IMPORTANT! THIS IS A "*SHREDDED*" DOCUMENT (created by Susan)

TO RETURN TO (this) pdf, ALWAYS CLICK THE BACK ARROW "←" AFTER *HYPER-LINKING away.*

BEGINNING NOTES – **26** total "notes": OR JUMP to Indictment START

(1) The section sign (§) is a typographical character used mainly to refer to a particular section of a document, **such as a legal code.** It is also called "double S" and "sectional symbol".

(2) https://en.wikipedia.org/wiki/International_Criminal_Court

(3) https://en.wikipedia.org/wiki/States_parties_to_the_Rome_Statute_of_the_International_Criminal_Court

(4) **Russia is NOT a member (or signatory) of the International Criminal Court (ICC).**

(5) Statutes violated: **(18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq.)**

(6) Title 18 of the United States Code " ... is the official compilation and codification of the general and permanent federal statutes of **the United States**. " The section sign (§) [as used] is a typographical character used mainly to refer to a particular section of a document, such as a legal code. ..."

(7) DETAILS of United States Statutes (presented by Cornell LAW SCHOOL) https://www.law.cornell.edu/uscode/text/18/2 Principals :: is punishable as a "principal" – defined, https://www.law.cornell.edu/uscode/text/18/371 Conspiracy to commit offense or to defraud United States, https://www.law.cornell.edu/uscode/text/18/1030 Fraud and related activity in connection with computers, https://www.law.cornell.edu/uscode/text/18/1028A Aggravated identity theft, https://www.law.cornell.edu/uscode/text/18/1956 Laundering of monetary instruments, https://www.law.cornell.edu/uscode/text/18/3551 Authorized sentences

(8) "et seq." (et seek) n. abbreviation for the Latin phrase et sequentes meaning "and the following." It is commonly used by lawyers to include numbered lists, pages or sections after the first number is stated, as in "the rules of the road are found in Vehicle Code Section 1204, et seq." source URL > https://dictionary.law.com/Default.aspx?selected=667

(9) **If read aloud, Americans would say:** " Title 18 of the United States Code " is the official compilation and codification of the general and permanent federal statutes of the United States of America. The symbol (§) is a typographical character used mainly to refer to a particular section of a document, such as a legal code. Thus, the numbers cited represent various portions of the USA "legal code" ; That is, '**2**' defines who is a "Principal" [for USA purposes]; **371** defines "Conspiracy to commit offense or to defraud United States"; **1030** defines " Fraud and related activity in connection with computers"; **1028A** defines "Aggravated identity theft"; **1956** defines " Laundering of monetary instruments"; AND, **3551** defines (the) "Authorized sentences" for these crimes. (IF committed by USA citizens!) Lastly, "**et seq.**" (et seek) is an abbreviation for the Latin phrase: *et sequentes* "and the following." It is commonly used by lawyers to include numbered lists, pages or sections after the first number is stated. "

(10) An "indictment document" – in the United States https://en.wikipedia.org/wiki/Indictment#United_States

(11) An Indictment document - in **the United States of America** (continued)

(12) The Fifth Amendment to **the Constitution of the United States** states in part: "…No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of **a Grand Jury**, except in cases arising in the land or naval forces, or in the Militia when in actual service in time of War or public danger… ". The requirement of an indictment has not been incorporated against the states; **therefore**, although the federal government uses grand juries and indictments, not all U.S. states do. In many, but not all, United States jurisdictions that use grand juries, prosecutors often have **a choice** between seeking an indictment from a grand jury **and** filing a charging document directly with the court. Such a document is usually called an information, accusation, or complaint, **to distinguish it from a grand-jury indictment.** To protect the **suspect's due-process rights** in felony cases (**where the suspect's interest in liberty is at stake**), there is usually a "preliminary hearing", at which a judge determines whether there was ***probable cause*** to arrest the suspect who is in custody. If the judge finds such probable cause, he or she binds, or holds over, the suspect for trial. The **substance** of an indictment or other **charging instrument** is usually the same, regardless of the jurisdiction: it (the **charging instrument)** consists of a short and plain statement of where, when, and how the defendant allegedly committed the offense. **Each offense usually is set out in a separate count.**
Indictments for complex crimes, particularly those involving ***conspiracy*** or numerous counts, **may run to hundreds of pages**; **[the FBI indictment (of interest) has 29 pages]** However, in other cases an indictment for a crime as serious as murder, may consist of a single sheet of paper**. Indictable offenses are normally tried by jury - *unless* the accused waives the right to a jury trial.** Although the Sixth Amendment mandates the right to a jury trial in any criminal prosecution, **the vast majority of criminal cases in the United States are resolved by the plea-bargaining process.**

(13) **In English: *A British propaganda leaflet* dropped over Essen (Germany) after a RAF bombing raid in March 1943. The main title says "Fortress Europe has no roof".** Source: Imperial War Museum, London.

https://commons.wikimedia.org/wiki/File:Die_Festung_Europa_hat_kein_Dach.JPG

Die Festung Europa hat kein Dach

IM April 1943 warf die R.A.F. mehr als 10 Millionen Kilogramm Bomben auf deutsche Industrieziele.

Im Mai 1943 wurden über 12 Millionen Kilogramm Bomben abgeworfen.

In einer einzigen Woche im Mai fielen 750 000 Kilogramm Bomben allein auf das Ruhrgebiet.

Bis 1. Juni 1943 haben englische Flugzeuge über 100 Millionen Kilogramm Bomben auf Deutschland abgeworfen.

Die Royal Air Force ist heute stärker als die deutsche und italienische Luftwaffe zusammen.

In Amerika wurden allein im April 1943 7 000 Flugzeuge fertiggestellt.

Die amerikanische Flugzeugindustrie hat am 31. Mai das 100 000. Flugzeug für diesen Krieg geliefert.

Amerika produziert heute mehr Flugzeuge als Deutchland, Italien und Japan zusammen.

Das sind die Tatsachen. Was folgt daraus? Man könnte sagen: Was die Engländer ausgehalten haben, können die Deutschen auch aushalten.

Aber der Vergleich hinkt. Die englisch-amerikanische Luftoffensive gegen Deutschland ist bereits jetzt weit schwerer als die deutsche Luftoffensive gegen England je war. In ihrem schwersten Angriff auf eine englische Stadt (London, 10. Mai 1941) warf die Luftwaffe 450 000 Kilogramm Bomben in einer Nacht.

In ihrem bisher schwersten Angriff auf eine deutsche Stadt (Dortmund, 23. Mai 1943) warf die R.A.F. 2 000 000 Kilogramm Bomben in einer Nacht. Mehr als viermal soviel — und das ist erst der Anfang.

Die Engländer konnten standhalten, weil sie wussten: Wenn sie standhalten, musste es besser werden. Sie hatten kaum angefangen zu rüsten. Sie kamen erst in Gang. Sie wussten, dass ihre eigene Luftmacht und Luftverteidigung von Tag zu Tag wuchs.

Sie sahen amerikanisches Kriegsmaterial in Massen ankommen und sie konnten hoffen, dass Amerika eines Tages als Verbündeter an ihrer Seite stehen würde.

Was haben heute die Deutschen zu hoffen, wenn sie sich standhaft weiter bomben lassen?

