Mueller Report Summary (by Hodey Johns)

- **What is the Mueller Report?**
  - It is an ongoing criminal investigation into the Russian government's effort to interfere with the 2016 presidential election.
    - The investigation is headed by Special Counsel Robert Mueller.
      - More on him in a sec
    - It is being conducted by the both the FBI and law enforcement
- **Who is Robert Mueller**
  - Longtime FBI director under George W. Bush
    - Took over one week before the 9/11 terror attacks
    - Was instrumental in going to war with Iraq
      - Achieved viral fame for giving sworn testimony before the Senate, saying, "[s]even countries designated as state sponsors of terrorism—Iran, Iraq, Syria, Sudan, Libya, Cuba, and North Korea—remain active in the United States and continue to support terrorist groups that have targeted Americans. As Director Tenet has pointed out, Secretary Powell presented evidence last week that Baghdad has failed to disarm its weapons of mass destruction, willfully attempting to evade and deceive the international community. Our particular concern is that Saddam Hussein may supply terrorists with biological, chemical or radiological material."

        - Stood up against “enhanced interrogation” techniques at the CIA, even proposing a public toast to honor Tom Wilner, a lawyer assigned to defend tortured detainees
    - Served with Attorney General John Ashcroft
    - Defended the Patriot Act
        - Said that the government's surveillance programs complied "in full with U.S. law and with basic rights guaranteed under the Constitution"
        - Claimed 9/11 would have been “derailed” with the surveillance program in place
    - Also led teams to find and execute Edward Snowden
        - After it was revealed the US attempted to assassinate Snowden on a plane out of Russia, Mueller defended the decision
            - “We are taking all necessary steps to hold Edward Snowden responsible for these disclosures”
    - After George W Bush, Obama asked him to stay on for two more years and then he went to the private sector
        - Was hired as an independent counsel to see if the NFL knew the video of Ray Rice striking his girlfriend existed before handing out his suspension
            - He determined they did not
        - Given the role of “Settlement Master” in the Volkswagen Emissions Scandal
            - Found that Volkswagen had knowingly tampered with every single emissions monitor on their commercial vehicles
            - Oversaw $11.2 billion in reparations to customers.
        - Performed an external review of the NSA after their massive data breach in 2016
            - Determined there was negligence in “security, personnel, and management processes and

practices" at the NSA, but it was no legal grounds with which to fine or punish them
        - While he was still private, he was hired by the Obama administration to decide to to press charges in the Boston Marathon terrorist attack
    - Mueller was interviewed to be director for the Trump administration, but Trump passed on him
        - Because of his history of working with George W Bush, Obama, and Trump passing up on him for the job, the Senate Intelligence Committee confirmed him to lead the investigation due to a lack of natural bias
- **The Mueller Report**
- I have decided to go section by section and provide a synopsis. The full version is available under our show notes. It is currently up to 37 pages, making it a pretty short read, so feel free to read it for yourself
    - It begins with a list of the 12 Russian Operatives who are being indicted
        - It is widely assumed that we will not actually make any real effort to arrest these people, nor that Russia will hand them over
    - Count One: Conspiracy to Commit an Offense Against the United States
        - The first paragraph specifically indicates that these names were indeed hired by Russia to create chaos
        - Counter to what many think, those indicted were not rogue agents, they were specifically hired by Russia to meddle in the election
        - Ordered "to gain unauthorized access (to "hack") into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election"

- Operation began in official capacity in March of 2016
    - Started by hacking into accounts of Clinton volunteers and, notably, they gained access to the e-mail of her campaign chairman
- In the following month, April, they gained access to hundreds of e-mail accounts at the DNC (along with all of the individual e-mails they sent or received)
    - These e-mails belonged to real people, but they were monitored and sent malware to others while the users were offline
- Later that month, they made plans to release the documents
- In June, they made the tens of thousands of documents obtained public
    - All were under fake personas or groups
    - Most were just a page or two here and there, but two names "DCLeaks" and "Guccifer 2.0" released all of the documents
    - The DNC and Clinton campaign countered that these documents were forged and/or fake, suppressing their own brief investigations that determined, quite immediately, that the leaks were real
- Due to their widespread control and access, they continued to release new documents all the way through November under the Guccifer 2.0 account
- In an attempt to hide their identities, they established bases of computers, including in the United States, to network investigators through. They also used BitCoin to hide their financial activity

