From Bytes to Bias

The GRU's Convergence of Hacking and Disinformation

A bit about me

- Working in security for 7 years
- Studied criminology and international relations
- Hacking related to geopolitics is a passion
- Cofounded Arachne Digital

ARACHNE

We will cover

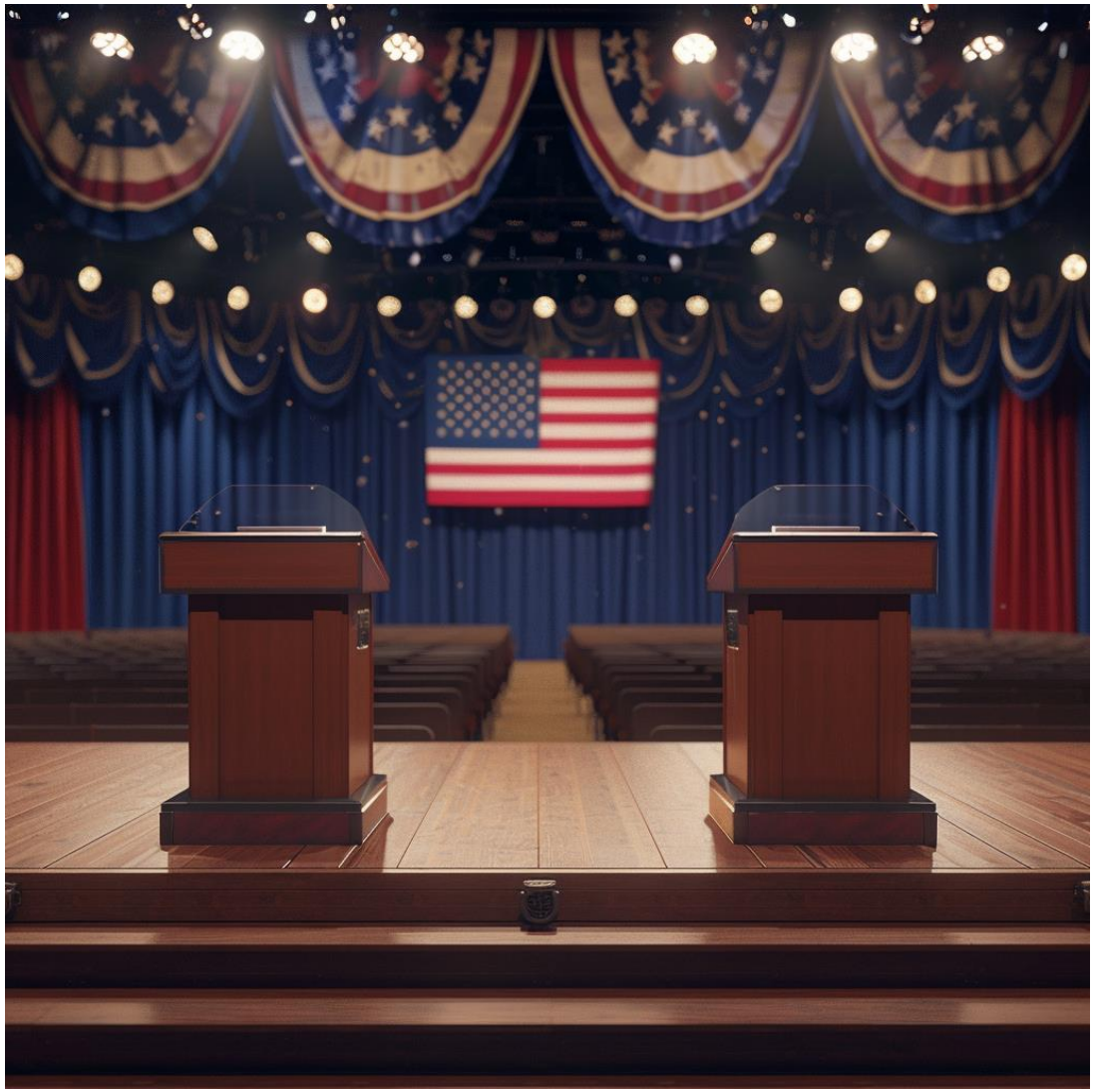
- 2016 U.S. presidential election interference
- Context – United States
- Context – Russia
- Timeline of events outlined in *The United States v Viktor Borisovich Netyksho et al.*
- What does all this mean? Hacking
- What does all this mean? Disinformation

ARACHNE

Context United States

2016 U.S. presidential election

- Between Hillary Clinton and Donald Trump
- Marked by scandals
  - Clinton's private email server used while Secretary of State
  - Trump's Access Hollywood tape
  - DNC/DCCC hack
- Election held November 8th
- Trump loses popular vote but secures the Electoral College vote, becoming the 45th president of the United States
- Trump presidency dogged by rumours of Russian collusion



ARACHNE

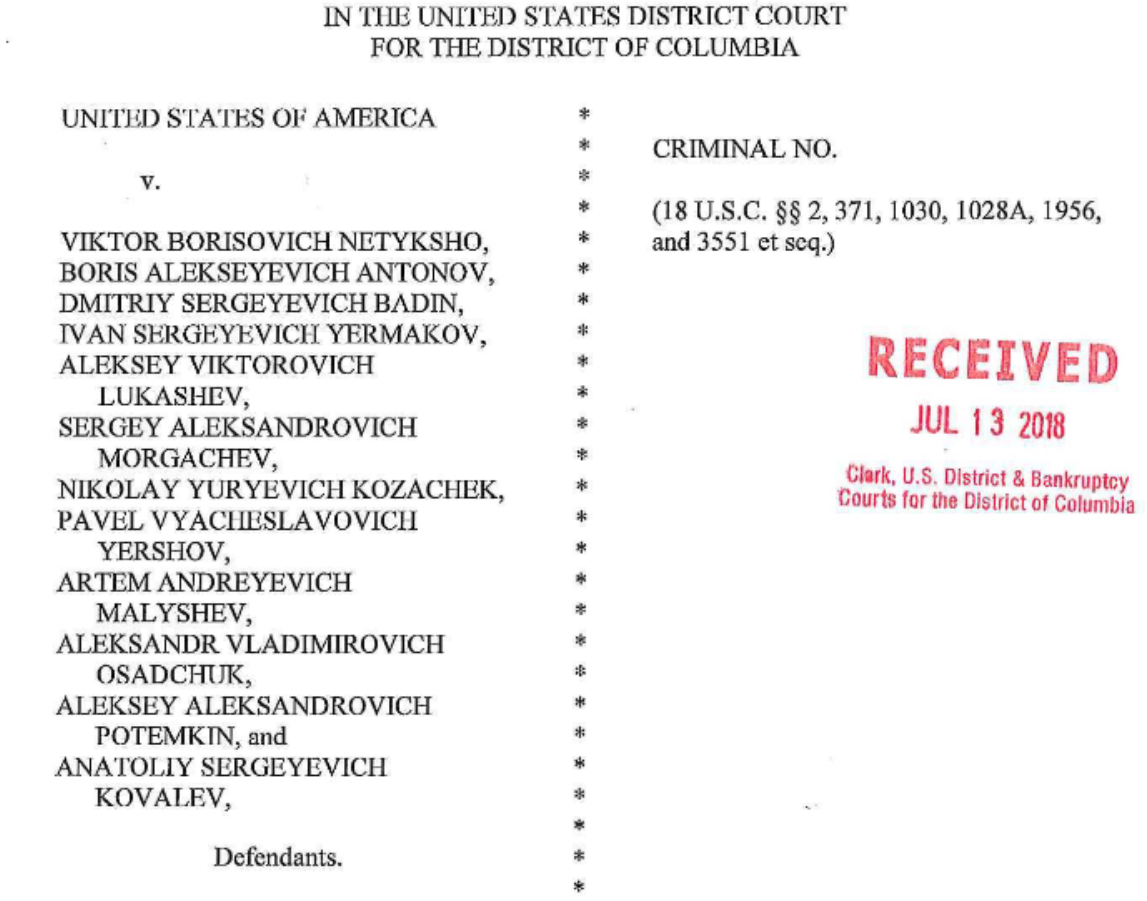
Why is the 2016 U.S. presidential election important?

- So many reasons they don't fit!
- Hillary Clinton was potentially going to be the first female U.S. President
- Donald Trump, a businessman with no prior political or military experience, secured the Republican nomination, challenging norms about who can be a successful candidate
- Bernie Sanders, a self-described democratic socialist, gained substantial support
- The rise of "fake news"
- Trump appointed three Justices to the U.S. Supreme Court
- Trump's victory led to significant changes in U.S. policy, both domestically (e.g., tax reform, deregulation) and internationally (e.g., withdrawal from the Paris

ARACHNE

Where has this information come from?

- Public domain
- Robert Mueller
- Many indictments and reports released, the events covered are restricted to *The United States v Viktor Borisovich Netyksho et al.*



IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	*	
	*	CRIMINAL NO.
v.	*	
	*	(18 U.S.C. §§ 2, 371, 1030, 1028A, 1956,
VIKTOR BORISOVICH NETYKSHO,	*	and 3551 et seq.)
BORIS ALEKSEYEVICH ANTONOV,	*	
DMITRIY SERGEYEVICH BADIN,	*	
IVAN SERGEYEVICH YERMAKOV,	*	
ALEKSEY VIKTOROVICH LUKASHEV,	*	
SERGEY ALEKSANDROVICH MORGACHEV,	*	
NIKOLAY YURYEVICH KOZACHEK,	*	
PAVEL VYACHESLAVOVICH YERSHOV,	*	
ARTEM ANDREYEVICH MALYSHEV,	*	
ALEKSANDR VLADIMIROVICH OSADCHUK,	*	
ALEKSEY ALEKSANDROVICH POTEMKIN, and	*	
ANATOLIY SERGEYEVICH KOVALEV,	*	
	*	
Defendants.	*	
	*	

RECEIVED
JUL 13 2018
Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

https://nsarchive.gwu.edu/document/16702-indictment

ARACHNE

Names of organisations

- DNC – Democratic National Committee
- DCCC – Democratic Congressional Campaign Committee
- Company 1 – CrowdStrike
- Organisation 1 – Wikileaks
- SBOE 1 – believed to be the Illinois State Board of Elections
- Vendor 1 – believed to be VR Systems, a Florida-based company that provides election management software and electronic poll books to several U.S. states

ARACHNE

Context Russia

Charged in *The United States v Viktor Borisovich Netyksho et al.*

- 12 GRU officers
- Unit 26165 and Unit 74455
- Fancy Bear and Sandworm

ARACHNE

GRU history

- The Main Directorate of the General Staff of the Armed Forces of the Russian Federation
- Foreign military intelligence agency of the Russian Armed Forces.
- Established in 1918, originally focused on protecting the Bolshevik regime.
- Expanded to foreign intelligence, human assets, propaganda, and sabotage operations.

https://en.wikipedia.org/wiki/GRU_(Russian_Federation)#/media/File:Emblem_of_the_GRU.svg

ARACHNE

GRU development

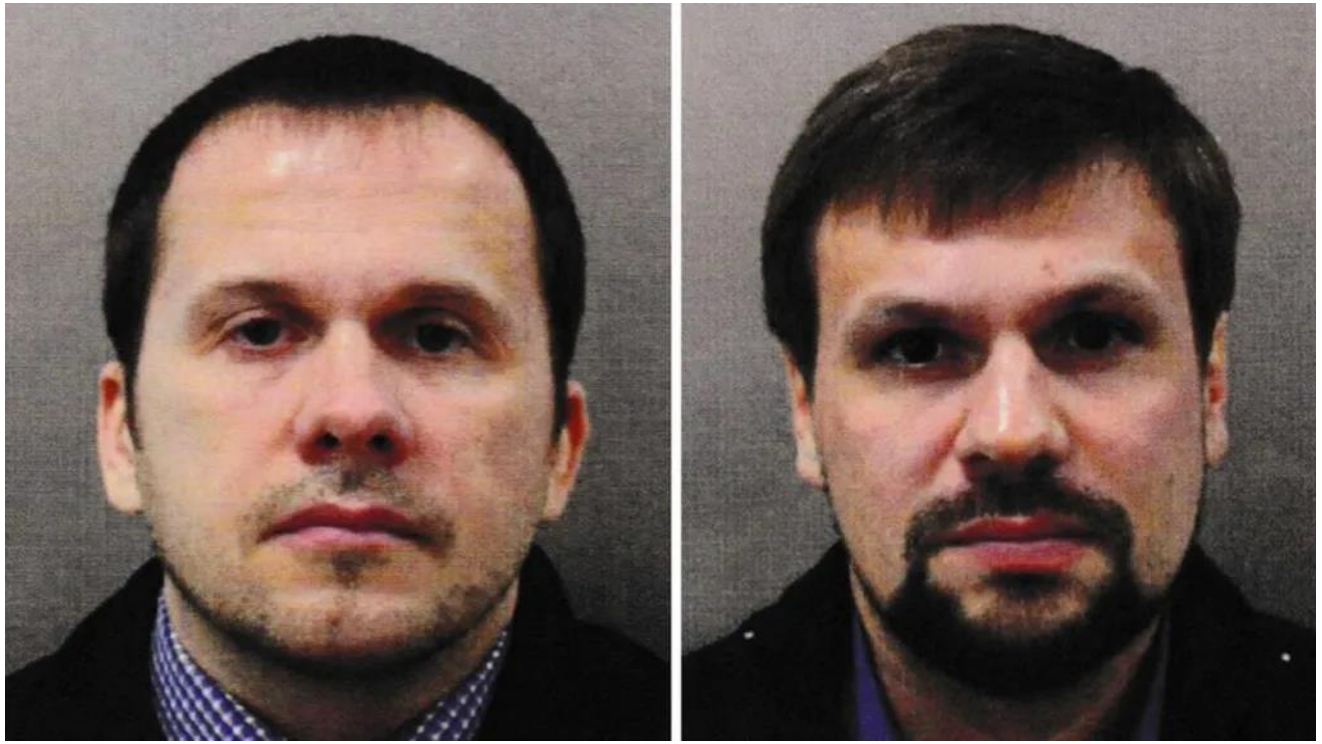
- Known for aggressive operations and rivalries with other Soviet agencies
- Became the Main Intelligence Directorate of the General Staff in 1942
- Played significant roles in WWII, Cold War espionage, and modern conflicts
    - Successful penetration of Britain's atom bomb program during the Cold War

https://en.wikipedia.org/wiki/Raising_a_Flag_over_the_Reichstag

ARACHNE

Post Soviet era

- Retained independence and foreign intelligence role after the Soviet Union's dissolution.
- Offering bounties to Taliban-linked fighters to attack U.S. and other international forces in Afghanistan.
- 2014 arms depot explosion in the Czech Republic, Russian occupation in Crimea
- 2015 Ukraine blackout
- 2016 interference in the U.S. presidential campaign, attempted coup in Montenegro, hacking World Anti-Doping Agency, second Ukraine blackout
- 2017 NotPetya
- 2018 Salisbury nerve agent attack on a former GRU officer living in Britain and his daughter, attempted hack of Organization for the Prohibition of Chemical Weapons
- 2022 Russian invasion of Ukraine



Alexander Mishkin (left) and Anatoliy Chepiga (right)

https://www.bbc.com/news/uk-51722301

ARACHNE

GRU organisational identity and culture

- Dual role in intelligence collection and military operations (spetsnaz)
- Culture of risk-taking and aggression to showcase its value to Russia's leadership
- Engages in cyber operations, disinformation campaigns, and traditional espionage
- Focuses on internal talent cultivation for cyber operations, contrasting with FSB's approach working with cybercriminals

https://www.ft.com/content/f28913f6-1d8f-11e4-8f0c-00144feabdc0

ARACHNE

Victor Netyksho

- Head of Unit 26165
- Unit 26165 had primary responsibility for hacking the DCCC and DNC, as well as the email accounts of individuals affiliated with the Clinton Campaign.

https://informnapalm.org/en/ukrainian-hacktivists-acquired-first-ever-photo-of-the-gru-hacker-unit-commander/

ARACHNE

Boris Antonov

- Head of Department A of Unit 26165
- Department A was dedicated to targeting military, political, governmental, and non-governmental organisations with spearphishing emails and other computer intrusion activity.
- Antonov supervised other co-conspirators who targeted the DCCC, DNC, and individuals affiliated with the Clinton Campaign.

