UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

January 2025 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

VICTORIA EDUARDOVNA DUBRANOVA,
aka "Vika,"
aka "Sovasonya,"
[redacted]

FNU LNU,
aka "Cyber_1ce_Killer,"
aka "Commander,"
[redacted]

CR 2:25-cr-00577-FMO

I N D I C T M E N T

[18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(B)(ii) (c)(4)(A)(i)(I), (IV), (VI): Unauthorized Damage to a Protected Computer; 18 U.S.C. § 2: Aiding and Abetting; 18 U.S.C. § 1028A(a)(1): Aggravated Identity Theft; 18 U.S.C. § 1029(a)(3): Access Device Fraud; [redacted]; 18 U.S.C. §§ 981(a)(1)(C), 982, 1029, 1030, [redacted], and 28 U.S.C. § 2461(c): Criminal Forfeiture]

[redacted]

Defendants.

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

At all times relevant to this Indictment:

A. The Conspiracy and Defendants

1. CyberArmyofRussia_Reborn ("CARR") was a group that conducted cyberattacks, including distributed denial of service attacks, or "DDoS," and intrusions against critical infrastructure and other victims around the world, including victims within the Central District of California, in support of Russia's geopolitical interests.

2. "Z-Pentest" was an alternate group name employed by CARR members in furtherance of CARR's campaign of cyberattacks, with a focus on Supervisory Control and Data Acquisition ("SCADA") intrusions against public water systems and other critical infrastructure.

3. Defendants VICTORIA EDUARDOVNA DUBRANOVA, also known as ("aka") "Vika," aka "Sovasonya" ("DUBRANOVA"); [redacted] FNU LNU, aka "Cyber_1ce_Killer," aka "Commander"

("CYBER_ICE"); [redacted], whose photographs are attached as Exhibit A, were members of CARR.

4. Defendant DUBRANOVA was a resident of Ukraine.

5. Defendants [redacted] CYBER_ICE, [redacted] were residents of Russia.

6. The moniker "Cyber_1ce_Killer" was associated with at least one Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) officer.

7. Defendants [redacted] and co-conspirators believed that defendant CYBER_ICE was at all relevant times a Russian government agent and defendant [redacted] worked for the Federal Security Service of the Russian Federation (FSB).

8. At times, CARR had more than 100 members and more than 75,000 followers on Telegram. CARR's membership included juveniles, including individuals who have been fully identified by U.S. authorities.

B. Victims

9. Victim Meat Packing Facility, located in Vernon, California, is a meat packing and processing company.

C. Definitions

10. A DDoS attack is a type of computer-based attack in which an internet-connected victim computer is flooded with data and/or queries in such a manner to render it unable to communicate with other devices on the internet or to perform the services which it is intended to perform. Layer 4 DDoS attacks target the transport layer of the network. These attacks disrupt the communication protocols that transfer data between systems. Layer 7 DDoS attacks target the application layer of the network. These attacks exhaust resources of the target server.

11. Telegram is a cloud-based encrypted messaging service that allows users to post messages in public channels and message other users directly.

12. Supervisory Control and Data Acquisition ("SCADA") is a computer-based system that collects, analyzes, and displays real-time data from remote sites to monitor and control industrial processes. SCADA systems are commonly used in utilities, manufacturing, oil and gas production, and water and wastewater treatment facilities.

COUNT ONE

[18 U.S.C. § 371]

[ALL DEFENDANTS]

The Grand Jury hereby realleges and incorporates paragraphs 1 through 10 of the Introductory Allegations and Definitions of this Indictment.

A. OBJECTS OF THE CONSPIRACY

Beginning no later than November 2022, and continuing to the present, in Los Angeles County, within the Central District of California, and elsewhere, defendants DUBRANOVA, [redacted] CYBER_ICE, [redacted] and others known and unknown to the Grand Jury, knowingly conspired and agreed with each other to:

1. knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally cause damage without authorization to protected computers, and specifically:

a. to cause loss to one or more persons during a one-year period aggregating at least $5,000 in value, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I);

b. to cause a threat to public health or safety, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(IV); and

c. to cause damage affecting ten or more protected computers during a one-year period, in violation of Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI);

2. to tamper with, attempt to tamper with, or make a threat to tamper with, a public water system, in violation of 42 U.S.C. § 300i-1.