- It then goes on to list each of the twelve indicted operatives, how they were caught, and what role they played

        - It is clear that the network was much, much more than these twelve individuals, but these twelve are all that are known at this time
            - The investigation is ongoing, so more could be added, but none have been added since the initial release of the report several months back, so it is thought to be unlikely that we will find more operatives
    - The Charge
        - The report explicitly states that the reason behind this activity was to interfere with the 2016 US Election
    - Details of the “spearphishing” operation
        - If you have Harry on for this episode, he’s going to eat this section up because it validates pretty much every paranoid thing people say about online security
        - Spearphishing is the process of asking someone to change their password, inadvertently giving the person who asks access with the new password as well
        - Fake username “john356gh” was created with a domain that appeared to be from a Google official but was actually Russian
            - This part might be what led to actually catching Russia’s official involvement. It was found that the domain was established and registered by their government sanctioned servers
            - Making it appear from an official at Google is a process known as “spoofing”
        - The biggest catch from this spearphishing operation was the chairman, John Podesta
            - Through his account alone, over 50,000 e-mails were accessed

- A few weeks after Podesta fell for the hoax, Robby Mook, the campaign manager, and Jake Sullivan, Senior Foreign Policy Advisor, also fell for the hoax
    - Each of these leaks contained notably damaging information
        - Podesta's leaks revealed Clinton was informed about the attack on Benghazi, she did not act on the information, and deliberately staged a plan to cover it up, lie about it, and pin the attack on a cartoonist
            - This particular leak accounted for a 12% swing in the polls in a single week, the largest swing in the election
        - Mook's leaks revealed Clinton's engagement with the media and conspiracy with the DNC. It was revealed she gained access to debate questions beforehand, planted questions from the media, and worked with DNC officials to keep funding from Bernie Sanders
        - Sullivan's leak contained the script for an unrecorded speech Clinton gave overseas. In it, the script said that she stated the following:
            - "What makes for successful immigration? It's no brain surgery, but the media have long failed to provide a clear credible answer. They are unable to come up with an answer or don't like the answer that's staring them in the face. The main reason behind successful immigration should be painfully obvious to even the most dimwitted of observers: Some groups of people are almost always highly successful given only half

> a chance (Jews*, Hindus/Sikhs and Chinese people, for example), while others (Muslims, blacks** and Roma***, for instance) fare badly almost irrespective of circumstances. The biggest group of humanity can be found somewhere between those two extremes – the perennial overachievers and the professional never-do-wells."

- Ultimately, it seems to conspirators used DCLeaks to release individual documents that may or may not have been important while others were used for the more important "fish" in the scheme
- All information phished in this way was relayed to e-mail "hi.mymail@yandex.com" a Russian domain server
    - This particular e-mail was Russian general domain and not a government server. It is theorized that the investigation would perhaps lead to this e-mail, accessible on any public server, and the conspirators had not counted on Mueller finding their government accounts
- On April 6th, the conspirators created an account "with a one-letter deviation from the actual spelling" of a well known staffer. They sent an e-mail from that account with a document attached, titled, "hillaryclinton-favorable-rating.xlsx"
    - This document, when opened, created duplicate actions on a Russian server, allowing the conspirators to read, see, and look at every keystroke from over 30 Clinton campaign staffers. With many of these 30 being administrators, they essentially gained almost every affiliate's password and login information

        - On July 27th, the conspirators sent e-mails from administrators whose accounts they had spearphished and keylogged, asking anyone who had a domain name under the Clinton campaign. They managed to gain access to another 76 accounts after this.
    - Hacking the DNC
        - Occurred during the same time frame, beginning in March
        - The DNC's security was much tougher than the Clinton campaign. The spent some time probing for weaknesses.
            - Using hacked Clinton campaign e-mail domains, on March 15th, the conspirators "ran a technical query for the DNC's internet protocol configurations to identify connected devices."
            - On the same day, they ran internal queries about the DNC, Democratic Party, and other Clinton affiliates
            - On April 7th, the conspirators "ran a technical query for the DCCC's internet protocol configurations to identify connected devices"
        - After the technical query, on the same day, the conspirators managed to send an e-mail from the DNC domain name. Using the same spearphishing technique as the Clinton campaign, an employee, who's name is redacted but was identified by the Mueller investigation, clicked the link sent and typed his/her password
            - This employee had a high-level access, and his/her password worked on 10 different computers. Using this information, the conspirators managed to steal the passwords and e-mails from everyone who used these 10 computers
            - They were also able to view the activity from these computers through an "X-Agent malware." This explained why the hack at the Clinton campaign was

released to the public in text format, while the DNC lifted information was produced in pictures of screenshots