Boris Alekseyevich Antonov

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

Dmitriy Badin

- Assistant head of Department A of Unit 26165
- Badin, along with Antonov, supervised other co-conspirators who targeted the DCCC, DNC, and individuals affiliated with the Clinton Campaign.

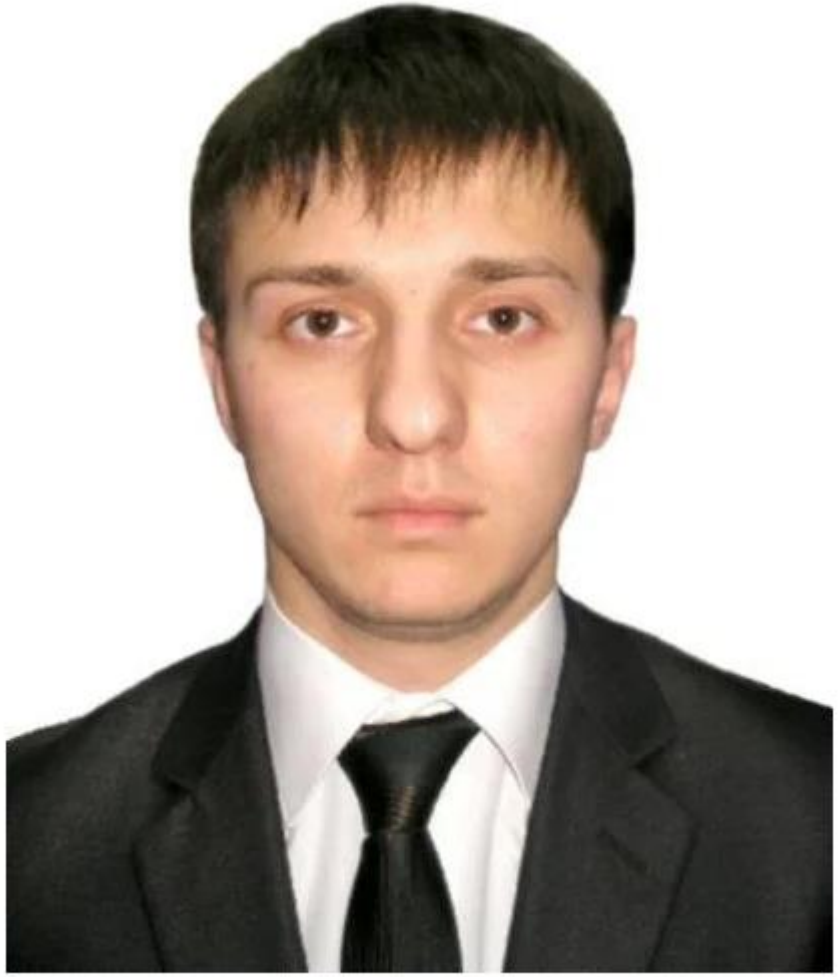
Dmitriy Sergeyevich Badin

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

Ivan Yermakov

- Member of Department A of Unit 26165
- Yermakov was responsible for hacking email accounts, hacking the DNC email server and stealing DNC emails.



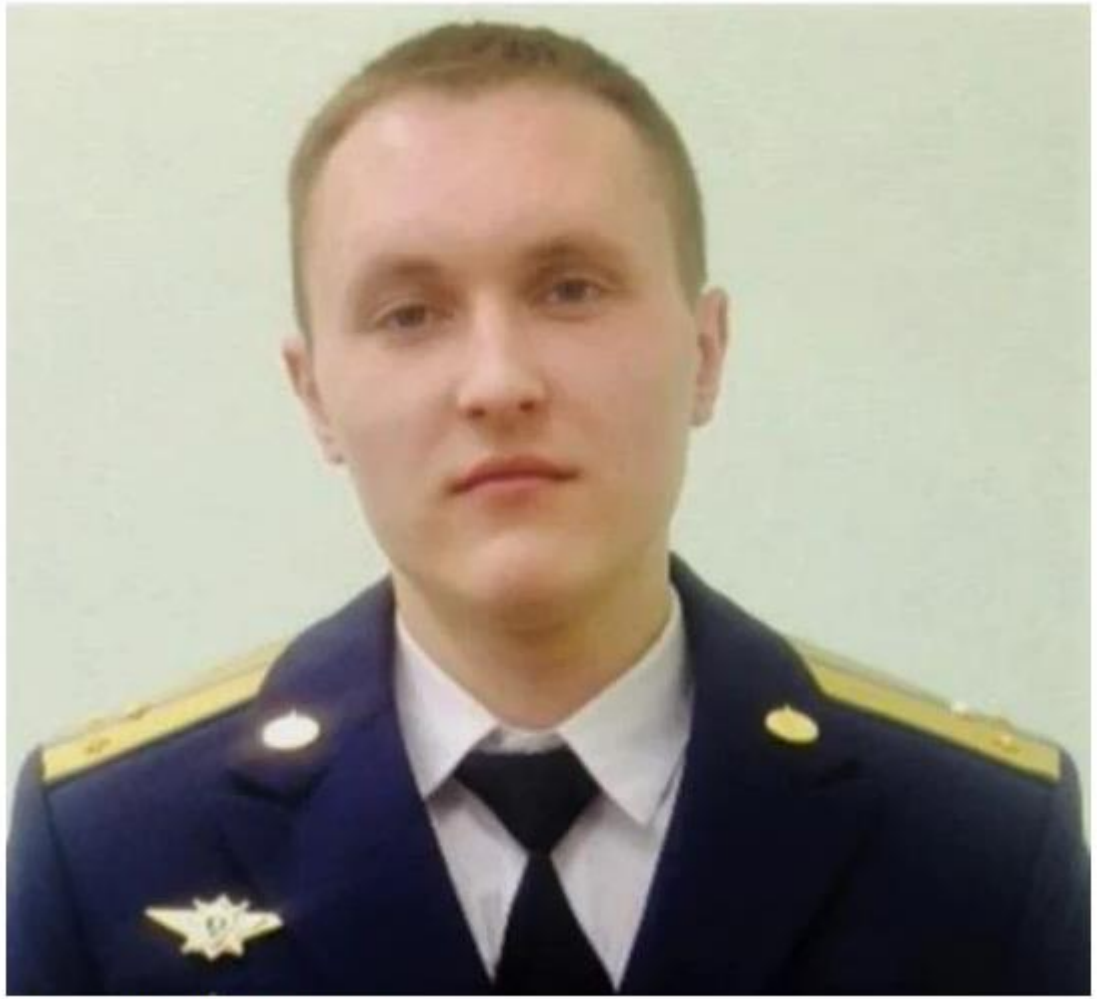
Ivan Sergeyevich Yermakov

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

Aleksey Lukashev

- Member of Department A of Unit 26165
- Lukashev was responsible for sending spearphishing emails to members of the Clinton Campaign and affiliated individuals, including the chairman of the Clinton Campaign.



Aleksey Viktorovich Lukashev

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

Sergey Morgachev

- Head of Department B of Unit 26165
- Morgachev supervised the co-conspirators who developed and monitored the X-Agent malware

Sergey Aleksandrovich Morgachev

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

Nikolay Kozachek

- Members of Department B of Unit 26165
- Kozachek developed, customised, and monitored X-Agent

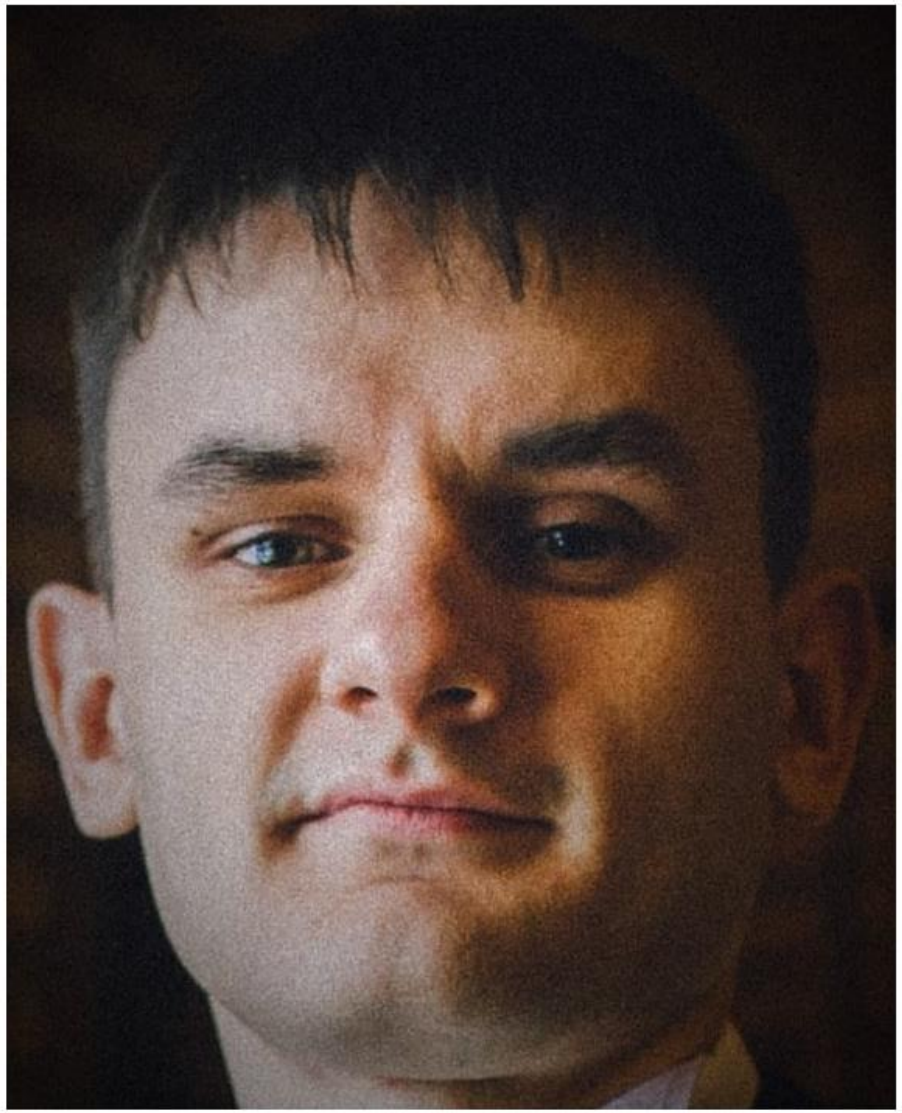
Nikolay Yuryevich Kozachek

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

Pavel Yershov

- Member of Department B of Unit 26165
- Yershov tested and customised X-Agent



Pavel Vyacheslavovich Yershov

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

Artem Malyshev

- Member of Department B of Unit 26165
- Malyshev monitored X-Agent

Artem Andreyevich Malyshev

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

Aleksandr Osadchuk

- Head of Unit 74455
- Unit 74455 assisted in the release and promotion of stolen documents, and the publication of anti-Clinton content on social media accounts

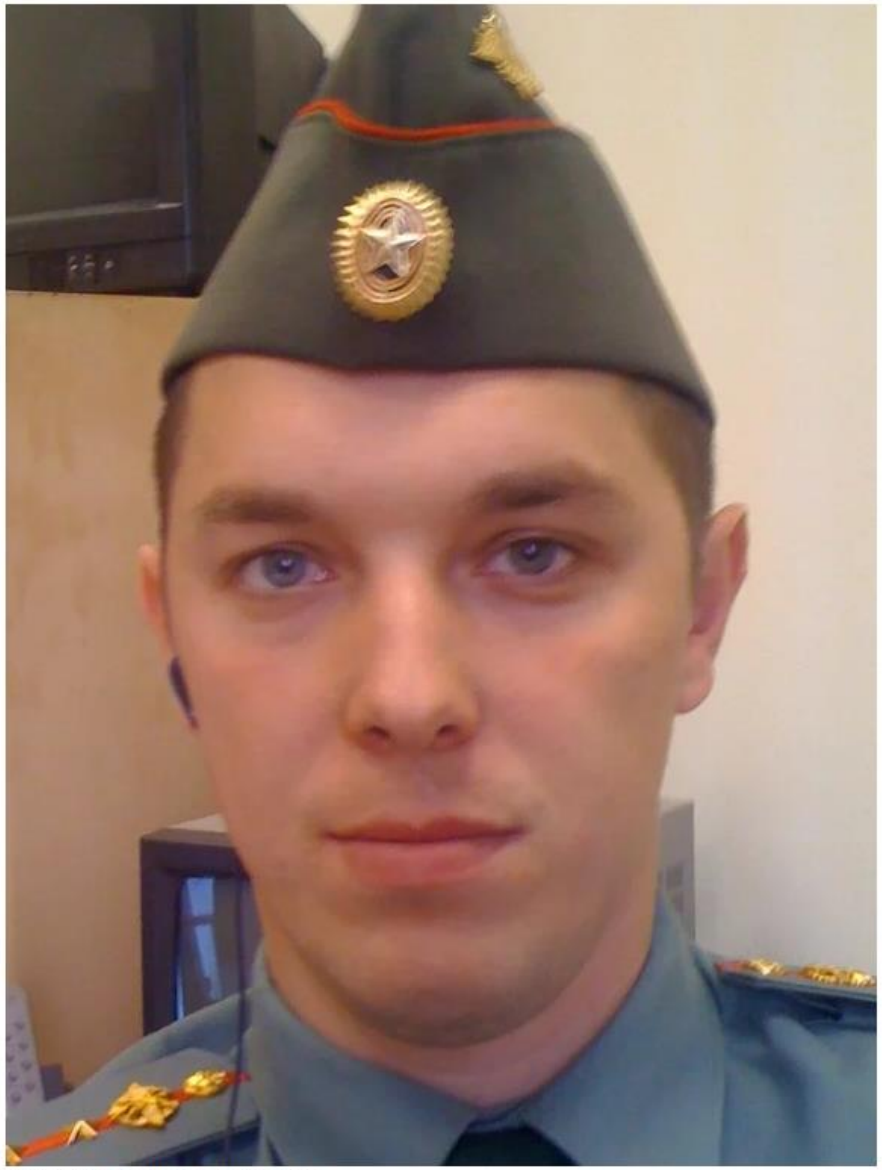
Aleksandr Vladimirovich Osadchuk

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

Aleksey Potemkin

- Head of Department 1
- Department 1 was dedicated to the administration of computer infrastructure that was both used in cyber operations, and in the release of stolen documents