Neue Verbündete gibt es nicht mehr. Deutschlands eigene Kampfkraft lässt nach. Die englisch-amerikanische wächst von Tag zu Tag. Deutschlands Fabriken werden bombardiert. Seine Produktion ist um 20% gesunken. Amerikas Produktion ist „bombensicher".

Deutschlands geschwächte Luftwaffe muss an drei Fronten kämpfen. Überall ist sie in der Defensive. Die R.A.F. und die amerikanische Heeresfliegerei haben, trotz Atlantik-Wall, eine Front im Herzen Deutschlands geschaffen. Die „Festung Europa" hat kein Dach.

Daran ist nichts mehr zu ändern. Die deutschen Arbeiter und Ingenieure, die in den Fabriken aushalten, können den Gang des Krieges nicht mehr wenden. Sie können den Krieg nur verlängern. Das heisst: Sie können dafür sorgen, dass noch mehr Bomben auf Deutschland fallen.

Es werden immer mehr werden von Monat zu Monat.

Wie lange soll das noch so weiter gehen ?

(14) Mr. Robert Mueller (https://en.wikipedia.org/wiki/Special_Counsel_investigation_(2017%E2%80%93present)

(15) Mr. Mueller's **Official Document Download Site:** https://www.justice.gov/file/1080281/download

(16) **NOTE: Named "Organization 1" (above) *appears* to be "WikiLeaks" only**

https://en.wikipedia.org/wiki/WikiLeaks "… **Allegations of Russian influence: In August 2016,** after WikiLeaks published thousands of DNC emails, it was claimed that Russian intelligence had hacked the e-mails and leaked them to WikiLeaks. At the time, DNC officials made such claims, along with a number of cybersecurity experts and cybersecurity firms.[276][277] In October 2016, the US intelligence community announced that it was "confident that the Russian Government **directed** the recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations".[16] The US intelligence agencies said that the **hacks were consistent with the methods of Russian-directed efforts**, and that people high up within the Kremlin were *likely* involved.[16] On 14 October 2016, CNN reported that "there is mounting evidence that the Russian government is supplying WikiLeaks with hacked emails pertaining to the U.S. presidential election."[278] WikiLeaks has denied any connection to or co-operation with Russia.[278] President Putin has strongly denied any Russian involvement in the election.[202][203]**… In September 2016,** the German weekly magazine *Focus* reported that according to a confidential German government dossier, **WikiLeaks had long since been infiltrated by Russian agents** aiming to discredit NATO governments. The magazine added that French and British intelligence services had come to the same conclusion and said Russian President Vladimir Putin and Prime Minister Dmitry Medvedev receive details about what WikiLeaks publishes before publication.[279] The *Focus* report followed a *New York Times* story that suggested that WikiLeaks may be a laundering machine for compromising material about Western countries gathered by Russian spies.[280]…On 10 December 2016, several news outlets, including *The Guardian* and *The Washington Post*, reported that the Central Intelligence Agency concluded that Russia intelligence operatives provided materials to WikiLeaks in an effort to help Donald Trump's election bid. *The Washington Post* article stated: "The CIA has concluded in a secret assessment that Russia intervened in the 2016 election to help Donald Trump win the presidency, rather than just to undermine confidence in the U.S. electoral system, according to officials briefed on the matter."[281] *The Guardian* article reported, "individuals linked to the Russian government had provided WikiLeaks with thousands of confidential emails stolen from the Democratic National Committee (DNC) and others."[282] WikiLeaks has frequently been criticised for its absence of whistleblowing on or criticism of Russia.[22] *The Guardian* notes that journalists are killed frequently in Russia, and notes that *Freedom House* has ranked Russian press freedom as "not free... The main national news agenda is firmly controlled by the Kremlin. The government sets editorial policy at state-owned television stations, which dominate the media landscape and generate propagandistic content.[283] …"

(17) (NOTE: What follows is my (Susan's) personal version – with hyperlinks, etc. added --- This technique of "absorbing" a document is called "shredding"

(18) https://en.wikipedia.org/wiki/United_States_Intelligence_Community

(19) https://en.wikipedia.org/wiki/Director_of_National_Intelligence [Dan Coates]

*(20) https://www.guru99.com/web-security-vulnerabilities.html :: **The Top 10 security vulnerabilities as per OWASP Top 10 are:** SQL Injection, Cross Site Scripting, Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery, Security*

Misconfiguration, Insecure Cryptographic Storage, Failure to restrict URL Access, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards

(21) https://www.pbs.org/wgbh/americanexperience/features/truman-leaflets/

(22) Leaflets Warning Japanese of Atomic Bomb

Leaflets dropped on cities in Japan warning civilians about the atomic bomb, dropped c. August 6, 1945.

(23) **TO THE JAPANESE PEOPLE:**

America asks that you take immediate heed of what we say on this leaflet.
-We are in possession of the most destructive explosion ever devised by man. A single one of our newly developed atomic bombs is actually the equivalent in explosive power to what 2000 of our giant B-29s can carry on a single mission. This awful fact is one for you to ponder and we solemnly assure you it is grimly accurate.
- We have just begun to use this weapon against your homeland. If you still have any doubt, make inquiry as to what happened to Hiroshima when just one atomic bomb fell on that city.
-Before using this bomb to destroy every resource of the military by which they are prolonging this useless war, we ask that you now petition the Emperor to end the war. Our president has outlined for you the thirteen consequences of an honorable surrender. We urge that you accept these consequences and begin the work of building a new, better and peace-loving Japan.
-You should take steps now to cease military resistance. Otherwise, we shall resolutely employ this bomb and all our other superior weapons to promptly and forcefully end the war. ---- **EVACUATE YOUR CITIES!**

(24) **ATTENTION JAPANESE PEOPLE. EVACUATE YOUR CITIES.**

- Because your military leaders have rejected the thirteen part surrender declaration, two momentous events have occurred in the last few days. [article – declaration]
- The Soviet Union, because of this rejection on the part of the military has notified your Ambassador Sato that it has declared war on your nation. Thus, all powerful countries of the world are now at war with you.
- Also, because of your leaders' refusal to accept the surrender declaration that would enable Japan to honorably end this useless war, we have employed our

atomic bomb.
- A single one of our newly developed atomic bombs is actually the equivalent in explosive power to what 2000 of our giant B-29s [aircraft] could have carried on a single mission. Radio Tokyo [A:B : "Tokyo Rose"] has told you that with the first use of this weapon of total destruction, Hiroshima was virtually destroyed.
- Before we use this bomb again and again to destroy every resource of the military by which they are prolonging this useless war, petition the emperor now to end the war. Our president [Truman] has outlined for you the thirteen consequences of an honorable surrender. We urge that you accept these consequences and begin the work of building a new, better, and peace-loving Japan.
- Act at once **or** we shall resolutely employ this bomb and all our other superior weapons to promptly and forcefully end the war.

(25) **EVACUATE YOUR CITIES.**

(Source: Harry S. Truman Library, Miscellaneous historical document file, no. 258.)

