/2017/02/15/the-firing-of-michael-flynn-a-timeline/?utm\_term=.c511e2afe2db [↑](#footnote-ref-109)
110. https://mobile.nytimes.com/2017/01/19/us/politics/trump-russia-associates-investigation.html [↑](#footnote-ref-110)
111. https://mobile.nytimes.com/2017/01/27/world/europe/russia-hacking-us-election.html [↑](#footnote-ref-111)
112. https://www.threatconnect.com/blog/state-board-election-rabbit-hole/ [↑](#footnote-ref-112)
113. https://themoscowtimes.com/news/russia-federal-agents-suspected-of-treason-are-reportedly-being-charged-with-passing-secrets-to-the-cia-56994 [↑](#footnote-ref-113)
114. https://www.washingtonpost.com/world/national-security/details-of-trump-putin-call-raise-new-white-house-leak-concerns/2017/02/09/162f0fe6-ef0b-11e6-b4ff-ac2cf509efe5\_story.html?utm\_term=.f3f646c9dbb5 [↑](#footnote-ref-114)
115. https://www.nytimes.com/2017/02/09/us/flynn-is-said-to-have-talked-to-russians-about-sanctions-before-trump-took-office.html [↑](#footnote-ref-115)
116. http://edition.cnn.com/2017/02/10/politics/russia-dossier-update/index.html [↑](#footnote-ref-116)
117. https://www.washingtonpost.com/world/national-security/trump-administration-sought-to-enlist-intelligence-officials-key-lawmakers-to-counter-russia-stories/2017/02/24/c8487552-fa99-11e6-be05-1a3817ac21a5\_story.html?utm\_term=.4dac39f3b0a5 [↑](#footnote-ref-117)
118. https://www.washingtonpost.com/world/national-security/fbi-director-to-testify-on-russian-interference-in-the-presidential-election/2017/03/20/cdea86ca-0ce2-11e7-9d5a-a83e627dc120\_story.html?tid=pm\_world\_pop&utm\_term=.4bb46cdc7359 [↑](#footnote-ref-118)
119. https://www.washingtonpost.com/world/national-security/us-counterintelligence-officials-are-examining-possible-ties-between-russia-and-trump-associates/2017/01/19/7e10f31c-debd-11e6-918c-99ede3c8cafa\_story.html?tid=a\_inl&utm\_term=.a5a15493baf9 [↑](#footnote-ref-119)
120. https://www.lawfareblog.com/what-heck-devin-nunes-talking-about-guide-perplexed [↑](#footnote-ref-120)
121. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking [↑](#footnote-ref-121)
122. http://www.politico.com/trump-russia-ties-scandal-guide/timeline-of-events [↑](#footnote-ref-122)
123. http://www.the-american-interest.com/2016/12/19/the-curious-world-of-donald-trumps-private-russian-connections/ [↑](#footnote-ref-123)
124. https://apnews.com/122ae0b5848345faa88108a03de40c5a/Manafort's-plan-to-'greatly-benefit-the-Putin-Government [↑](#footnote-ref-124)
125. https://www.washingtonpost.com/world/new-documents-say-trump-aide-hid-payments-from-pro-moscow-ukraine-party/2017/03/21/92ec85f2-0e11-11e7-9d5a-a83e627dc120\_story.html?utm\_term=.89ba7b2962b8 [↑](#footnote-ref-125)
126. http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/ [↑](#footnote-ref-126)
127. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [↑](#footnote-ref-127)
128. http://arstechnica.com/security/2016/12/the-public-evidence-behind-claims-russia-hacked-for-trump/ [↑](#footnote-ref-128)
129. https://www.emptywheel.net/2016/12/10/evidence-prove-russian-hack/ [↑](#footnote-ref-129)
130. https://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack [↑](#footnote-ref-130)
131. http://icitech.org/its-the-russians-or-is-it-cold-war-rhetoric-in-the-digital-age/ [↑](#footnote-ref-131)
132. Dima’s CDD chapter [↑](#footnote-ref-132)
133. http://www.alexlanoszka.com/LanoszkaIAHybrid.pdf [↑](#footnote-ref-133)
134. https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html [↑](#footnote-ref-134)
135. <http://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services> [↑](#footnote-ref-135)
136. https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html [↑](#footnote-ref-136)
137. https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf [↑](#footnote-ref-137)
138. <https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf> [↑](#footnote-ref-138)
139. https://www.secureworks.com/research/iron-twilight-supports-active-measures [↑](#footnote-ref-139)
140. http://www.rand.org/pubs/perspectives/PE198.html [↑](#footnote-ref-140)
141. https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html [↑](#footnote-ref-141)
142. https://www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af66098fe\_story.html?utm\_term=.b7dced31abed [↑](#footnote-ref-142)
143. https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html?\_r=0 [↑](#footnote-ref-143)
144. https://www.buzzfeed.com/jamieross/this-guy-tricked-infowars-into-publishing-a-completely-fake?utm\_term=.bhM0bLMNm#.oxAvOyqo1 [↑](#footnote-ref-144)
145. http://www.vanityfair.com/news/2017/03/how-the-explosive-russian-dossier-was-compiled-christopher-steele [↑](#footnote-ref-145)
146. https://www.nytimes.com/2017/01/16/us/politics/donald-trump-russia-business.html?smid=pl-share&\_r=0 [↑](#footnote-ref-146)
147. http://www.esquire.com/news-politics/a49902/the-russian-emigre-leading-the-fight-to-protect-america/ [↑](#footnote-ref-147)
148. http://www.politico.com/magazine/story/2017/01/democrats-trump-administration-wilderness-comeback-revival-214650 [↑](#footnote-ref-148)
149. http://www.npr.org/sections/thetwo-way/2016/03/11/470064826/former-putin-aide-died-of-blunt-force-injuries-in-d-c-medical-report-says [↑](#footnote-ref-149)
150. http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/ [↑](#footnote-ref-150)