Aleksey Aleksandrovich Potemkin

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

Anatoliy Kovalev

- Member of Unit 74455
- The indictment does not specify that he worked in Potemkin's department
- Kovalev researched domains used by U.S. state boards of elections, secretaries of state, and other election-related entities for website vulnerabilities
- Searched for state political party email addresses
- Hacked the website of a state board of elections and stole information related to approximately 500,000 voters
- Kovalev hacked into the computers of a U.S. vendor that provides election management software and electronic poll books to several U.S. states

Anatoliy Sergeyevich Kovalev

https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

ARACHNE

GRU structure

- Indictment talks about departments within both units but does not name them
- For this presentation, they will be referred to as Department A and Department B of Unit 26165 and Department 1 of Unit 74455

Unit 26165 APT 28/Fancy Bear

- Department A - targeting organisations with spearphishing emails and other computer intrusion activity
- Department B - developing and managing malware, including X-Agent

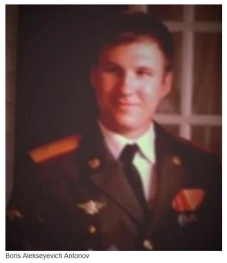
Unit 74455 Main Center for Special Technologies (GTsST)/Sandworm

- Department 1 - administration of computer infrastructure that was both used in cyber operations, and in the release of stolen documents

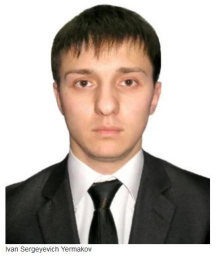
ARACHNE

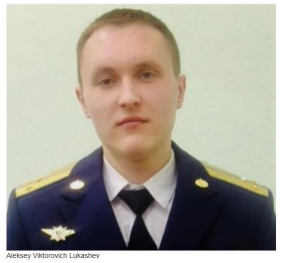
Unit 26165

Department A – Hacking and Phishing


Boris Alekseyevich Antonov

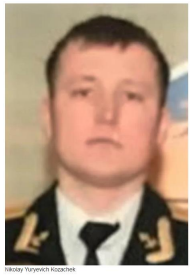

Dmitriy Sergeyevich Badin

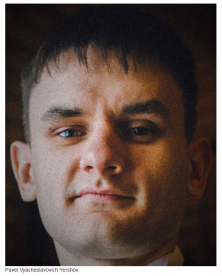

Ivan Sergeyevich Yermakov

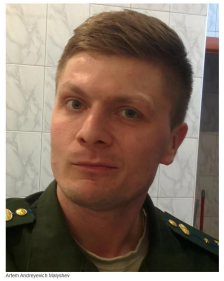

Aleksey Viktorovich Lukashev

Department B – Malware development and monitoring


Sergey Aleksandrovich Morgachev


Nikolay Yuryevich Kozachek

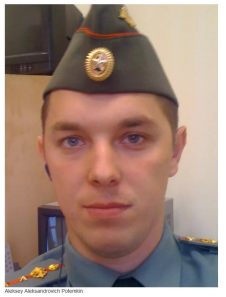

Pavel Vyacheslavovich Yershov


Artem Andreyevich Malyshev

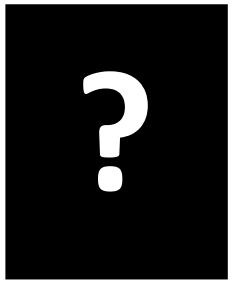
Unit 74455


Aleksandr Vladimirovich Osadchuk

Department 1 - Infrastructure


Aleksey Alekseyevich Polumtsn

??– Hacking and Phishing




Anatoliy Sergeyevich Kovalev

ARACHNE

Timeline of events outlined in *The United States v Viktor Borisovich Netyksho et al.*

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

2015

- Unit 26165 renewed the registration of the linuxkrnl.net domain that was encoded in the X-Agent malware
- They used Bitcoin, and used the same computers to make the transfer as perform the renewal, and send test phishing for later actions

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

Extra content

- between June and September 2015, Dutch intelligence informed U.S. counterparts of a separate hack of the DNC
- The U.S. State Department, the White House, and the DNC had already been hacked by a group referred to as APT29, or Cozy Bear
- Attributed to the Foreign Intelligence Service of the Russian Federation, the SVR RF
- APT29 was already in the DNC network when the GRU hacked the DNC
- It is believed that APT29 stayed in the DNC network until they were evicted along with their GRU counterparts in roughly October of 2016

ARACHNE

February 1, 2016

- An account called gfadel47 received the instruction to “[p]lease send exactly 0.026043 bitcoin to” a certain thirty-four character Bitcoin address
- Shortly thereafter, a transaction matching those exact instructions was added to the Blockchain

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

March 14, 2016

- Using funds in a Bitcoin address, members of Unit 74455 purchased a VPN account later used to log into the @Guccifer_2 Twitter account
- Some funds left over

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

March 15, 2016

- Yermakov ran a technical query for the DNC's internet protocol configurations to identify connected devices.
- Yermakov searched for open-source information about the DNC network, the Democratic Party, and Hillary Clinton.

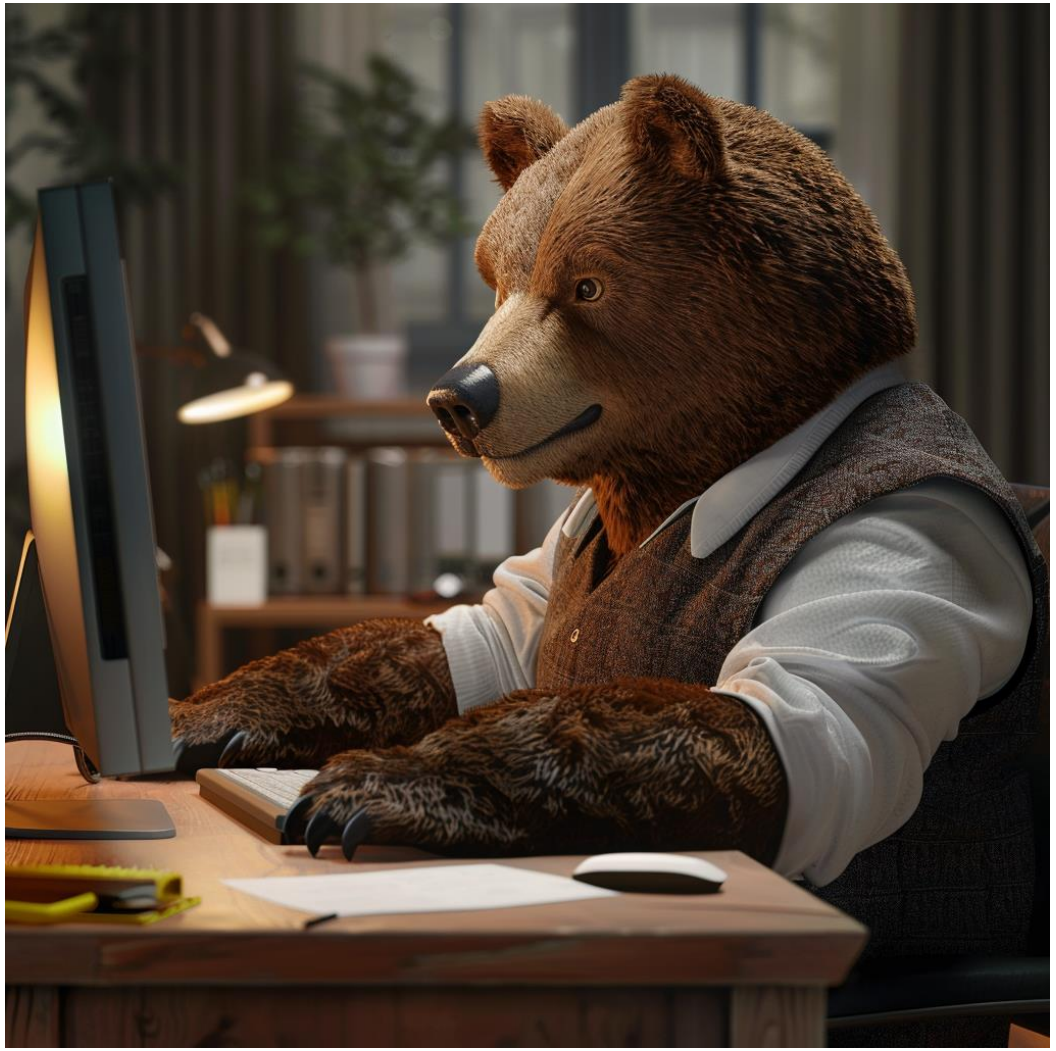
ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

March 19, 2016

- Lukashev and members of Department A of Unit 26165 created and sent a spearphishing emails to the personal accounts of people related to the Clinton campaign, including of the chairman of the Clinton Campaign and a senior foreign policy advisor.
- Lukashev used the account “john356gh” registered with a URL-shortening service.
- Lukashev used the account to mask a link contained in the spearphishing email, which directed the recipient to a GRU-created website.
- Lukashev altered the appearance of the sender email address to make it look like the email was a security notification from Google, instructing the users to change their password by clicking the embedded link.



ARACHNE

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Election Nov16	Dec16	2017

March 21, 2016

- Lukashev, Yermakov, and members of Department A of Unit 26165 stole the contents of the chairman's email account, which consisted of over 50,000 emails.
- Victim 3 had the username and password to their personal email account compromised.
- The names of the victims who had accounts compromised are not revealed in the court documents

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

March 25, 2016

- Lukashev used the john356gh account for the URL shortener service seen earlier to mask additional links included in spearphishing emails sent to numerous individuals affiliated with the Clinton Campaign, including Victims 1 and 2
- Lukashev sent these emails from the Russia-based email account hi.mymail@yandex.com that he spoofed to appear to be from Google
- Victim 1 had the username and password to their personal email account compromised
- Emails from Victim 1 are given to a reporter later on June 27

ARACHNE

March 28, 2016

- Yermakov researched the names of Victims 1 and 2 and their association with Clinton on various social media sites.
- Unit 26165 and Unit 74455 began to plan the release of materials stolen from the Clinton Campaign, DCCC, and DNC.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

April 6, 2016

- Department A of Unit 26165 created an email account in the name (with a one-letter deviation from the actual spelling) of a known member of the Clinton Campaign.
- They then used that account to send spearphishing emails to the work accounts of more than thirty different Clinton Campaign employees.
- In the spearphishing emails, Lukashev and members of Department A of Unit 26165 embedded a link purporting to direct the recipient to a document titled “hillary-clinton-favorable-rating.xlsx.”
- This link directed the recipients’ computers to a GRU-created website that harvested credentials. One of these emails was received by DCCC Employee 1 who input her credentials into the credential harvesting form somewhere between April 6 and April 12.

ARACHNE

April 7, 2016

- Yermakov ran a technical query for the DCCC's internet protocol configurations to identify connected devices.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

April 12, 2016

- Department A used the stolen credentials of DCCC Employee 1 to access the DCCC network.
- They installed and managed different types of malware to explore the DCCC network and steal data. Among them is the X-Agent malware.
- Malyshev and members of Department B of Unit 26165 monitored the X-Agent malware from the AMS (admin management system) panel and captured data from the victim computers.
- The AMS panel collected thousands of keylog and screenshot results from the DCCC and DNC computers, such as a screenshot and keystroke capture of DCCC Employee 2 viewing the DCCC's online banking information.
- Victim 4 also had the username and password to their account for the DCCC network compromised.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