A U.S. Air Force C-47 releases psychological warfare leaflets near Nha Trang, South Vietnam (August 1969)

https://commons.wikimedia.org/wiki/File:A_U.S._Air_Force_C-47_releases_psychological_warfare_leaflets_near_Nha_Trang,_South_Vietnam._-_NARA_-_542339.tif

(26) *Indictment* ***TABLE of CONTENTS****:*

COUNT 1 *- START see statement numbered 1. (Conspiracy to Commit an Offense Against the United States) :: Conspiracy*

"Hacking into the DNC Network" *START see statement numbered 26*

COUNTs 2-9 *- START see statements numbered 54 and 55 - Table format. (Aggravated Identity Theft)*

COUNT 10 *- START see statement numbered 56. (Conspiracy to Launder Money)*

COUNT 11 *- START see statement numbered 66. :: Object of the Conspiracy :: Manner and Means of the Conspiracy*

Statutory Allegations *- see statement numbered 65 & 77.*

FORFEITURE ALLEGATION *- see statement numbered 79.*

TAG-START RETURN to This document's "top" / Start

Mr. Mueller's document follows (as copied AND "shredded" – by Susan [**])
NOTE :: Indictment "page numbering" from original is ALSO maintained.
Example: **" Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 1 of 29"**

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, and 3551 et seq.)
[the 12 named "defendants – are ALL Russian persons & citizens]
1) VIKTOR BORISOVICH NETYKSHO, *
2) BORIS ALEKSEYEVICH ANTONOV, *
3) DMITRIY SERGEYEVICH BADIN, *
4) IVAN SERGEYEVICH YERMAKOV, *
5) ALEKSEY VIKTOROVICH * LUKASHEV, *
6) SERGEY ALEKSANDROVICH * MORGACHEV, *
7) NIKOLAY YURYEVICH KOZACHEK, *
8) PAVEL VYACHESLAVOVICH * YERSHOV, *
9) ARTEM ANDREYEVICH * MALYSHEV, *
10) ALEKSANDR VLADIMIROVICH * OSADCHUK, *
11) ALEKSEY ALEKSANDROVICH * POTEMKIN,*
12) and * ANATOLIY SERGEYEVICH * KOVALEV, *[12 Defendants.] *

INDICTMENT [NOTE (in America): YOU can "indict" a ham sandwich!]

The Grand Jury for the District of Columbia charges:

COUNT ONE *(Conspiracy to Commit an Offense Against the United States)*

[NOTE: *SEE Prosecuting Criminal Conspiracies (a 65 page PDF)]*

1. In or around 2016, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). **The GRU** had multiple units, including **Units 26165** and **74455**, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. **These units** conducted largescale cyber operations to interfere with the 2016 U.S. presidential election. [How is it known, the purpose was "interference"? Specifically, Did Mr. Putin prefer that Donald J. Trump win the 2016 Presidential election? (link)]

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 1 **of 29**

2. Defendants [named above] … were GRU officers [ALL members of the Russian Military] who knowingly and intentionally conspired with each other, and with persons known and unknown to the Grand Jury (collectively the "*Conspirators*"), to: [Were these Russian citizens under "orders"?]

A) gain unauthorized access (to "hack") into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election,

[When the USA "interfered – on numerous occasions (see CMU database) – in other country's elections – Did the USA seek permission?]

B) steal documents from those computers, and [Did the authors mean "copy"?]

C) stage releases of the stolen [*copied*] documents

[AND] **D**) to " interfere with the 2016 U.S. presidential election." [How is ALL of this "known"?]

[Define "know": https://www.merriam-webster.com/dictionary/know

3. Starting in at least March 2016, the *Conspirators* used a variety of means to ***hack*** the email accounts of volunteers and employees of the U.S. presidential campaign of Hillary Clinton (the "Clinton Campaign"), including the email account of the Clinton Campaign's chairman. [John Podesta] [How is this known?] [Do the "victims" bear any responsibility – for their laziness & stupidity regarding "Information Security"?]

4. By in or around April 2016, the *Conspirators* also ***hacked*** into the computer networks of the Democratic Congressional Campaign Committee ("DCCC") and the Democratic National Committee ("DNC"). (I.E.) The *Conspirators*

a) covertly monitored the computers of dozens of DCCC and DNC employees, **b)** implanted hundreds of files containing malicious computer code ("malware"), and **c)** stole [copied] emails and other documents from the DCCC and DNC. [How is this known?] [Did the document author mean "copied" ?]

5. By in or around April 2016, the *Conspirators* began to plan the release of materials stolen from (copied from) the Clinton Campaign, DCCC, and DNC. [How is this known?]

6. Beginning in or around June 2016, the *Conspirators* staged and released tens of thousands of the stolen emails and documents. **They did so** using fictitious online personas, including ["DCLeaks" and "Guccifer 2.0."] [How is this known?] [ALSO, literally – any human can create such "personas" (link)] [This being a FACT – then, why is it alleged the "Defendants" did this?]

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 2 **of 29** 3

"DCLeaks" and "Guccifer 2.0."

7. The *Conspirators* also used the Guccifer 2.0 persona to release additional stolen documents through a website maintained by an organization ("Organization 1"), that had previously posted documents *stolen* from U.S. persons, entities, and the U.S. government. [Please cite the specifics of this Previous incident.] The *Conspirators* continued their U.S. election-interference operations through in or around November 2016. [How is this known?]

8. To hide their connections to Russia and the Russian government, the *Conspirators* used false identities and made false statements about their identities. [Motive? Why would the Defendants seek to "hide"] To further avoid detection, the *Conspirators* used a network of computers located across the world, including in the United States, and paid for this infrastructure using cryptocurrency. [How is this known? Please note the use of the term "likely" in the WikiLeaks article.]

(Defendants)

9. Defendant 1 VIKTOR BORISOVICH NETYKSHO (Нетыкшо Виктор Борисович) was the Russian military officer in command of Unit 26165, located at 20 Komsomolskiy Prospekt, Moscow, Russia. Unit 26165 **had primary**

responsibility for hacking the DCCC and DNC, as well as the email accounts of individuals affiliated with the Clinton Campaign. [How is this known?]

10. Defendant 2 BORIS ALEKSEYEVICH ANTONOV (Антонов Борис Алексеевич) was a Major in the Russian military assigned to Unit 26165. ANTONOV oversaw a department within Unit 26165 dedicated to targeting military, political, governmental, and non-governmental organizations with spear-phishing emails and other computer intrusion activity. ANTONOV held the title "Head of Department." In or around 2016, ANTONOV supervised other co-*conspirators* who targeted the DCCC, DNC, and individuals affiliated with the Clinton Campaign. [Please see the USA Naval web site – related to obtaining a Inter-disciplinary degree in Cyber…]

11. Defendant3 DMITRIY SERGEYEVICH BADIN (Бадин Дмитрий Сергеевич) was a Russian military officer assigned to Unit 26165 who held the title "Assistant Head of Department." In or around 2016, BADIN, along withANTONOV, supervised other co-*conspirators* who targeted the DCCC, DNC, and individuals affiliated with the Clinton Campaign. [How is this known?]

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 3 of 29 4

12. Defendant4 IVAN SERGEYEVICH YERMAKOV (Ермаков Иван Сергеевич) was a Russian military officer assigned to ANTONOV's department within Unit 26165. Since in or around 2010, YERMAKOV used various online personas, including "Kate S. Milton," "James McMorgans," and "Karen W. Millen," to conduct hacking operations on behalf of Unit 26165. In or around March 2016, YERMAKOV participated in hacking at least two email accounts from which campaign-related documents were released through DCLeaks. In or around May 2016, YERMAKOV also participated in hacking the DNC email server and stealing DNC emails that were later released through Organization 1. NOTE: "DCleaks" is known: https://en.wikipedia.org/wiki/DCLeaks

13. Defendant5 ALEKSEY VIKTOROVICH LUKASHEV (Лукашев Алексей Викторович) was a Senior Lieutenant in the Russian military assigned to ANTONOV's department within Unit 26165. LUKASHEV used various online personas, including "Den Katenberg" and "Yuliana Martynova." In or around 2016, LUKASHEV sent spear-phishing emails to members of the Clinton Campaign and affiliated individuals, including the chairman of the Clinton Campaign. [How is this known?]