- One of the computers was accessed by a high-level government official, and his/her password was able to be used to unlock a leased set of servers in Arizona. This set of servers contained the usernames, e-mails, passwords, and personal information for everyone at the DNC. The conspirators gained access to all of it
- On April 14th, the original employee contacted a major fundraiser for the Clinton campaign through a messaging system. The conversation, which lasted for 8 hours, detailed major campaign violations, as well as collusion between the Clinton campaign and the DNC
    - The information was so specific, the hackers found the specific account where the illegal transactions were occurring, but were not able to view the transactions
- On April 19th, knowing that the release of the information would force the DNC and Clinton campaign to change their security protocols, the conspirators set up a “middle server” to the one in Arizona.
    - This actually made the problem for the DNC and Clinton campaign worse. When the two hacked entities changed their security protocol, and transferred servers, all of the old information, as well as new security information, went from the Arizona server through this unknown “middle server” on the way to the new server
    - This gave the conspirators complete access to all existing login and personal information as well as all future information as soon as it was created

        - Through more malware, they then gained access to another 33 computers by June
        - One of these computers belonged to the major fundraiser for the Clintons that was speaking to the redacted employee. Using a keylog, the hackers gained access to the bank account along with all of the illegal transactions
    - Finding documents of note
        - With information piling up, the some of the conspirators dedicated their time to finding worthwhile information
            - They initially searched for documents containing the words “hillary” “cruz” and “trump”
        - After reading through the e-mails dealing with Benghazi, they found a thread titled “Benghazi Investigation” which detailed initial warning, the lack of response, and the commands to destroy information about how the attack was predicted by US Intelligence
            - The conspirators followed the e-mail chain and forum thread around, unearthing the damning information that we know about Benghazi today
        - To lift such a large chunk of documents, the conspirators inserted an “X-Tunnel” malware virus, which compressed these files into small data chunks that would not be caught by firewalls or security
            - On April 22nd, information on candidates and opposition was sent to a computer in Illinois
                - It is through this set of data that it was discovered Hillary Clinton had ordered millions of dollars to be spent targeting Rand Paul, far more than any other candidate. She believed him to be the most difficult candidate for her to defeat in the 2016 election
            - Another chunk of data was sent to the same computer on April 28th

        - Between May 25 and June 1, the conspirators found their way into the Microsoft software of the DNC
            - They began constructing a “PowerShell” command, which would restore documents on the computers, even ones that had been deleted
        - On May 30th, one of the conspirators managed to access the DNC security and firewall systems
            - He/She set the settings to allow the thirteen different malware systems on the computers
        - Beginning May 13th and going through June 20th, the conspirators began to erase their steps
            - Once information was lifted, they deleted the logs, destroying any electronic evidence that anything had been stolen
            - This also included erasing login history, making it difficult to find who was hacked
    - Detecting the intruders
        - By the end of May, with the release of a few documents here and there, the DNC and Clinton campaign became painfully aware they were hacked
        - A single private-sector company (name is redacted) was hired to try to root out the conspirators
            - In a fun little victory for libertarians, e-mail correspondence showed that public officials turned to the private sector whenever there were serious problems, admitting candidly to one another that the government security systems weren’t as good
        - The conspirators managed to stay on the servers, to some degree, until the end of October
        - On May 31st, the conspirators researched the company’s open source code for finding threats and adjusted their malware