April 14, 2016

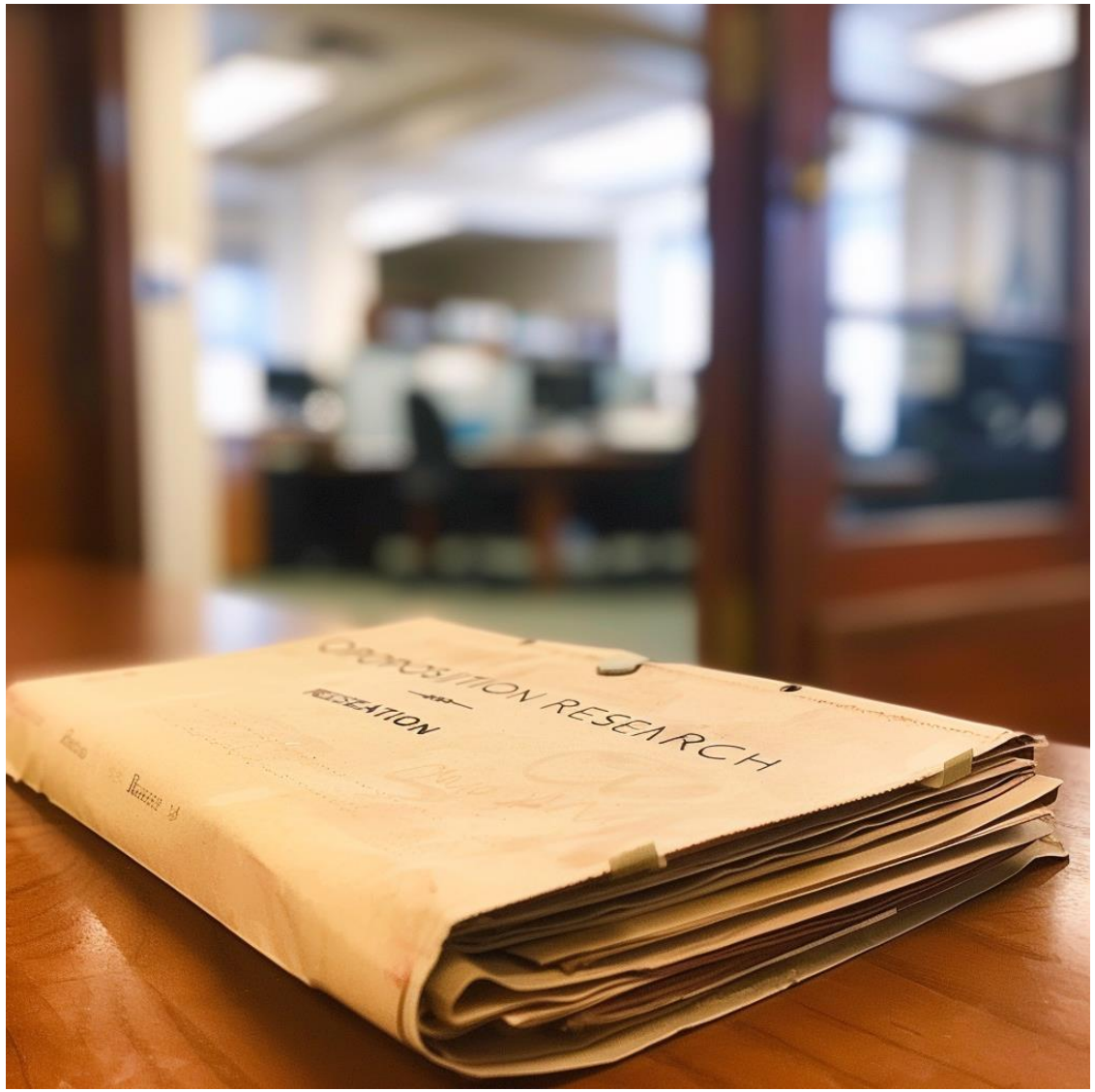
- Department B of Unit 26165 repeatedly activated X-Agent's keylog and screenshot functions to surveil DCCC Employee 1's computer activity over the course of eight hours.
- Department B captured DCCC Employee 1's communications with co-workers and the passwords she entered while working on fundraising and voter outreach projects.

ARACHNE

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Election Nov16	Dec16	2017

April 15, 2016

- Unit 26165 searched one hacked DCCC computer for terms that included “hillary,” “cruz,” and “trump.”
- Unit 26165 copied select DCCC folders, including “Benghazi Investigations.”
- Unit 26165 targeted computers containing information such as opposition research and field operation plans for the 2016 elections.
- Victim 5 had the username and password to their account for the DCCC network compromised.



ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

April 18, 2016

- Department B of Unit 26165 activated X-Agent's keylog and screenshot functions to steal credentials of a DCCC employee who was authorized to access the DNC network.
- Unit 26165 hacked into the DNC network from the DCCC network using stolen credentials.
- Unit 26165 installed and managed different types of malware to explore the DNC network and steal documents.
- Victim 6 had the username and password to their account for the DCCC network compromised.

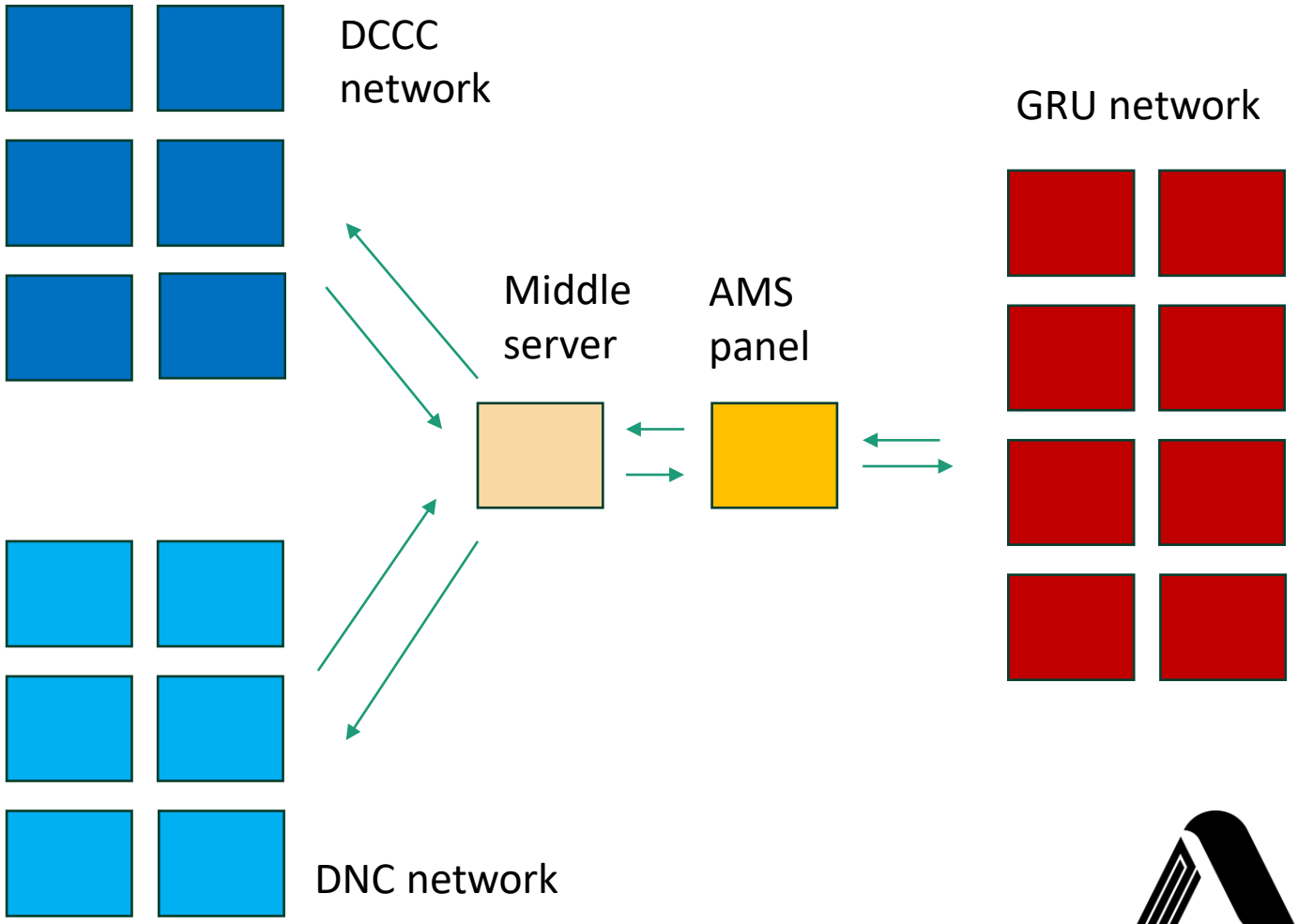
ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

April 19, 2016

- Kozacheck, Yershov, and members of Department B of Unit 26165 remotely configured an overseas computer to relay communications between X-Agent malware and the AMS panel.
- Unit 26165 referred to this computer as a "middle server."
- The middle server acted as a proxy to obscure the connection between malware and the AMS panel.



ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

April 19, 2016

- After attempting to register the domain electionleaks.com, Unit 74455 registered the domain dcleaks.com through a service that anonymized the registrant
- The funds used to pay for the dcleaks.com domain originated from an account at an online cryptocurrency service that Unit 26165 and Unit 74455 also used to fund the lease of a virtual private server registered with the operational email account dirbinsaabol@mail.com
- The dirbinsaabol email account was also used to register the john356gh URL-shortening account seen earlier that was used by Lukashev

https://slate.com/news-and-politics/2016/08/russian-hackers-tried-dc-leaks-site-for-emails-before-wikileaks.html

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

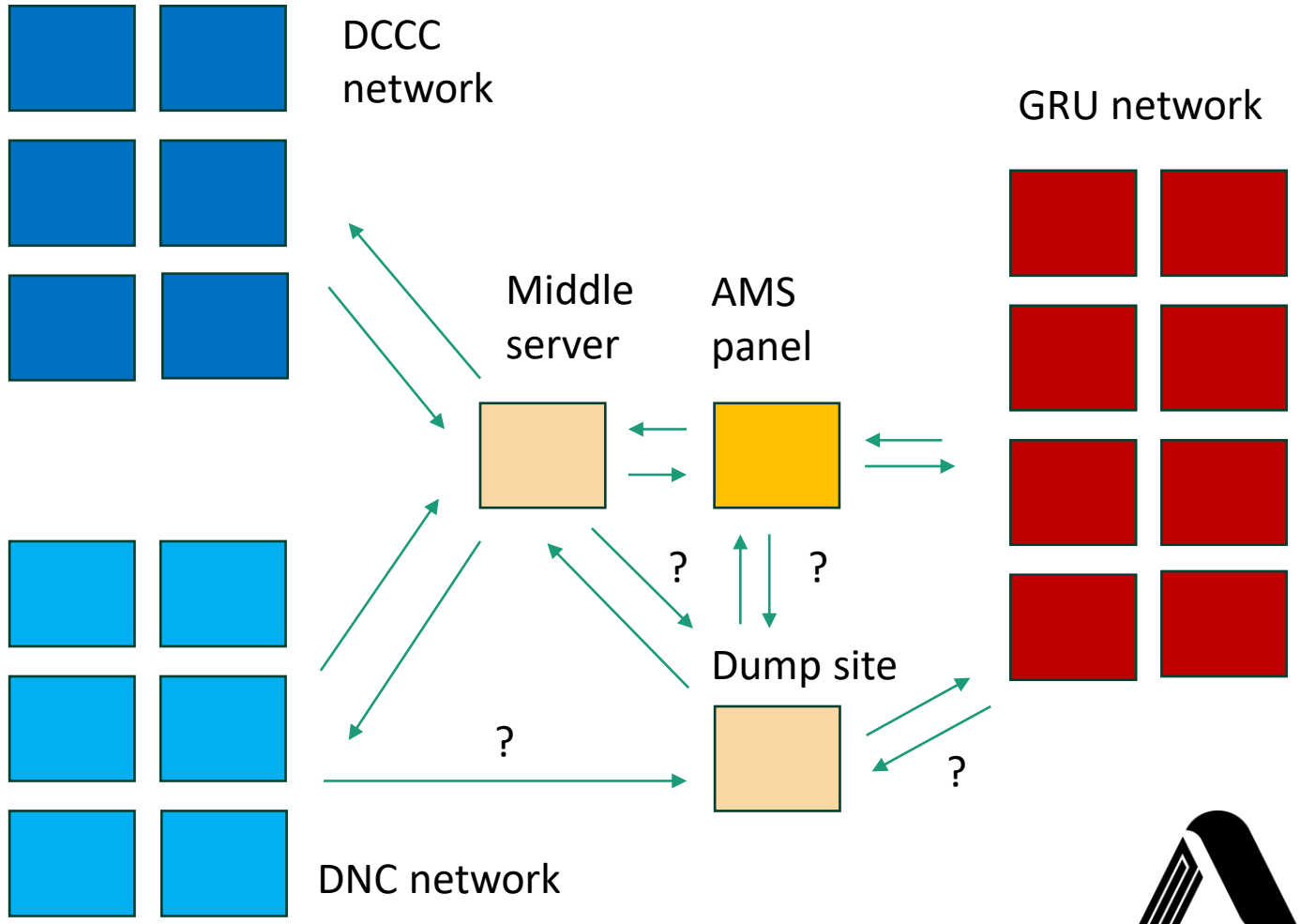
April 20, 2016

- Department B of Unit 26165 directed X-Agent malware on the DCCC computers to connect to the middle server and receive directions.

ARACHNE

April 22, 2016

- Department B activated X-Agent's keylog and screenshot functions to capture the discussions of DCCC Employee 2 about the DCCC's finances, as well as her individual banking information and other personal topics.
- Unit 26165 compressed gigabytes of data from DNC computers, including opposition research.
- Unit 26165 later moved the compressed DNC data using X-Tunnel to a GRU-leased computer located in Illinois.

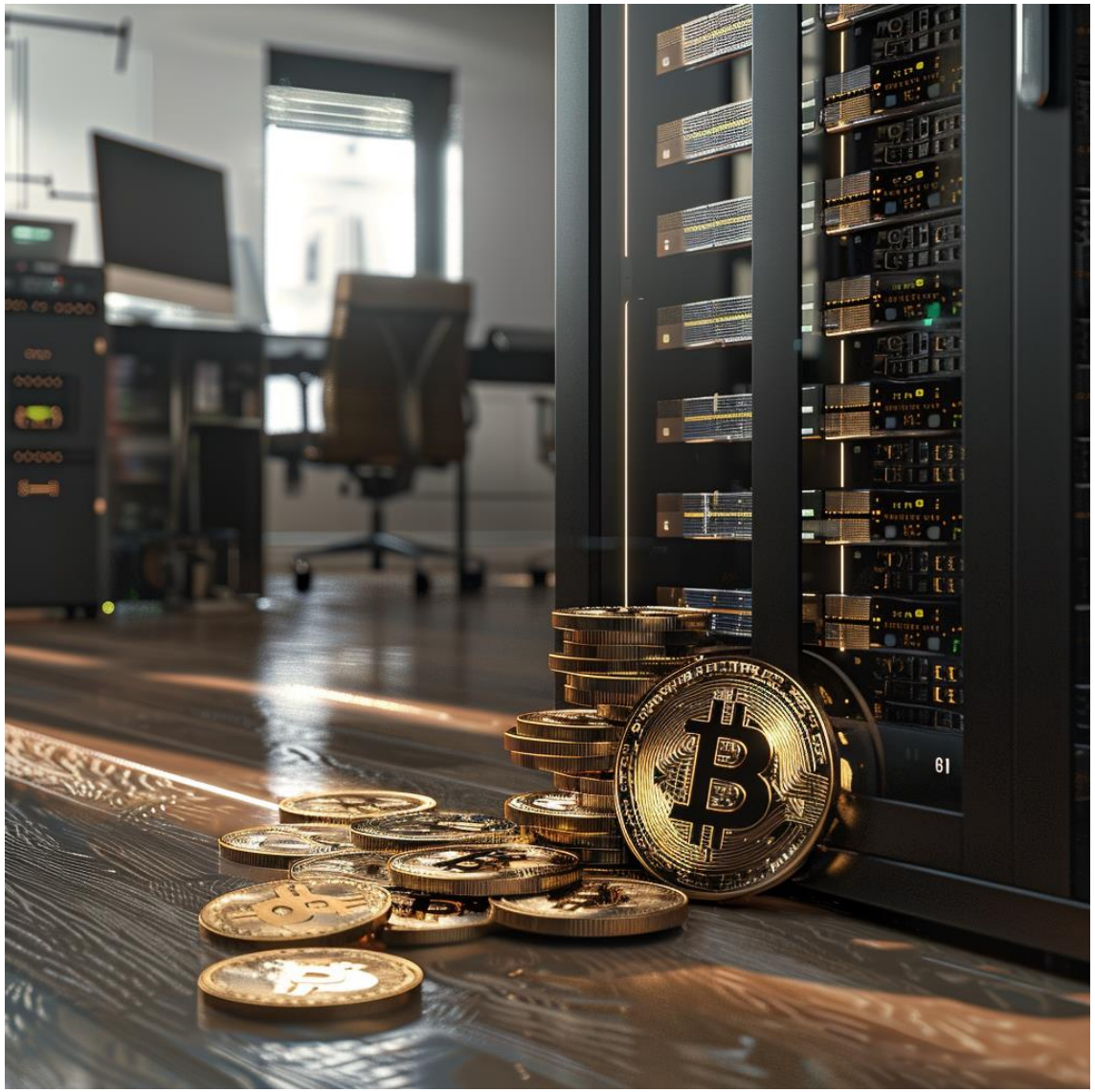


ARACHNE

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Election Nov16	Dec16	2017

April 28, 2016

- Department B connected to and tested the computer located in Illinois.
- Department B used X-Tunnel to steal additional documents from the DCCC network.
- The remaining funds from the Bitcoin address that was used to purchase the VPN account back in March were used to lease a Malaysian server that hosted the dcleaks.com website.



ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

May ??, 2016

- The DCCC and DNC became aware that they had been hacked and hired a security company (“Company 1/CrowdStrike”)

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

May 10, 2016

- Victim 7 had the username and password to their account for the DNC network compromised.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

May 13, 2016

- Unit 26165 cleared the event logs from a DNC computer to hamper the CrowdStrike's investigation.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

May 25, 2016

- From now until June 1, Unit 26165 hacked the DNC Microsoft Exchange Server and stole thousands of emails from the work accounts of DNC employees.
- Yermakov researched PowerShell commands related to accessing and managing the Microsoft Exchange Server.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

May 30, 2016

- Malyshev accessed the AMS panel that connected to X-Agent to upgrade custom AMS software on the server.
- The AMS panel received updates from approximately thirteen different X-Agent malware implants on DCCC and DNC computers.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

May 31, 2016

- Yermakov searched for open-source information about CrowdStrike and its reporting on X-Agent and X-Tunnel

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

June ??, 2016

- Kovalev and members of Unit 74455 researched domains used by U.S. state boards of elections, secretaries of state, and other election-related entities for website vulnerabilities.
- They searched for state political party email addresses, including filtered queries for email addresses listed on state Republican Party websites.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

June 1, 2016

- Unit 26165 attempted to delete traces of their presence on the DCCC network using the computer program CCleaner

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

June 2, 2016

- Victim 2 had the username and password to their personal email account compromised.

ARACHNE

June 8, 2016

- Unit 74455 used the Malaysian server they leased to launch the public website dcleaks.com
- Unit 74455 falsely claimed on the site that DCLeaks was started by a group of “American hacktivists”
- Unit 74455 created a DCLeaks Facebook page using an account under the name “Alice Donovan”
- Unit 74455 used other social media accounts in the names of fictitious U.S. persons such as “Jason Scott” and “Richard Gingrey” to promote the DCLeaks website

https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

ARACHNE

Still June 8, 2016

- Unit 74455 created the Twitter account @dcleaks_
- Unit 74455 created @BaltimoreIsWhr, through which they encouraged U.S. audiences to “[j]oin our flash mob” opposing Clinton and to post images with the hashtag #BlacksAgainstHillary
- Unit 74455 accessed all these accounts from computers managed by Department 1, lead by Potemkin

https://medium.com/dfrlab/trolltracker-russias-other-troll-team-4efd2f73f9b5

ARACHNE

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Election Nov16	Dec16	2017

June 14, 2016

- The DNC—through CrowdStrike—publicly announced that it had been hacked by Russian government actors
- Unit 26165 and Unit 74455 registered the domain actblues.com, which mimicked the domain of a political fundraising platform that included a DCCC donations page
- The real site is actblue.com
- Unit 26165 and Unit 74455 used stolen DCCC credentials to modify the DCCC website and redirect visitors to the actblues.com domain

https://secure.actblue.com/

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

June 15, 2016

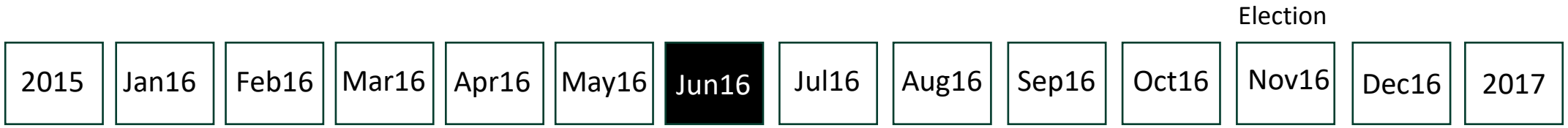
- A member or members of Unit 74455 logged into a Moscow-based server and, between 4:19 PM and 4:56 PM Moscow Standard Time, searched for certain words and phrases, including:
  - “some hundred sheets”
  - “some hundreds of sheets”
  - dcleaks
  - illuminati
  - широко известный перевод [widely known translation]
  - “worldwide known”
  - “think twice about”
  - “company’s competence”

ARACHNE

Still June 15, 2016

- 7:02 PM Moscow Standard Time, the online persona Guccifer 2.0 published its first post on a blog site created through WordPress.
- Entitled “DNC’s servers hacked by a lone hacker,” the post used numerous English words and phrases that Unit 74455 had searched for earlier that day
- Guccifer 2.0 claims to be a lone wolf hacker from Romania, not Russian and not a team of intelligence operatives

ARACHNE



Worldwide known cyber security company Crowdstrike 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 Crowdstrike’s customers should **think twice** about **company’s competence**.

Fuck the **Illuminati** and their conspiracies!!!!!!!!! Fuck Crowdstrike!!!!!!!!!

[Emphasis added]

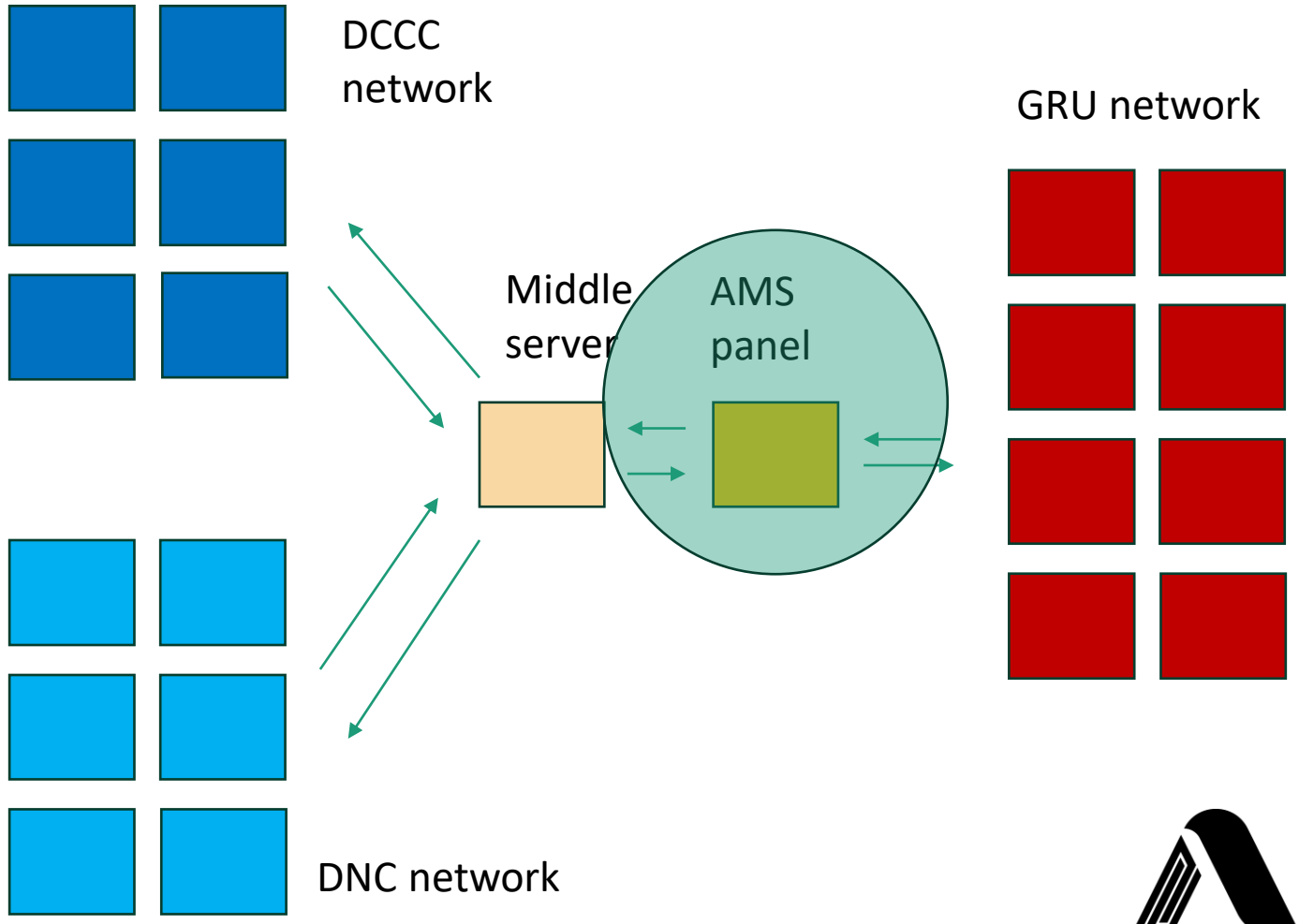
ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

June 20, 2016

- After CrowdStrike disabled X-Agent on the DCCC network Unit 26165 spent over seven hours trying to connect to X-Agent. Unit 26165 also tried to access the DCCC network using previously stolen credentials
- Despite these efforts, Unit 26165 gained access to approximately thirty-three DNC computers, and a Linux-based version of X-Agent, programmed to communicate with the GRU-registered domain linuxkrnl.net, remained on the DNC network until in or around October 2016
- Unit 26165 deleted logs from the AMS panel that documented their activities on the panel, including the login history.



ARACHNE

June 22, 2016

- Wikileaks, referred to as Organisation 1 in the indictment, sent a private message to Guccifer 2.0 to "[s]end any new material [stolen from the DNC] here for us to review and it will have a much higher impact than what you are doing."

https://wikileaks.org/

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

June 27, 2016

- Unit 74455, posing as Guccifer 2.0, contacted a U.S. reporter with an offer to provide stolen emails from “Hillary Clinton’s staff.”
- Unit 74455 then sent the reporter the password to access a nonpublic, password-protected portion of dcleaks.com containing emails stolen from Victim 1 by Lukashev, Yermakov, and members of Unit 26165 in or around March 2016.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

July ??, 2016

- Kovalev and members of Unit 74455 hacked the website of SBOE 1, believed to be the Illinois State Board of Elections.
- They stole information related to approximately 500,000 voters, including names, addresses, partial social security numbers, dates of birth, and driver's license numbers.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

July 6, 2016

- Wikileaks added, “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.” Unit 74455 responded, “ok . . . i see.” Wikileaks explained, “we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting.”
- Victim 8 had the username and password to personal email account compromised.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

July 14, 2016

- Unit 74455, posing as Guccifer 2.0, sent Wikileaks an email with an attachment titled “wk dnc link1.txt.gpg.”
- Unit 74455 explained to Wikileaks that the encrypted file contained instructions on how to access an online archive of stolen DNC documents.

ARACHNE

July 18, 2016

- Wikileaks confirmed it had “the 1Gb or so archive” and would make a release of the stolen documents “this week.”

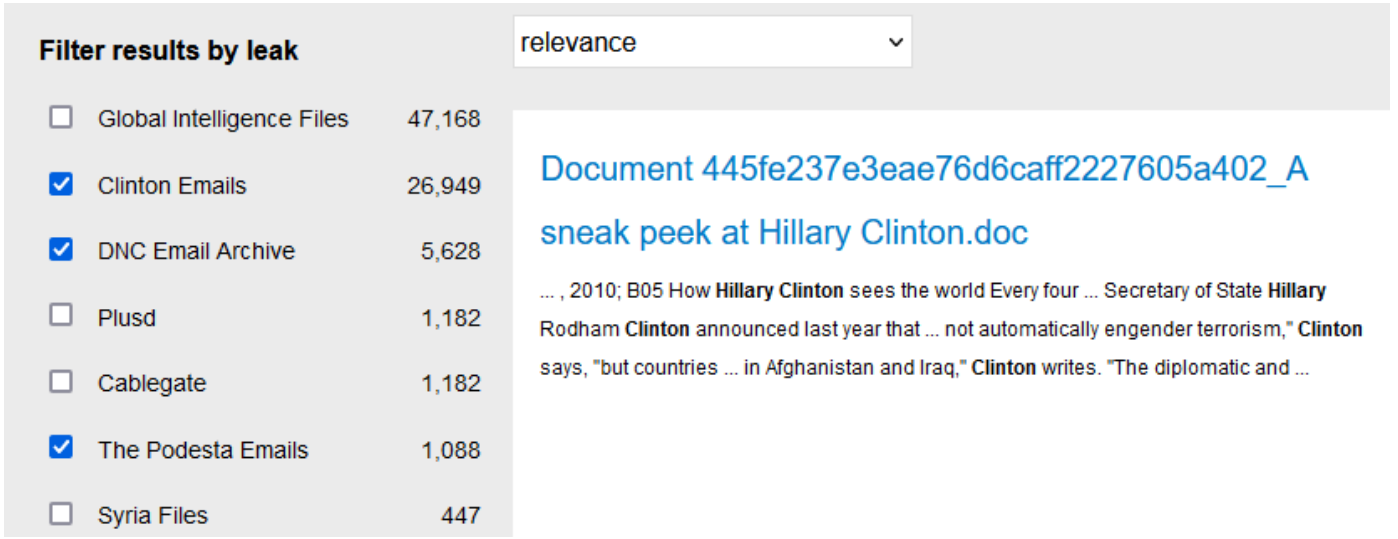
ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