14. Defendant6 SERGEY ALEKSANDROVICH MORGACHEV (Моргачев Сергей Александрович) was a Lieutenant Colonel in the Russian military assigned to Unit 26165. MORGACHEV oversaw a department within Unit 26165 dedicated to developing and managing malware, including a hacking tool used by the GRU known as "X-Agent." During the hacking of the DCCC and DNC networks, MORGACHEV supervised the co-*conspirators* who developed and monitored the X-Agent malware implanted on those computers. [How is this known?]

15. Defendant7 NIKOLAY YURYEVICH KOZACHEK (Козачек Николай Юрьевич) was a Lieutenant Captain in the Russian military assigned to MORGACHEV's department within Unit 26165. KOZACHEK used a variety of monikers, including "kazak" and "blablabla1234565." KOZACHEK developed, customized, and monitored X-Agent malware used to hack the DCCC networks beginning in or around April 2016. [How is this known?]

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 4 of 29 5 and DNC

16. Defendant8 PAVEL VYACHESLAVOVICH YERSHOV (Ершов Павел Вячеславович) was a Russian military officer assigned to MORGACHEV's department within Unit 26165. In or around 2016, YERSHOV assisted KOZACHEK and other co-*conspirators* in testing and customizing X-Agent malware before actual deployment and use. [How is this known?]

17. Defendant9 ARTEM ANDREYEVICH MALYSHEV (Малышев Артём Андреевич) was a Second Lieutenant in the Russian military assigned to MORGACHEV's department within Unit 26165. MALYSHEV used a variety of monikers, including "djangomagicdev" and "realblatr." In or around 2016, MALYSHEV monitored X-Agent malware implanted on the DCCC and DNC networks. [How is this known?]

18. Defendant10 ALEKSANDR VLADIMIROVICH OSADCHUK (Осадчук Александр Владимирович) was a Colonel in the Russian military and the commanding officer of Unit 74455. Unit 74455 was located at 22 Kirova Street, Khimki, Moscow, a building referred to within the GRU as the "Tower." Unit 74455 assisted in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU. [How is this known?]

19. Defendant11 ALEKSEY ALEKSANDROVICH POTEMKIN (Потемкин Алексей Александрович) was an officer in the Russian military assigned to Unit 74455. POTEMKIN was a supervisor in a department within Unit 74455 responsible for the administration of computer infrastructure used in cyber operations. Infrastructure and social media accounts administered by POTEMKIN's department were used, among other things, to assist in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas. [How is this known?]

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 5 of 29 6 Object of the

Conspiracy

20. The object of the conspiracy was to

a) ***hack*** into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election,

b) steal documents from those computers, [Does the author mean "copy"?]

and c) stage releases of the stolen documents to interfere with the 2016 U.S. presidential election. [How do actions a), b) and c) result in "interference" …?]

[I.E. The USA has very strong Freedom of Speech laws & history SEE New York Times versus Sullivant]

Manner and Means of the Conspiracy ## Spear-phishing Operations

21. ANTONOV, BADIN, YERMAKOV, LUKASHEV, and their co-conspirators targeted victims using a technique known as spear-phishing to steal victims' passwords or otherwise gain access to their computers. Beginning by at least March 2016, the *Conspirators* targeted over 300 individuals affiliated with the Clinton Campaign, DCCC, and DNC. [How is this known?]

a. For example, on or about March 19, 2016, LUKASHEV and his co-*conspirators* created and sent a spear-phishing email to the chairman of the Clinton Campaign.[?Podesta?] LUKASHEV used the account "john356gh" at an online service [name please] that abbreviated lengthy website addresses (referred to as a "URL-shortening service"). LUKASHEV used the account to mask a link contained in the spear-phishing email, which directed the recipient to a GRU-created website. LUKASHEV altered the appearance of the sender email address in order to make it look like the email was a security notification from Google (a technique known as "spoofing"), instructing the user to change his password by

clicking the embedded link. Those instructions were followed. On or about March 21, 2016, LUKASHEV, YERMAKOV, and their co-*conspirators* stole the contents of the chairman's email account, which consisted of over 50,000 emails.
b. Starting on or about March 19, 2016, LUKASHEV and his co-*conspirators* sent spear-phishing emails to the personal accounts of other individuals affiliated with

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 6 of 29 7

the Clinton Campaign, including its campaign manager (John Podesta?) and a senior foreign policy advisor (Jacob Jeremiah Sullivan?). On or about March 25, 2016, LUKASHEV used the same john356gh account to mask additional links included in spear-phishing 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.
c. On or about March 28, 2016, YERMAKOV researched the names of Victims 1 and 2 and their association with Clinton on various social media sites. Through their spear-phishing operations, LUKASHEV, YERMAKOV, and their co-*conspirators* successfully stole email credentials and thousands of emails from numerous individuals affiliated with the Clinton Campaign. Many of these stolen emails, including those from Victims 1 and 2, were later released by the Conspirators through DCLeaks.
d. On or about April 6, 2016, the *Conspirators* created an email account in the name (with a one-letter deviation from the actual spelling) of a known member of the Clinton Campaign. The *Conspirators* then used that account to send spear-phishing emails to the work accounts of more than thirty different Clinton Campaign employees. In the spear-phishing emails, LUKASHEV and his co-*conspirators* embedded a link purporting to direct the recipient to a document titled "hillaryclinton-favorable-rating.xlsx." In fact, this link directed the recipients' computers to a GRU-created website.

22. The *Conspirators* spear-phished individuals affiliated with the Clinton Campaign throughout the summer of 2016. For example, on or about July 27, 2016, the Conspirators

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 7 of 29 8

attempted after hours to spearphish for the first time email accounts at a domain hosted by a thirdparty 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. Hacking into the DCCC Network

23. Beginning in or around March 2016, the Conspirators, in addition to their spear-phishing efforts, researched the DCCC and DNC computer networks to identify technical specifications and vulnerabilities.

a. For example, beginning on or about March 15, 2016, YERMAKOV ran a technical query for the DNC's internet protocol configurations to identify connected devices.

b. On or about the same day, YERMAKOV searched for open-source information about the DNC network, the Democratic Party, and Hillary Clinton.

c. On or about April 7, 2016, YERMAKOV ran a technical query for the DCCC's internet protocol configurations to identify connected devices.

24. By in or around April 2016, within days of YERMAKOV's searches regarding the DCCC, the Conspirators hacked into the DCCC computer network. Once they gained access, they installed and managed different types of malware to explore the DCCC network and steal data.

a. On or about April 12, 2016, the Conspirators used the stolen credentials of a DCCC Employee ("DCCC Employee 1") to access the DCCC network. DCCC Employee 1 had received a spear-phishing email from the Conspirators on or about April 6, 2016, and entered her password after clicking on the link.

b. Between in or around April 2016 and June 2016, the Conspirators installed multiple versions of their X-Agent malware on at least ten DCCC computers, which allowed them to monitor individual employees' computer activity, steal passwords, and maintain access to the DCCC network.