        - On June 14th, the conspirators created a website “actblues.com” on their own servers to mimic and existing and well-known Democratic fundraising link
            - The money still was sent and received successfully, but the hackers now had record of where it went from and to
                - The violations were extensive and were a big part of the eventual Wikileaks release
        - On June 20th, the private security company had detected and shut down the malware to the DNC. They also blocked the logins based on the area the computers were logging in from
        - In September, the conspirators regained access to the DNC logins through a third party cloud hosting service
            - They were only able to access a fraction of the computers as before, but they did manage to get ahold of the DNC analytics
            - They used snapshots and sent each shot individually to avoid setting off data breach signals
    - The Leak
        - On April 19th, the documents began to surface slowly
            - After attempting and failing to establish the domain “electionleaks.com” the conspirators managed to successfully establish a domain called “dcleaks.com”
            - It was established under the e-mail “dirbinsaabol@mail.com” and paid for with cryptocurrency
                - This e-mail was the same one used to establish the “john356gh” URL that originally infiltrated the Clinton campaign
        - On June 8th, the bulk of the data was released through the DC Leaks website

- The website falsely claimed the conspirators were “American hacktivists”
- It was shut down quickly, but received over 1 million views before it could be dealt with
    - After petition from the conspirators, the website was reo-opened
- DC Leaks continued to release new documents almost daily all the way through the election
    - Some of these leaks, oddly, were from an infiltration into Republican donor account back in 2015
        - The information wasn’t useful or damaging, but did lend some credence to the idea that the conspirators were trying to create chaos and the Democrats simply got back luck when it came to hiring people who didn’t understand phishing and spoofing scams

- The conspirators also turned to creating fake social media identities to get the information out
    - Names included “Alice Donovan” “Jason Scott” and “Richard Gingrey”
    - They also promoted the DC Leaks website
    - On June 8th, a Twitter account for DC Leaks was created under “@dcleaks_”
        - “the Conspirators used the same computer to operate the Twitter account @BaltimoreIsWhr, through which they encouraged U.S. audiences to “[j]oin our flash mob” opposing Clinton and to post images with the hashtag #BlacksAgainstHillary”

- Guccifer 2.0 Sidetrack

- On June 16th, after nearly a month after claiming the documents were forged, the DNC admitted they had been hacked
    - Specifically, the private company identified the origin as “Russian agents”
- In an attempt to remain anonymous, the Russian hackers launched an online persona “Guccifer 2.0” who claimed to be a Romanian and the lone hacker behind the infiltration
- The company, unbeknownst to the hackers, was not fooled
    - In fact, the day before, they had traced the origin to a computer in Moscow where the conspirators had a virus planted on their computers
        - The virus was very limited and could only pick up on browser search results
        - The conspirators had searched for the following things before getting rid of the virus: “some hundred sheets” “some hundreds of sheets” “dcleaks” “illuminati” “широко известный перевод” “worldwide known” “think twice about” and “company’s competence”
    - The private cyber security firm managed to find an online document from Guccifer 2.0
        - It read: “Worldwide known cyber security company [Company 1] announced that the Democratic National Committee (DNC) servers had been hacked by “sophisticated” hacker groups. I’m very pleased the company appreciated my skills so highly))) [. . .] Here are just a few docs from many thousands I extracted when hacking into DNC’s network. [. . .] Some hundred sheets! This’s a serious

case, isn't it? [. . .] I guess [Company 1] customers should think twice about company's competence. F[***] the Illuminati and their conspiracies!!!!!!!!! F[***] [Company 1]!!!!!!!!!"

- This meant that Company 1, the private firm, was able to tie the Russians to this red herring identity

- Even with their cover blown, Guccifer 2.0 was still used to release documents through WordPress between June and October
  - It is unclear if the conspirators knew this account had been compromised. They may have continued to use it even though they were no longer fooling the private security company because its popularity surpassed that of even DC Leaks

- Others caught in the trap
  - It should be noted that, because this was an investigation into the Russian hackers, everyone who committed a crime's name is redacted. But because this investigation led to other indictments, which no longer protect the identity of the indicted, we have found out the following information
  - On August 15th, Paul Manafort asked Guccifer 2.0 directly for a copy of the stolen documents. Guccifer 2.0 complied. This was, of course, against the law as the chairman for the Trump campaign to ask for illegally obtained information
  - Guccifer 2.0 transferred the 2.5 Gigabytes of data to Wikileaks founder Julian Assange after he requested the information about 3 days before the Democratic National Convention. This information included numerous illegal

donations tied to 2,000 donors, who were mentioned by name in the release

- Assange said, “if you have anything hillary related we want it in the next tweo [sic] days prefable [sic] because the DNC [Democratic National Convention] is approaching and she will solidify bernie supporters behind her after...we. think trump has only a 25% chance of winning against hillary ... so conflict between bernie and hillary is interesting.”
- WikiLeaks did not publicly admit to asking Guccifer 2.0 for the documents until the Mueller report was released