July 22, 2016

- Wikileaks released over 20,000 emails and other documents stolen from the DNC network.
- This release occurred approximately three days before the start of the Democratic National Convention.
- Wikileaks did not disclose Guccifer 2.0's role in providing them.
- The latest-in-time email released through Wikileaks was dated on or about May 25, 2016, approximately the same day Unit 26165 hacked the DNC Microsoft Exchange Server.



https://search.wikileaks.org

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

July 27, 2016

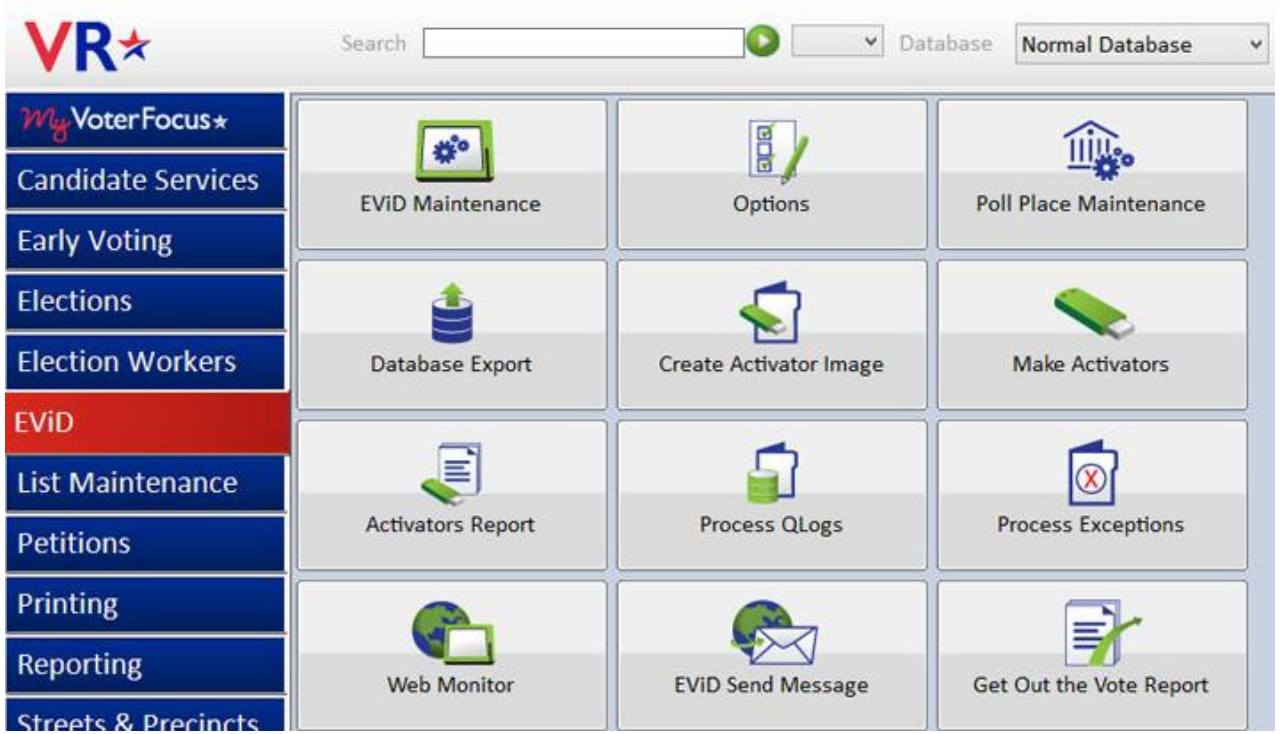
- Unit 26165 attempted after hours to spearphish for the first time email accounts at a domain hosted by a third-party provider and used by Clinton's personal office.
- At or around the same time, they also targeted seventy-six email addresses at the domain for the Clinton Campaign.

ARACHNE

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017
											Election		

August ??, 2016

- Kovalev and members of Unit 74455 hacked into the computers of Vendor 1, believed to be VR Systems
- VR Systems supplied software used to verify voter registration information for the 2016 U.S. elections.
- They used some of the same infrastructure to hack into VR Systems that they had used to hack into the Illinois State Board of Elections.



https://www.vrsystems.com

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

August 15, 2016

- Unit 74455, posing as Guccifer 2.0, received a request for stolen documents from a candidate for the U.S. Congress.
- Unit 74455 responded using the Guccifer 2.0 persona and sent the candidate stolen documents related to the candidate's opponent.
- Unit 74455, posing as Guccifer 2.0, wrote to a person 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?" It is presumed that Unit 74455 was writing to Roger Stone.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

August 17, 2016

- Unit 74455 added, “please tell me if i can help u anyhow . . . it would be a great pleasure to me.”

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

August 22, 2016

- Unit 74455, posing as Guccifer 2.0, transferred approximately 2.5 gigabytes of data stolen from the DCCC to a then-registered state lobbyist and online source of political news.
- The stolen data included donor records and personal identifying information for more than 2,000 Democratic donors.
- This information matches that published by Aaron Nevins, a political consultant who published information purportedly obtained from the DCCC.
- They also sent a reporter stolen documents pertaining to the Black Lives Matter movement. The reporter responded by discussing when to release the documents and offering to write an article about their release.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

September ??, 2016

- Unit 26165 successfully gained access to DNC computers hosted on a third-party cloud-computing service.
- These computers contained test applications related to the DNC's analytics.
- After conducting reconnaissance, Unit 26165 gathered data by creating backups, or "snapshots," of the DNC's cloud-based systems using the cloud provider's own technology.
- Unit 26165 then moved the snapshots to cloud-based accounts they had registered with the same service, thereby stealing the data from the DNC.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

September 9, 2016

- Unit 74455, again posing as Guccifer 2.0, referred to a stolen DCCC document posted online and asked the person that is believed to be Roger Stone, “what do u think of the info on the turnout model for the democrats entire presidential campaign.”
- The person responded, “[p]retty standard.”

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

October??, 2016

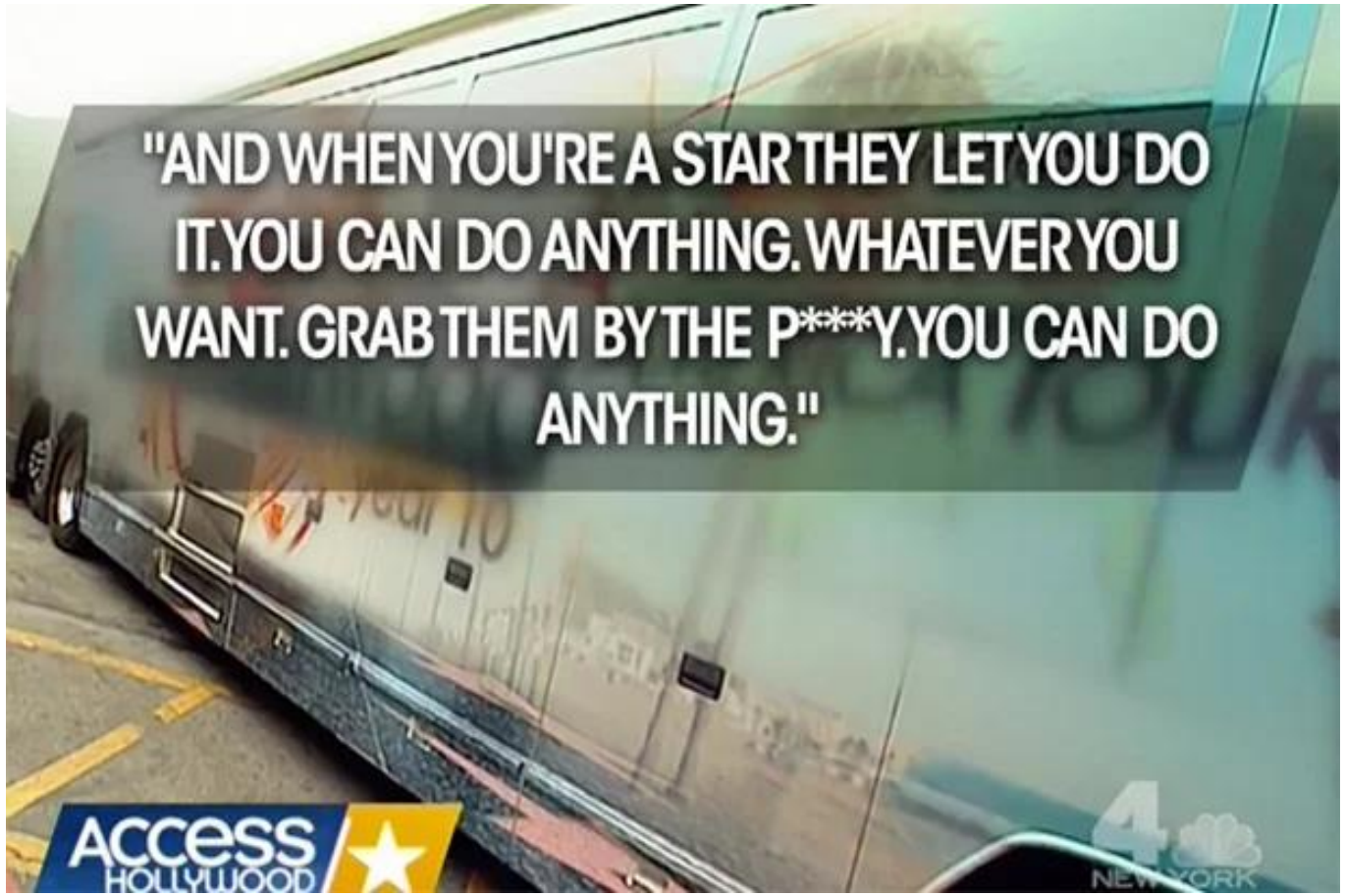
- Unit 26165 is successfully evicted from the DNC network
- Unknown about DCCC network but likely evicted from there as well if not evicted earlier
- X-Agent was removed from the DCCC network June 20
- Given the DCCC and the DNC have staff that have access to both networks and accounts continue to be compromised it is unknown if Unit 26165 was able to re-enter the DCCC network after June 20

ARACHNE

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017
											Election		

October 7, 2016

- Wikileaks released the first set of emails from the chairman of the Clinton Campaign that had been stolen by Lukashev and Unit 26165
- In total, over 50,000 stolen documents were released
- The same day as the Access Hollywood tape was published by *The Washington Post*
- This continued until November 7
- The election is November 8



https://www.thewrap.com/how-access-hollywood-found-the-trump-tape-and-why-nbc-news-probably-leaked-it-exclusive/

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

October 28, 2016

- Kovalev and members of Unit 74455 visited the websites of certain counties in Georgia, Iowa, and Florida to identify vulnerabilities.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

November ??, 2016

- Prior to November 8, Kovalev and members of Unit 74455 used an email account designed to look like a VR Systems email address to send over 100 spearphishing emails to organizations and personnel involved in administering elections in numerous Florida counties.
- The spearphishing emails contained malware that Unit 74455 embedded into Word documents bearing VR Systems logo.

ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	**Nov16**	Dec16	2017

November 8, 2016

- Election is held

ARACHNE

January 12, 2017

- Unit 74455 published a statement on the Guccifer 2.0 WordPress blog, claiming that the intrusions and release of stolen documents had “totally no relation to the Russian government.”

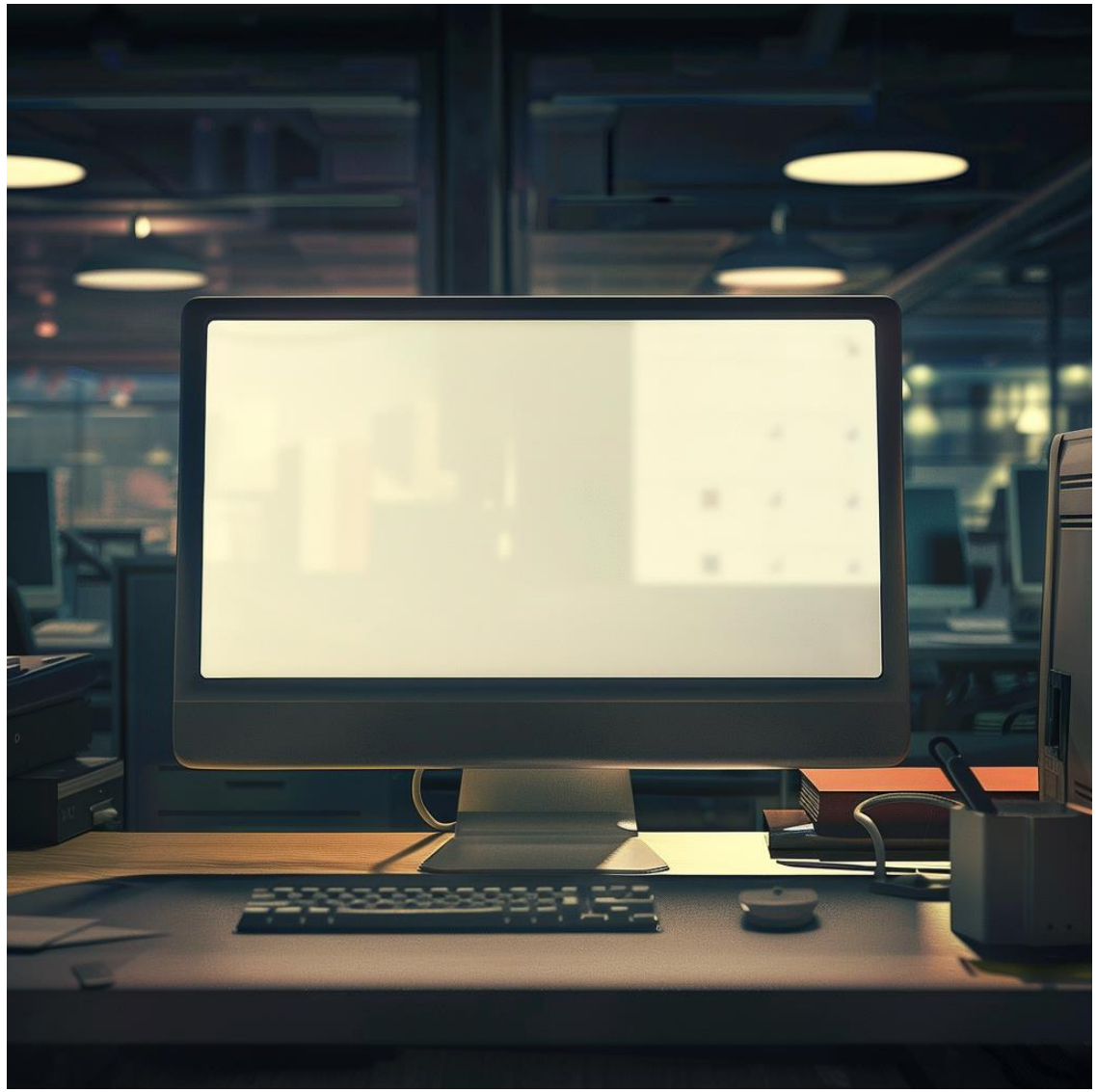
ARACHNE

Election

2015	Jan16	Feb16	Mar16	Apr16	May16	Jun16	Jul16	Aug16	Sep16	Oct16	Nov16	Dec16	2017

March ??, 2017

- DCLeaks shut down
- DCLeaks received over one million page views.