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 8 of 29 9

c. X-Agent malware implanted on the DCCC network transmitted information from the victims' computers to a GRU-leased server located in Arizona. The Conspirators referred to this server as their "AMS" panel. KOZACHEK, MALYSHEV, and their co-conspirators logged into the AMS panel to use X-Agent's keylog and screenshot functions in the course of monitoring and surveilling activity on the DCCC computers. The keylog function allowed the Conspirators to capture keystrokes entered by DCCC employees. The screenshot function allowed the Conspirators to take pictures of the DCCC employees' computer screens. d. For example, on or about April 14, 2016, the Conspirators repeatedly activated X-Agent's keylog and screenshot functions to surveil DCCC Employee 1's computer activity over the course of eight hours. During that time, the Conspirators captured DCCC Employee 1's communications with co-workers and the passwords she entered while working on fundraising and voter outreach projects. Similarly, on or about April 22, 2016, the Conspirators activated X-

Agent's keylog and screenshot functions to capture the discussions of another DCCC Employee ("DCCC Employee 2") about the DCCC's finances, as well as her individual banking information and other personal topics.

25. On or about April 19, 2016, KOZACHEK, YERSHOV, and their co-conspirators remotely configured an overseas computer to relay communications between X-Agent malware and the AMS panel and then tested X-Agent's ability to connect to this computer. The Conspirators referred to this computer as a "middle server." The middle server acted as a proxy to obscure the connection between malware at the DCCC and the Conspirators' AMS panel. On or about April 20, 2016, the *Conspirators* directed X-Agent malware on the DCCC computers to connect to this middle server and receive directions from the *Conspirators*.

Hacking into the DNC Network

26. On or about April 18, 2016, the Conspirators hacked into the DNC's computers through their access to the DCCC network. The Conspirators then installed and managed different types of malware (as they did in the DCCC network) to explore the DNC network and steal documents.

a. On or about April 18, 2016, the Conspirators activated X-Agent's keylog and screenshot functions to steal credentials of a DCCC employee who was authorized to access the DNC network. The Conspirators hacked into the DNC network from the DCCC network using stolen credentials. By in or around June 2016, they gained access to approximately thirty-three DNC computers.

b. In or around April 2016, the Conspirators installed X-Agent malware on the DNC network, including the same versions installed on the DCCC network. MALYSHEV and his co-conspirators monitored the X-Agent malware from the AMS 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. Theft of DCCC and DNC Documents

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 9 of 29 10

27. The Conspirators searched for and identified computers within the DCCC and DNC networks that stored information related to the 2016 U.S. presidential election. For example, on or about April 15, 2016, the Conspirators searched one hacked DCCC computer for terms that included "hillary," "cruz," and "trump." The Conspirators also copied select DCCC folders, including "Benghazi Investigations." The Conspirators targeted computers containing information such as opposition research and field operation plans for the 2016 elections.

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 10 of 29 11

28. To enable them to steal a large number of documents at once without detection, the Conspirators used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks. The Conspirators then used other GRU malware, known as "X-Tunnel," to move the stolen documents outside the DCCC and DNC networks through encrypted channels. a. For example, on or about April 22, 2016, the Conspirators compressed gigabytes of data from DNC computers, including opposition research. The Conspirators later moved the compressed DNC data using X-Tunnel to a GRU-leased computer located in Illinois. b. On or about April 28, 2016, the Conspirators connected to and tested the same computer located in Illinois. Later that day, the Conspirators used X-Tunnel to connect to that computer to steal additional documents from the DCCC network.
29. Between on or about May 25, 2016 and June 1, 2016, the Conspirators hacked the DNC Microsoft Exchange Server and stole thousands of emails from the work accounts of DNC employees. During that time, YERMAKOV researched PowerShell commands related to accessing and managing the Microsoft Exchange Server.
30. On or about May 30, 2016, MALYSHEV accessed the AMS panel in order to upgrade custom AMS software on the server. That day, the AMS panel received updates from approximately thirteen different X-Agent malware implants on DCCC and DNC computers.

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 11 of 29 12

31. During the hacking of the DCCC and DNC networks, the *Conspirators "covered their tracks"* by intentionally deleting logs and computer files.

For example, on or about May 13, 2016, the *Conspirators* cleared the event logs from a DNC computer. On or about June 20, 2016, the *Conspirators* deleted logs from the AMS panel that documented their activities on the panel, including the login history. Efforts to Remain on the DCCC and DNC Networks

32. Despite the Conspirators' efforts to hide their activity, beginning in or around May 2016, both the DCCC and DNC **became aware that they had been hacked and hired a security company ("Company 1")** to identify the extent of the intrusions. By in or around June 2016, Company 1 took steps to exclude intruders from the networks. Despite these efforts, 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. [How was/is it known this "registered" internet domain – is "GRU" associated?] [Susan has an internet domain (www.hansANDcassady.org) – her domain was "registered through "GOdaddy" – I have NO recollection (that) GD required me to identify myself as an American.]

33. In response to Company 1's efforts, the Conspirators took countermeasures to maintain access to the DCCC and DNC networks. [US Navy Washdown Countermeasures – Susan worked on the WC for the DDG51 War Ship]
a. On or about May 31, 2016, YERMAKOV searched for open-source information about Company 1 and its reporting on X-Agent and X-Tunnel. On or about June 1, 2016, the Conspirators attempted to delete traces of their presence on the DCCC network using the computer program CCleaner.
b. On or about June 14, 2016, the Conspirators registered the domain actblues.com, which mimicked the domain of a political fundraising platform that included a DCCC donations page. Shortly thereafter, the Conspirators used stolen DCCC credentials to modify the DCCC website and redirect visitors to the actblues.com domain.
c. On or about June 20, 2016, after Company 1 had disabled X-Agent on the DCCC network, the Conspirators spent over seven hours unsuccessfully trying to connect to X-Agent. The Conspirators also tried to access the DCCC network using previously stolen credentials.

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 12 of 29 13

34. In or around September 2016, the Conspirators also 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, the Conspirators gathered data by creating backups, or "snapshots," of the DNC's cloud-based systems using the cloud provider's own technology. The Conspirators then moved the snapshots to cloud-based accounts they had registered with the same service, thereby stealing the data from the DNC.
Stolen Documents Released through DCLeaks

35. More than a month before the release of any documents, the *Conspirators* constructed the online persona DCLeaks to release and publicize stolen election-related documents. On or about April 19, 2016, after attempting to register the domain electionleaks.com, the *Conspirators* registered the domain dcleaks.com through a service that anonymized the registrant. [WHY is a business – which

defeats USA law purposes – even permitted to exist?] The funds used to pay for the dcleaks.com domain originated from an account at an online cryptocurrency service that the *Conspirators* 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 used by LUKASHEV to spear-phish the Clinton Campaign chairman [John Podesta?] and other campaign-related individuals.

36. On or about June 8, 2016, the Conspirators launched the public website dcleaks.com, which they used to release stolen emails. Before it shut down in or around March 2017, the site received over one million page views. The Conspirators falsely claimed on the site that DCLeaks was started by a group of "American hacktivists," when in fact it was started by the *Conspirators*.