- On or about August 15, 2016, the Conspirators, posing as Guccifer 2.0, wrote to Roger Stone who was in regular contact with senior members of the presidential campaign of Donald J. Trump, “thank u for writing back . . . do u find anyt[h]ing interesting in the docs i posted?” On or about August 17, 2016, the Conspirators added, “please tell me if i can help u anyhow . . . it would be a great pleasure to me.” On or about September 9, 2016, the Conspirators, again posing as Guccifer 2.0, referred to a stolen DCCC document posted online and asked the person, “what do u think of the info on the turnout model for the democrats entire presidential campaign.” The person responded, “[p]retty standard.”
  - Stone, of course, indicated that he’d read the illegally obtained documents and, as an advisor, broke the law by doing so
  - Notably, Mueller recovered a Twitter record of Stone’s conversation with Guccifer 2.0, but the record indicates that Stone never told Trump about the documents.

        - An undisclosed reporter was given copies of papers that showed Black Lives Matter had funded the Clinton campaign. This reporter responded, asking for more information, but the information was never given and the story was never released. Several reporters have come forward saying it was him/her
        - Another US reporter was given the chance to access documents from "Hillary Clinton's Staff" but the reporter never opened the document, fearing it might be a virus
            - The Mueller investigation reveals it was, indeed, the files
        - Guccifer 2.0 had already been tied to the conspirators by the private security firm, but they tied this identity to DC Leaks by tracing the funding for both of them to the same pool of BitCoin.
            - This bitcoin had also been used to buy a server in Malaysia to throw off the investigation, but, as previously noted, it was too late
            - The conspirators still had the Guccifer 2.0 account claim that it had "totally no relation to the Russian government."
    - Counts 2-9 "Aggravated Identity Theft"
        - It's hard to believe, but everything before this was just one count of "Conspiracy to Commit an Offense Against the United States"
            - It's the most difficult charge to prove, which is why it took up the majority of the indictment
        - Counts 2-9 are all "Aggravated Identity Theft." While well more than this many identities were stolen, only 8 could be tied to an exact operative
            - Mueller had to go to great lengths to prove which Russian agent was on the other end of the computer
    - Count 10 "Conspiracy to Launder Money"

        - Money Laundering is the act of taking money from an illegal source or for insidious means and making that source and transaction look legal
            - By using the money intended for National Defense and spending it on hacking, Mueller believes he has a case to say this BitCoin money was laundered
    - Count 11 “Conspiracy to Commit an Offense Against the United States”
        - This one, while the same as the first charge, is for a different reason
        - Two of the conspirators, using a Russian server, attempted to hack into “U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections”
            - Some have alleged that this was to literally steal the election, which is not what the Mueller report suggests
            - Mueller alleges that the conspirators were attempting to gain information about voters and perhaps use their information to sway their decision
        - In July of 2016, these conspirators, using the same techniques as before, managed to gain access to personal information on over 500,000 voters “including names, addresses, partial social security numbers, dates of birth, and driver’s license numbers”
            - They managed to do this by spearphishing a State Board of Election Office
            - With information acquired by the DNC, they hacked into a Vendor in August and verified the data was accurate

        - This breach did not go undetected, however, and the FBI began rapidly tracing the two conspirators
            - They then erased their history and deleted their malware
    - Having breached voter data at the federal level, the two then attempted the same techniques at the state level, starting with “Georgia, Iowa, and Florida”
        - Mueller is unclear if this hack was successful, but it does not appear they got past the “probing” stage for spearphishing
            - Yes, the states had better cybersecurity than the federal government
    - In November, right before the election, the two hackers sent out 100 spearphishing emails to organizations and personnel involved in administering elections in numerous Florida counties. They used the vendor’s logo and domain from the hack
        - This attempt was unsuccessful
- The rest
    - Statutory allegations, such as attempting to steal funds through the Act Blues website, hacking into a computer worth over $5,000, and causing over $5,000 in damage due to property replacement
    - A notice to the indicted that they forfeit their rights on US Property and will be taken into custody
    - A notice that their property, not just their personage, is subject to be seized

Show Notes

Full Mueller Report Here: https://www.justice.gov/file/1080281/download