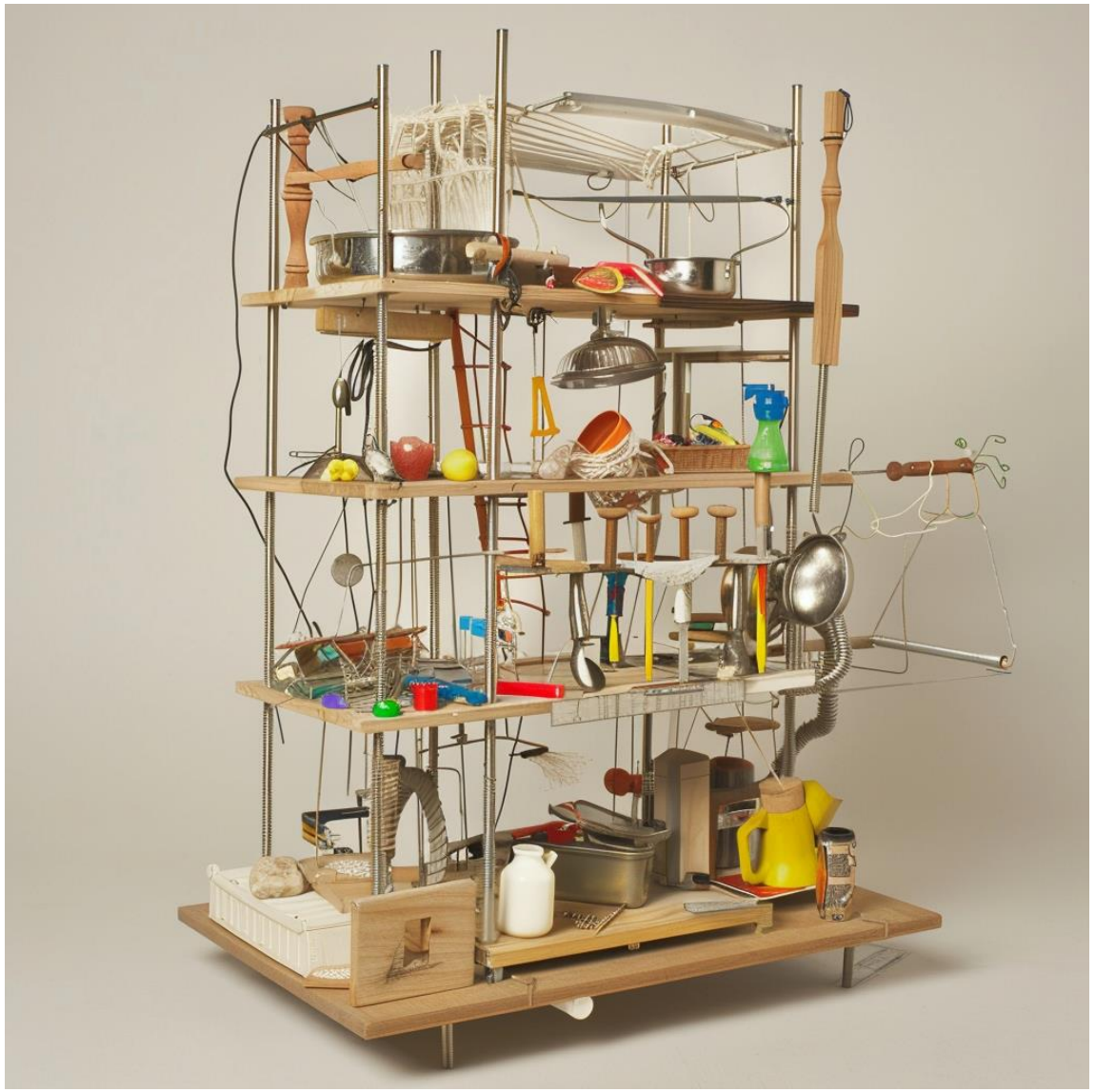
ARACHNE

What does all this mean?

Hacking

Low technical high operational sophistication

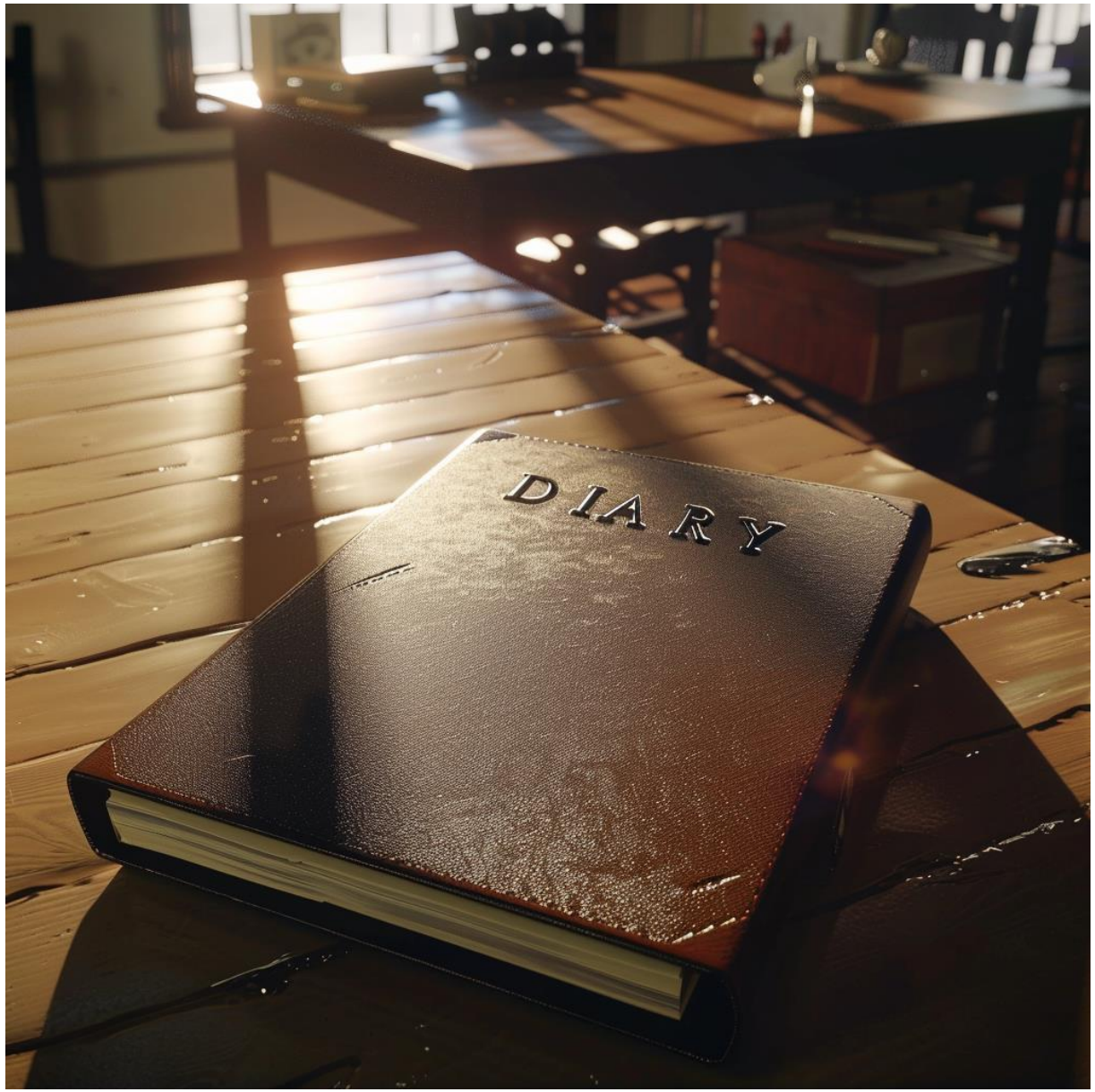
- Phishing for initial access, basic keylogger to capture credentials and moving laterally, and transferring files over a VPN with X-Tunnel
- Phishing never stopped
- Credentials continuously compromised through X-Agent
- On multiple machines at any one time, up to 13, accessed 33
- Moved from DCCC to DNC network
- Monitored CrowdStrike
- Deleted evidence on victim network and their own



ARACHNE

Things get personal

- Personal accounts compromised
- Threat actors will look you up on social media



ARACHNE

Attackers have bosses and budgets, too

- There are realities to being an adversary
- There is associated infrastructure to build and maintain, servers, domains, VPN accounts, social media accounts, credential harvesting and leak websites
- Purchases made in cryptocurrency
- They cleaned their own infrastructure, presumably preparing for it to be accessed by someone the GRU considers an adversary

ARACHNE

Phishing

- Address spoofing
- Registering an address one letter different
- Links in emails and in documents
- URL shorteners to hide the appearance of links
- Content “please change your password” or “please login to view the contents”

ARACHNE

Takeaway

- Do the basics well
- Never stop

ARACHNE

What does all this mean?

Disinformation

DISARM Framework

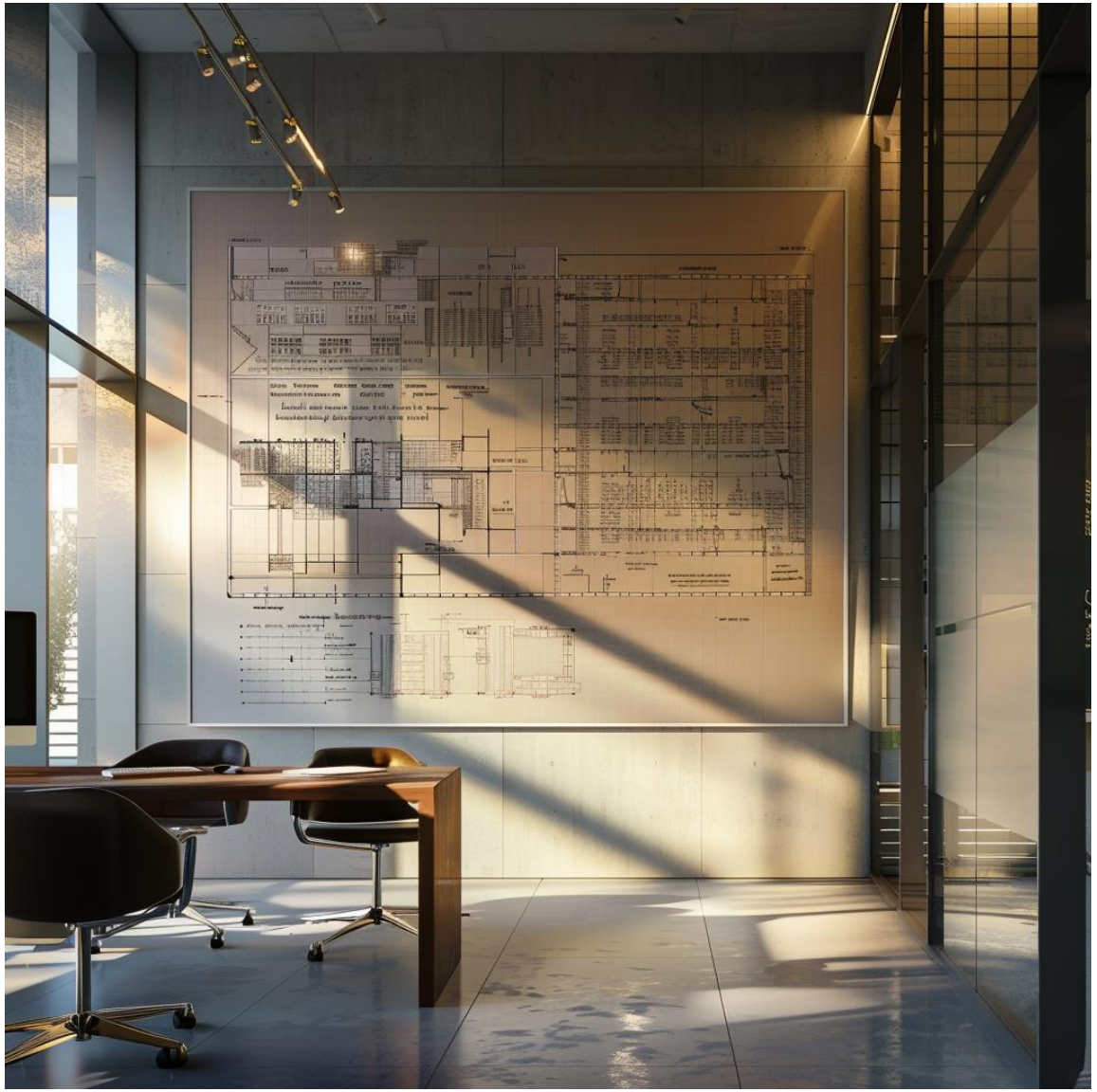
- The following points are mapped to the DISARM Framework
- https://disarmframework.herokuapp.com
- Not a comprehensive analysis

https://www.disarm.foundation/

ARACHNE

TA02 "Plan Objectives"

- T0066 "Degrade Adversary" – degrade Clinton
- T0076 "Distort" – Guccifer 2.0, Illuminati
- T0077 "Distract" – away from Trump, Hollywood Access tape, Benghazi, email server
- T0079 "Divide" – Create polarisation