37. Starting in or around June 2016 and continuing through the 2016 U.S. presidential election, the Conspirators used DCLeaksto release emailsstolen from individuals affiliated with the Clinton Campaign. The Conspirators also released documents they had stolen in other spear-phishing operations, including those they had conducted in 2015 that collected emails from individuals affiliated with the Republican Party.

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 13 of 29 14

38. On or about June 8, 2016, and at approximately the same time that the dcleaks.com website was launched, the Conspirators created a DCLeaks Facebook page using a preexisting social media account under the fictitious name "Alice Donovan." In addition to the DCLeaks Facebook page, the Conspirators 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. The Conspirators accessed these accounts from computers managed by POTEMKIN and his co-conspirators.

39. On or about June 8, 2016, the *Conspirators* created the Twitter account @dcleaks_. The Conspirators operated the @dcleaks_ Twitter account from the same computer used for other efforts to interfere with the 2016 U.S. presidential election. For example, 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. Stolen Documents Released through Guccifer 2.0

40. On or about June 14, 2016, the DNC—through Company 1—publicly announced that it had been hacked by Russian government actors. In response, the Conspirators created the online persona Guccifer 2.0 and falsely claimed to be a lone Romanian hacker to undermine the allegations of Russian responsibility for

the intrusion.
41. On or about June 15, 2016, the Conspirators logged into a Moscow-based server used and managed by Unit 74455 and, between 4:19 PM and 4:56 PM Moscow Standard Time, searched for certain words and phrases, including: Search Term(s) "some hundred sheets" "some hundreds of sheets" dcleaks illuminati широко известный перевод [widely known translation] "worldwide known" "think twice about" "company's competence"

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 14 of 29 15
42. Later that day, at 7:02 PM Moscow Standard Time, the online persona Guccifer 2.0 published its first post on **a blog site created through WordPress.** Titled "**DNC's servers hacked by a lone hacker,**" the post used numerous English words and phrases that the *Conspirators* had searched for earlier that day (bolded below): **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]!!!!!!!!!

43. Between in or around June 2016 and October 2016, the *Conspirators* used Guccifer 2.0 to release documents through WordPress that they had stolen from the DCCC and DNC. The *Conspirators*, posing as Guccifer 2.0, also shared stolen documents with certain individuals.
a. On or about August 15, 2016, the Conspirators, posing as Guccifer 2.0, received a request for stolen documents from a candidate for the U.S. Congress. The *Conspirators* responded using the Guccifer 2.0 persona and sent the candidate stolen documents related to the candidate's opponent.
b. On or about August 22, 2016, the Conspirators, 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. c. On or about August 22, 2016, the *Conspirators*, posing as Guccifer 2.0, 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.

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 15 of 29 16

44. The *Conspirators*, posing as Guccifer 2.0, also communicated with U.S. persons about the release of stolen documents. On or about August 15, 2016, the Conspirators, 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?" 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."

45. The *Conspirators* conducted operations as Guccifer 2.0 and DCLeaks using overlapping computer infrastructure and financing. a. For example, between on or about March 14, 2016 and April 28, 2016, the Conspirators used the same pool of bitcoin funds to purchase a virtual private network ("VPN") account and to lease a server in Malaysia. In or around June 2016, the Conspirators used the Malaysian server to host the dcleaks.com website. On or about July 6, 2016, the Conspirators used the VPN to log into the @Guccifer_2 Twitter account. The Conspirators opened that VPN account from the same server that was also used to register malicious domains for the hacking of the DCCC and DNC networks. b. On or about June 27, 2016, the Conspirators, posing as Guccifer 2.0, contacted a U.S. reporter with an offer to provide stolen emails from "Hillary Clinton's staff." The Conspirators 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 their co-conspirators in or around March 2016.
Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 16 of 29 17
46. On or about January 12, 2017, the Conspirators published a statement on the Guccifer 2.0 WordPress blog, falsely claiming that the intrusions and release of stolen documents had "totally no relation to the Russian government." Use of Organization 1

47. In order to expand their interference in the 2016 U.S. presidential election, the Conspirators transferred many of the documents they stole from the DNC and the chairman of the Clinton Campaign to Organization 1. The Conspirators, posing as Guccifer 2.0, discussed the release of the stolen documents and the timing of those releases with Organization 1 to heighten their impact on the 2016 U.S. presidential election. a. On or about June 22, 2016, Organization 1 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

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 17 of 29 18

have a much higher impact than what you are doing." On or about July 6, 2016, Organization 1 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." The Conspirators responded, "ok . . . i see." Organization 1 explained, "we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting." b. After failed attempts to transfer the stolen documents starting in late June 2016, on or about July 14, 2016, the Conspirators, posing as Guccifer 2.0, sent Organization 1 an email with an attachment titled "wk dnc link1.txt.gpg." The Conspirators explained to Organization 1 that the encrypted file contained instructions on how to access an online archive of stolen DNC documents. On or about July 18, 2016, Organization 1 confirmed it had "the 1Gb or so archive" and would make a release of the stolen documents "this week."

48. On or about July 22, 2016, Organization 1 released over 20,000 emails and other documents stolen from the DNC network by the *Conspirators*. This release occurred approximately three days before the start of the Democratic National Convention. Organization 1 did not disclose Guccifer 2.0's role in providing them. The latest-in-time email released through Organization 1 was dated on or about May 25, 2016, approximately the same day the *Conspirators* hacked the DNC Microsoft Exchange Server.

49. On or about October 7, 2016, Organization 1 released the first set of emails from the chairman of the Clinton Campaign that had been stolen by LUKASHEV and his co-conspirators. Between on or about October 7, 2016 and November 7, 2016, Organization 1 released approximately thirty-three tranches of documents that had been stolen from the chairman of the Clinton Campaign. In total, over 50,000 stolen documents were released. Statutory Allegations

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 18 of 29 19

50. Paragraphs 1 through 49 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

51. From at least in or around March 2016 through November 2016, in the District

of Columbia and elsewhere, Defendants (named) together with others known and unknown to the Grand Jury, **knowingly and intentionally conspired to commit offenses against the United States, namely:**
a. To knowingly access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, where the value of the information obtained exceeded $5,000, **in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B);**
and **b.** To knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to intentionally cause damage without authorization to a protected computer, and where the offense did cause and, if completed, would have caused, loss aggregating $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least ten protected computers during a one-year period, **in violation of**
Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

52. In furtherance of the Conspiracy and to effect its illegal objects, the Conspirators committed the overt acts set forth in paragraphs 1 through 19, 21 through 49, 55, and 57 through which are re-alleged and incorporated by reference as if fully set forth herein.

53. In furtherance of the Conspiracy, and as set forth in paragraphs 1 through 19, 21 through 49, 55, and 57 through 64, the Conspirators knowingly falsely registered a domain name and knowingly used that domain name in the course of committing an offense, namely, the Conspirators registered domains, including dcleaks.com and actblues.com, with false names and addresses, and used those domains in the course of committing the felony offense charged in Count One. All **in violation of Title 18, United States Code, Sections 371 and 3559(g)(1).**

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 19 of 29 20 64,

COUNTS TWO THROUGH NINE [listed below]
(Aggravated Identity Theft)

54. Paragraphs 1 through 19, 21 through 49, and 57 through 64 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

55. On or about the dates specified below, in the District of Columbia and elsewhere, Defendants (named)
did knowingly transfer, possess, and use, without lawful authority, a means of

identification of another person during and in relation to **a felony violation enumerated in**

Title 18, United States Code, Section 1028A(c),

namely, computer fraud **in violation of**

Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B),

knowing that the means of identification belonged to another real person:

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 20 of 29 21

Count#: Approximate Date: Victim# : Means of Identification [stolen for fraud]
2: March 21, 2016 Victim 3 Username and password for personal email account
3: March 25, 2016 Victim 1 Username and password for personal email account
4: April 12, 2016 Victim 4 Username and password for DCCC computer network
5: April 15, 2016 Victim 5 Username and password for DCCC computer network
6: April 18, 2016 Victim 6 Username and password for DCCC computer network
7: May 10, 2016 Victim 7 Username and password for DNC computer network
8: June 2, 2016 Victim 2 Username and password for personal email account
9:July 6, 2016 Victim 8 Username and password for personal email account

All in violation of

Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT TEN
(Conspiracy to Launder Money)

56. Paragraphs 1 through 19, 21 through 49, and 55 are re-alleged and incorporated by reference as if fully set forth herein.

57. To facilitate the purchase of infrastructure used in their hacking activity—including hacking into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election and releasing the stolen documents—the Defendants (named) conspired to launder the equivalent of more than $95,000 through a web of transactions structured to capitalize on the perceived anonymity

of cryptocurrencies such as bitcoin.

58. Although the *Conspirators* caused transactions to be conducted in a variety of currencies, including U.S. dollars, they principally used bitcoin when purchasing servers, registering domains, and otherwise making payments in furtherance of hacking activity. Many of these payments were processed by companies located in the United States (UN-NAMED companies) that provided " payment processing services" to hosting companies, domain registrars, and other vendors both international and domestic.

The use of "bitcoin" allowed the *Conspirators* to avoid direct relationships with traditional financial institutions, allowing them to evade greater scrutiny of their identities and sources of funds. ["allowed" versus enabled / permitted/ "made possible]

59. All bitcoin transactions are added to a public ledger called the Blockchain, but the Blockchain identifies the parties to each transaction only by alpha-numeric identifiers known as "bitcoin addresses". To further avoid creating a centralized paper trail of all of their purchases, the *Conspirators* purchased infrastructure using hundreds of different email accounts, in some cases using a new account for each purchase. The *Conspirators* used fictitious names and addresses in order to obscure their identities and their links to Russia and the Russian government. [MOTIVE? Why did the Defendants seek to …?]

For example, the dcleaks.com domain was registered and paid for using the fictitious name "Carrie Feehan" and an address in New York. In some cases, as part of the payment process, the *Conspirators* provided vendors with nonsensical addresses such as "usa Denver AZ," "gfhgh ghfhgfh fdgfdg WA," and "1 2 dwd District of Columbia." [Why did "vendors" accept this "nonsensical" …?]

60. The *Conspirators* used several dedicated email accounts to track basic bitcoin transaction information and to facilitate bitcoin payments to vendors. One of these dedicated accounts, registered with the username "gfadel47," received hundreds of bitcoin payment requests from approximately 100 different email accounts.
For example, on or about February 1, 2016, the gfadel47 account 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.

61. On occasion, the *Conspirators* facilitated bitcoin payments using the same

computers that they used to conduct their hacking activity, including to create and send test spear-phishing emails. [NOTE: Previous statement does NOT make sense – in the American English language. Please clarify.] Additionally, one of these dedicated accounts was used by the *Conspirators* in or around 2015 to renew the registration of a domain (linuxkrnl.net) encoded in certain X-Agent malware installed on the DNC network.[Is the author saying a domain was "encoded" by non-alphaNumeric symbols or NON-HTML recognized characters?]

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 21 of 29 22
Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 22 of 29 23

62. The *Conspirators* funded the purchase of computer infrastructure for their hacking activity in part by "mining" bitcoin. [That is,] Individuals and entities can "mine bitcoin" by allowing their computing power to be used to verify and record payments on the bitcoin public ledger, a service for which they are rewarded with freshly-minted bitcoin.
The pool of bitcoin generated from the GRU's mining activity was used, for example, to pay **a Romanian company** to register the domain dcleaks.com through a payment processing company located in the United States. [Please identify this USA company & "**Romanian company".**]
63. In addition to "mining bitcoin", the *Conspirators* acquired bitcoin through a variety of means designed to obscure the origin of the funds. This included:

a) purchasing bitcoin through peer-to-peer exchanges,
b) moving funds through other digital currencies,
and c) using pre-paid cards. [What USA company would provide "pre-paid cards" to Russian citizens ?] They [The *Conspirators*] also enlisted the assistance of one or more " third-party exchangers" who facilitated layered transactions through digital currency exchange platforms providing heightened anonymity. [Canada's laws]

64. The *Conspirators* used the same funding structure—and in some cases, the very same pool of funds—to purchase key accounts, servers, and domains used in their election-related hacking activity.
a. The bitcoin mining operation that funded the registration payment for dcleaks.com also sent newly-minted bitcoin to a bitcoin address controlled by "Daniel Farell," the persona that was used to renew the domain linuxkrnl.net. The bitcoin mining operation also funded, through the same bitcoin address, the purchase of servers and domains used in the GRU's spear-phishing operations, including **accountsqooqle.com** and **account-goooogle.com**.

b. On or about March 14, 2016, using funds in a bitcoin address, the *Conspirators* purchased a VPN account, which they later used to log into the @Guccifer_2 Twitter account. The remaining funds from that bitcoin address were then used on or about April 28, 2016, to lease a Malaysian server that hosted the dcleaks.com website. c. The *Conspirators* used a different set of fictitious names (including "Ward DeClaur" and "Mike Long") to send bitcoin to a U.S. company in order to lease a server used to administer X-Tunnel malware implanted on the DCCC and DNC networks, and to lease two servers used to hack the DNC's cloud network.

Statutory Allegations

65. From at least in or around 2015 through 2016, within the District of Columbia and elsewhere, Defendants (named), together with others, known and unknown to the Grand Jury, did knowingly and intentionally conspire to transport, transmit, and transfer monetary instruments and funds to a place in the United States from and through a place outside the United States and from a place in the United States to and through a place outside the United States, with the intent to promote the carrying on of **specified unlawful activity**, namely,

a violation of Title 18, United States Code, Section 1030,

contrary to Title 18, United States Code, Section 1956(a)(2)(A).

All in violation of Title 18, United States Code, Section 1956(h).

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 23 of 29 24

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 24 of 29 25

COUNT ELEVEN

(Conspiracy to Commit an Offense Against the United States)

66. Paragraphs 1 through 8 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein. Defendants: named

67. Paragraph 18 of this Indictment relating to ALEKSANDR VLADIMIROVICH OSADCHUK is re-alleged and incorporated by reference as if fully set forth herein.

68. Defendant12 ANATOLIY SERGEYEVICH KOVALEV (Ковалев Анатолий Сергеевич) was an officer in the Russian military assigned to Unit 74455 who worked in the GRU's 22 Kirova Street building (the Tower).

69. Defendants OSADCHUK and KOVALEV were GRU officers who knowingly and intentionally conspired with each other and with persons, known and unknown to the Grand Jury, to hack into the computers of 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.

Object of the Conspiracy

70. The object of the conspiracy was to hack into protected computers of persons and entities charged with the administration of the 2016 U.S. elections in order to access those computers and steal voter data and other information stored on those computers.