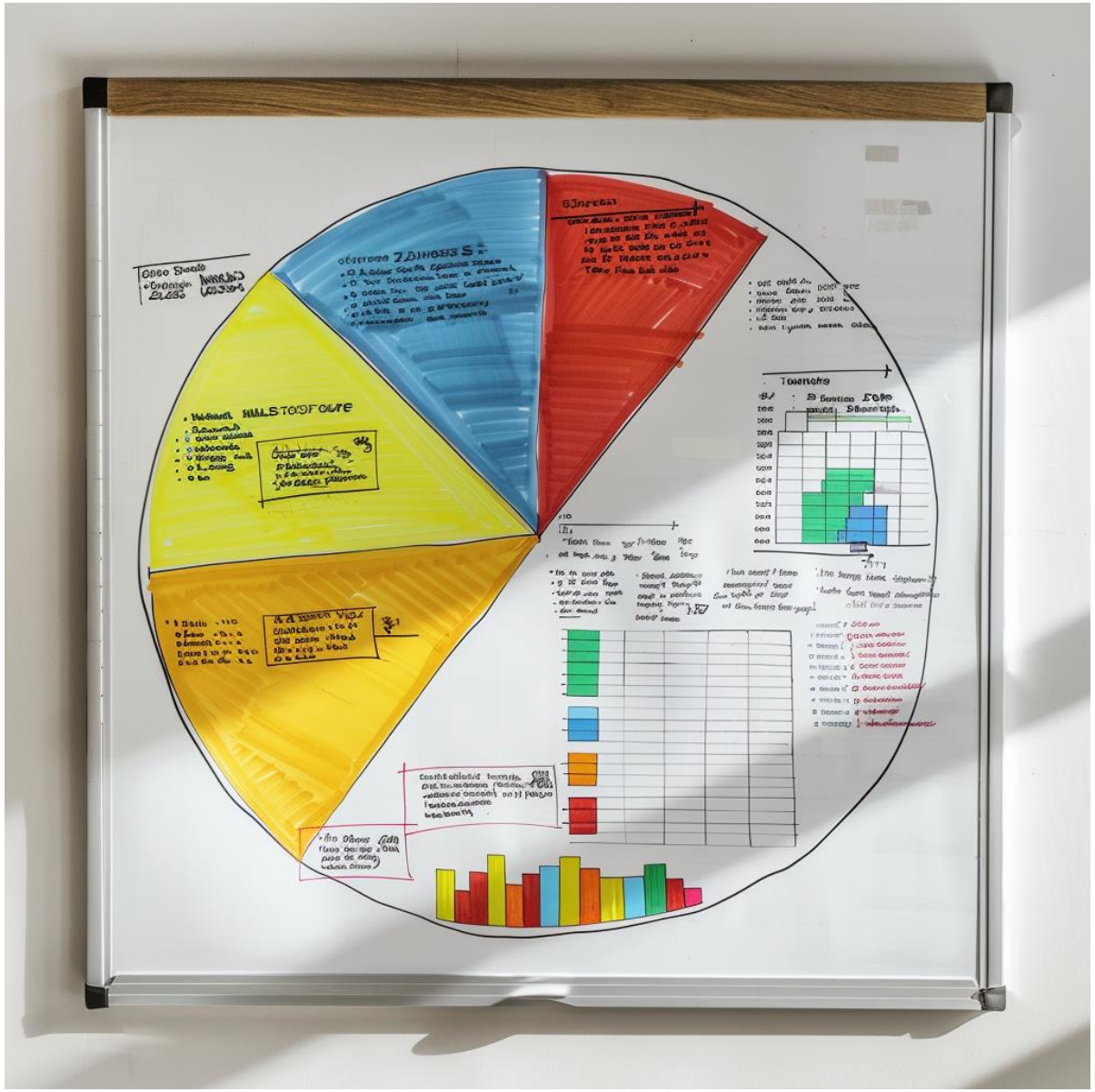
ARACHNE

Polarisation is a national security issue

ARACHNE

TA13 "Target Audience Analysis"

- T0072.001 "Geographic Segmentation" – Baltimore is Everywhere
- T0072.002 "Demographic Segmentation" – Blacks against Hillary
- T0072.005 "Political Segmentation" – democratic donor information to republican consultant
- Unit 74455 never gave all leaked material to any one person or group



ARACHNE

TA15 "Establish Social Assets"

- T0007 "Create Inauthentic Social Media Pages and Groups" – Facebook for American hacktivists
- T0010 "Cultivate ignorant agents" – journalists, WikiLeaks, Roger Stone, political consultant
- T0013 "Create inauthentic websites" – DCLeaks
- T0090.004 "Create Sockpuppet Accounts" – Guccifer 2.0

ARACHNE

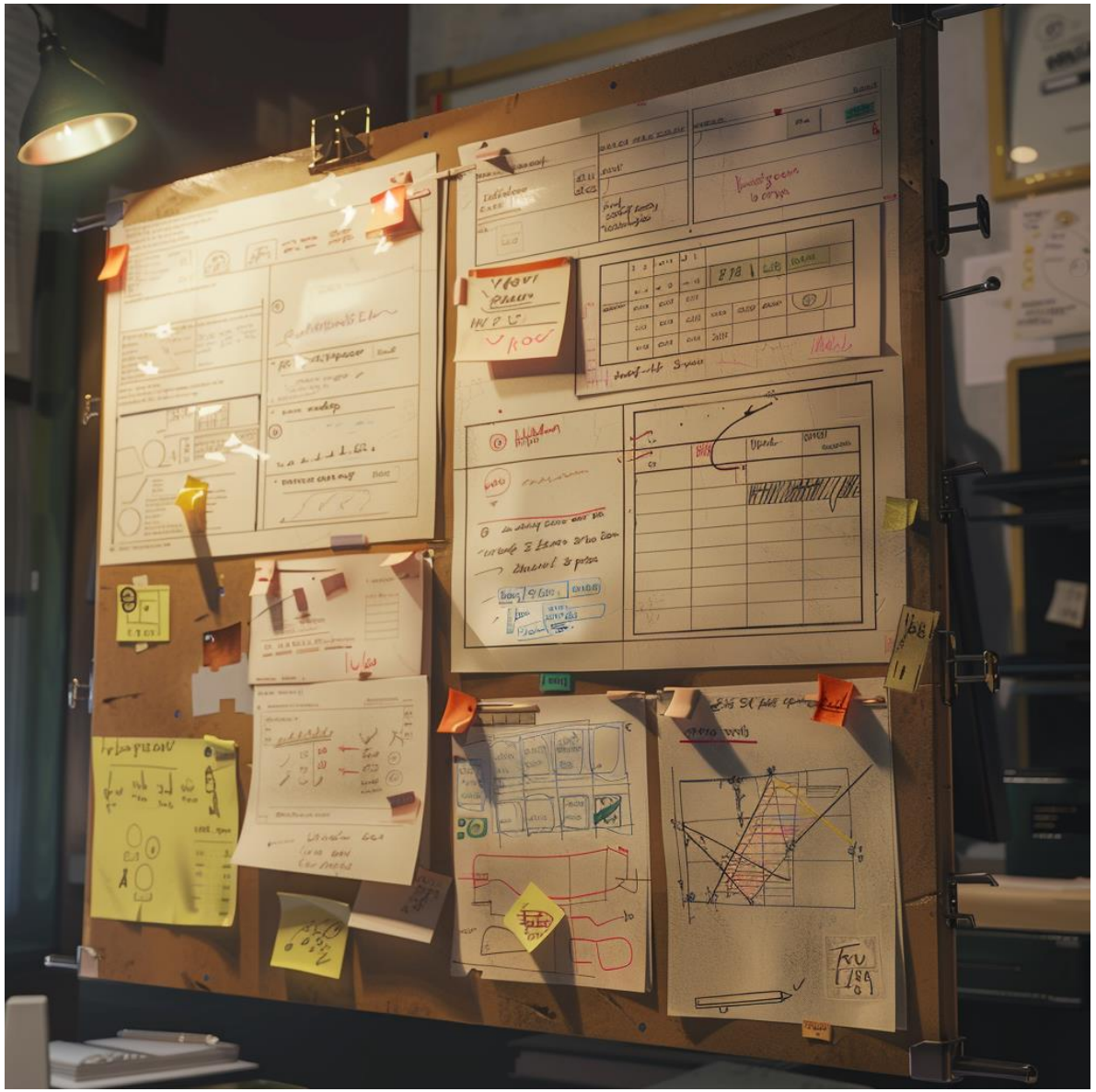
TA17 "Maximize Exposure"

- T0049 "Flooding the Information Space" – Release from Wikileaks from October onwards

ARACHNE

TA11 "Persist in the Information Environment"

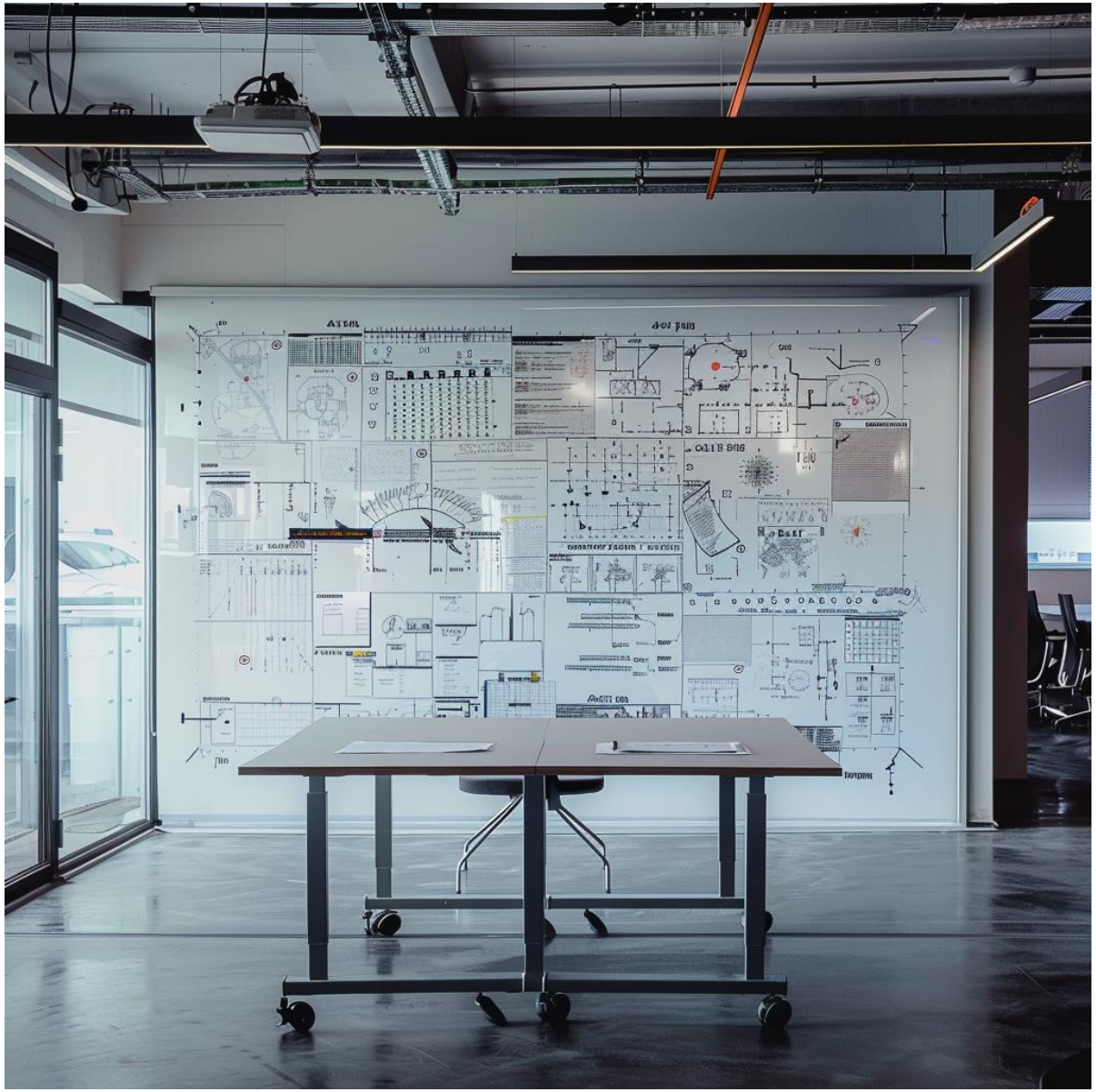
- T0059 "Play the long game" – leaking information all through the year and even after the election putting out statements
- T0129 "Conceal Operational Activity" – paying with Bitcoin, using VPNs



ARACHNE

Takeaway

- Low technical high operational sophistication
- There were constantly negative stories about Clinton in the information space
- The source of the negative stories to be obfuscated so the stories seemed legitimate
- This was by design



ARACHNE

Can’t say this decided the election, but…

- A foreign adversary was able to fuel the 24 hour news cycle for months to malign a candidate they didn’t like
- Issues dogged subsequent presidencies to this day
- Increased polarisation lowers the effectiveness of democracy
- Tools of statecraft for authoritarian regimes
- These tools are cheap
- If you do your basics well these tools are effective

ARACHNE

References

- https://www.justice.gov/file/1080281/download
- https://www.reuters.com/article/gabksworldNews/idUSTRE53N3K820090424
- https://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K
- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and
- https://www.justice.gov/opa/press-release/file/1328521/download
- https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/
- https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
- https://archive.ph/0RG40
- https://www.justice.gov/opa/press-release/file/1328521/download
- https://www.bbc.com/news/world-europe-56798001
- https://sgp.fas.org/crs/intel/R46616.pdf
- https://www.nprillinois.org/statehouse/2018-07-13/russia-indictments-likely-cover-illinois-hack-state-official-says
- https://theintercept.com/2018/07/13/a-swing-state-election-vendor-repeatedly-denied-being-hacked-by-russians-new-mueller-indictment-says-otherwise/
- https://www.wired.com/story/russian-hackers-attack-ukraine/
- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

- https://cybernews.com/news/us-election-hacker-viktor-netyksho-exposed/
- https://www.ft.com/content/3391bf8c-e431-415c-b7c5-9eeee08b3374
- https://www.bellingcat.com/news/2020/05/05/who-is-dmitry-badin-the-gru-hacker-indicted-by-germany-over-the-bundestag-hacks/
- https://www.zdnet.com/article/german-authorities-charge-russian-hacker-for-2015-bundestag-hack/
- https://nsarchive.gwu.edu/document/17596-united-states-v-alexei-sergeyevich-morenets-et
- https://informnapalm.org/en/hacked-russian-gru-officer/
- https://www.justice.gov/d9/press-releases/attachments/2020/10/19/2020_10_19_unsealed_indictment_0.pdf
- https://www.wired.com/story/russia-gru-sandworm-serebriakov/
- https://www.wired.co.uk/article/dnc-hack-proof-russia-democrats
- https://nos.nl/nieuwsuur/artikel/2213767-dutch-intelligence-first-to-alert-u-s-about-russian-hack-of-democratic-party
- https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a
- https://www.marshallcenter.org/en/publications/security-insights/intelligence-and-security-services-and-strategic-decision-making-0
- https://www.bbc.com/news/world-us-canada-46378863
- https://www.cbsnews.com/news/the-russian-hack-60-minutes-freedom-of-information-request-to-reveal-candidate-denied-by-doj-2020-08-23/
- https://www.nbcnews.com/politics/first-read/how-team-trump-capitalized-russia-s-interference-2016-n891661
- https://www.reuters.com/article/us-usa-trump-russia-indictments-idUSKBN1K32DJ
- https://www.sun-sentinel.com/2018/07/16/who-is-aaron-nevins/
- https://attack.mitre.org/software/S0023/

kade@arachne.digital