Manner and Means of the Conspiracy

71. In or around June 2016, KOVALEV and his co-conspirators researched domains used by U.S. state boards of elections, secretaries of state, and other election-related entities for website vulnerabilities. KOVALEV and his co-conspirators also searched for state political party email addresses, including filtered queries for email addresses listed on state Republican Party websites.

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 25 of 29 26

72. In or around July 2016, KOVALEV and his co-conspirators hacked the website of a state board of elections ("SBOE 1") **and stole information related to approximately 500,000 voters**, including names, addresses, partial social security numbers, dates of birth, and driver's license numbers. [Who is "SBOE 1"?]
73. In or around August 2016, KOVALEV and his co-conspirators hacked into the computers of a U.S. vendor ("Vendor 1") that supplied software used to verify voter registration information for the 2016 U.S. elections. KOVALEV and his co-conspirators used some of the same infrastructure to hack into Vendor 1 that they had used to hack into SBOE 1. [Who is "Vendor 1"?]
74. In or around August 2016, the Federal Bureau of Investigation issued an alert

about the hacking of SBOE 1 [FBI Cyber-ALERT] **and identified some of the infrastructure that was used to conduct the hacking**. In response, KOVALEV deleted his search history. KOVALEV and his co-conspirators also deleted records from accounts used in their operations targeting state boards of elections and similar election-related entities.

75. In or around October 2016, KOVALEV and his co-conspirators further targeted state and county offices responsible for administering the 2016 U.S. elections. [How is this known?]

For example, on or about October 28, 2016, KOVALEV and his co-conspirators **visited the websites of certain counties in Georgia, Iowa, and Florida to identify vulnerabilities.** [What "**vulnerabilities" (if any) were identified?]**

76. In or around November 2016 and prior to the 2016 U.S. presidential election, KOVALEV and his co-conspirators used an email account designed to look like a *Vendor 1* email address to send over 100 spear-phishing emails to organizations and personnel involved in administering elections in numerous Florida counties.

The spear-phishing emails contained malware that the *Conspirators* embedded into Word documents bearing Vendor 1's logo. [How is this known? Does MicroSoft realize that Word-User documents can be "embedded" – by a malicious party?]

Statutory Allegations

77. Between in or around June 2016 and November 2016, in the District of Columbia and elsewhere, Defendants OSADCHUK and KOVALEV, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to commit offenses against the United States, namely:

a. To knowingly access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, where the value of the information obtained exceeded $5,000, **in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)**; [ACT]

and **b.** To knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to intentionally cause damage without authorization to a protected computer, and where the offense did cause and, if completed, would have caused, loss aggregating $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least ten protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

78. In furtherance of the Conspiracy and to effect [***affect?***] its illegal objects, OSADCHUK, KOVALEV, and their co-conspirators committed the overt acts set forth in paragraphs 67 through 69 and 71 through 76, which are re-alleged and incorporated by reference as if fully set forth herein. All **in violation of Title 18, United States Code, Section 371**.

FORFEITURE ALLEGATION

79. Pursuant to Federal Rule of Criminal Procedure 32.2, notice is hereby given to Defendants that the United States will seek forfeiture as part of any sentence in the event of Defendants' convictions under Counts One, Ten, and Eleven of this Indictment. Pursuant to **Title 18, United** States Code, Sections 982(a)(2) and 1030(i), upon conviction of the offenses charged in Counts One and Eleven, Defendants (named) shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds obtained directly or indirectly as a result of such violation, and any personal property that was used or intended to be used to commit or to facilitate the commission of such offense.

Pursuant to **Title 18, United States Code, Section 982(a)(1)**, upon conviction of the offense charged in Count Ten, Defendants (named) shall forfeit to the United States any property, real or personal, involved in such offense, and any property traceable to such property. Notice is further given that, upon conviction, the United States intends to seek a judgment against each Defendant for a sum of money representing the property described in this paragraph, as applicable to each Defendant (to be offset by the forfeiture of any specific property). Substitute Assets

80. If any of the property described above as being subject to forfeiture, as a result of any act or omission of any Defendant --
a. cannot be located upon the exercise of due diligence;
b. has been transferred or sold to, or deposited with, a third party;
c. has been placed beyond the jurisdiction of the court;
d. has been substantially diminished in value;
or **e.** has been commingled with other property that cannot be subdivided without difficulty; it is the intent of the United States of America, **pursuant to Title 18, United States Code,** Section [END]

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 27 of 29 28
Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 28 **of 29**
Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 29 **of 29**

https://www.pbs.org/wgbh/americanexperience/features/truman-leaflets/

TRUMAN | **PRIMARY SOURCE**

Leaflets Warning Japanese of Atomic Bomb

Leaflets dropped on cities in Japan warning civilians about the atomic bomb, dropped c. August 6, 1945.

TO THE JAPANESE PEOPLE:
America asks that you take immediate heed of what we say on this leaflet.
-We are in possession of the most destructive explosion ever devised by man. A single one of our newly developed atomic bombs is actually the equivalent in explosive power to what 2000 of our giant B-29s can carry on a single mission. This awful fact is one for you to ponder and we solemnly assure you it is grimly accurate.
- We have just begun to use this weapon against your homeland. If you still have any doubt, make inquiry as to what happened to Hiroshima when just one atomic bomb fell on that city.
-Before using this bomb to destroy every resource of the military by which they are prolonging this useless war, we ask that you now petition the Emperor to end the war. Our president has outlined for you the thirteen consequences of an honorable surrender. We urge that you accept these consequences and begin the work of building a new, better and peace-loving Japan.
-You should take steps now to cease military resistance. Otherwise, we shall resolutely employ this bomb and all our other superior weapons to promptly and forcefully end the war. ---- **EVACUATE YOUR CITIES!**

ATTENTION JAPANESE PEOPLE. EVACUATE YOUR CITIES.
- Because your military leaders have rejected the thirteen part surrender declaration, two momentous events have occurred in the last few days. [article – declaration]

- The Soviet Union, because of this rejection on the part of the military has notified your Ambassador Sato that it has declared war on your nation. Thus, all powerful countries of the world are now at war with you.

- Also, because of your leaders' refusal to accept the surrender declaration that would enable Japan to honorably end this useless war, we have employed our atomic bomb.
- A single one of our newly developed atomic bombs is actually the equivalent in explosive power to what 2000 of our giant B-29s [aircraft] could have carried on a single mission. Radio Tokyo [A:B : "Tokyo Rose"] has told you that with the first use of this weapon of total destruction, Hiroshima was virtually destroyed.
- Before we use this bomb again and again to destroy every resource of the military by which they are prolonging this useless war, petition the emperor now to end the war. Our president [Truman] has outlined for you the thirteen consequences of an honorable surrender. We urge that you accept these consequences and begin the work of building a new, better, and peace-loving Japan.
- Act at once **or** we shall resolutely employ this bomb and all our other superior weapons to promptly and forcefully end the war.

EVACUATE YOUR CITIES.

(Source: Harry S. Truman Library, Miscellaneous historical document file, no. 258.)

Hhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh

A U.S. Air Force C-47 releases psychological warfare leaflets near Nha Trang, South Vietnam (August 1969)

https://commons.wikimedia.org/wiki/File:A_U.S._Air_Force_C-47_releases_psychological_warfare_leaflets_near_Nha_Trang,_South_Vietnam._-_NARA_-_542339.tif

Hhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh

[END]