B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

The objects of the conspiracy were to be accomplished, in substance, as follows:

1. Defendant CYBER_ICE would instruct defendant [redacted] and other CARR leaders regarding what kinds of victims CARR should target with cyberattacks;

2. Defendant CYBER_ICE would finance CARR's access to various cybercriminal services, including subscriptions to DDoS-for-hire services;

3. Defendants DUBRANOVA, [redacted], and co-conspirators would research and identify potential victims for CARR cyberattacks;

4. Using private Telegram chats, defendants would coordinate cyberattacks against victims around the world, including critical infrastructure within the United States;

5. Defendants DUBRANOVA, [redacted] CYBER_ICE, [redacted], and co-conspirators would serve as administrators for various private Telegram chats and public Telegram channels associated with CARR, controlling the membership in the chats and moderating posts in the channels;

6. Defendants [redacted], and co-conspirators would conduct research on past and present CARR members to maintain intelligence regarding group members' allegiance to CARR;

7. For SCADA intrusion attacks, defendants [redacted], and co-conspirators would hack into victim public water systems and other SCADA systems, tampering with pumps and industrial equipment and intentionally causing damage;

8. For such SCADA intrusion attacks, defendants [redacted] and co-conspirators would take photos and videos documenting their cyberattacks;

9. For DDoS attacks, co-conspirators would use [redacted] "Killweb," CARR's DDoS script, and/or a paid subscription to a DDoS-for-hire service, to conduct cyberattacks against hundreds of victims around the world;

10. For DDoS attacks, co-conspirators would take photos documenting their cyberattacks and circulate links to co-conspirators showing that the DDoS victim website had been taken offline or otherwise degraded;

11. Defendants [redacted] and co-conspirators would send photos and videos documenting their cyberattacks to defendant DUBRANOVA, who would create promotional videos and media claiming credit for the cyberattacks;

12. Some of CARR's promotional media exaggerated its abilities and activities, in an effort to gain increased notoriety, raise funds, and recruit new members;

13. Defendants [redacted] and [redacted] would post DUBRANOVA's media to CARR's public Telegram channels, along with messages claiming credit for CARR's cyberattacks and at times providing purported explanations for why CARR had targeted the depicted victim(s) and aligning CARR with Russian geopolitical interests;

14. Defendants [redacted] and [redacted] would post messages to

CARR's public Telegram channels recruiting new members and soliciting resources to fund CARR's subscription to a paid DDoS-for-hire service;

15. Defendants [redacted] and co-conspirators would instruct CARR members to obtain hacked, stolen, or sensitive data, including personal identifying information, to be posted to CARR's public Telegram channels and/or shared with Russian government authorities, including the FSB.

C. OVERT ACTS

In furtherance of the conspiracy and to accomplish its objects, on or about the following dates, defendants DUBRANOVA, [redacted] CYBER_ICE, [redacted], and others, committed various overt acts within the Central District of California, and elsewhere, including but not limited to the following:

Administration, Promotion and Coordination of CARR

Overt Act No. 1: On March 10, March 13, April 28, and July 1, 2022, defendant CYBER_ICE emailed at least six individuals asking them to promote online CARR's posts claiming credit for cyberattacks.

Overt Act No. 2: On or before April 26, 2022, defendant CYBER_ICE created CARR's Instagram account, called "caofrussia."

Overt Act No. 3: On October 13, 2022, defendant CYBER_ICE created CARR's Twitter account, called "CAofRussia."

Overt Act No. 4: On December 23, 2022, defendant CYBER_ICE created CARR's public YouTube channel, with display name "CyberArmyofRussia."

Overt Act No. 5: On September 4, 2023, defendant [redacted]

directed a correspondent from a Russian news media outlet looking to interview CARR about its "recent operation against the Poles and the Balts" to contact defendant CYBER_ICE.

Overt Act No. 6: On or before October 20, 2023, defendant CYBER_ICE created a private Telegram chat including defendants [redacted], and other co-conspirators, to facilitate their coordination of CARR cyberattacks.

Overt Act No. 7: On December 12 and 16, 2023, defendants [redacted], and co-conspirators recruited "specialists in DDoS" to join CARR and directed anyone interested to contact defendant [redacted] on Telegram.

Overt Act No. 8: On December 21, 2023, defendants [redacted] and [redacted] instructed CARR members to conduct online research for individuals expressing support for the individual who killed a Russian military blogger in St. Petersburg in April 2023. Defendant [redacted] instructed CARR members to send such information to defendant [redacted] whom she described as an "FSB Captain" and "our FSB colleague," so that defendant [redacted] could initiate "investigative actions" and "criminal cases" against those individuals.

Overt Act No. 9: On an unknown date, defendant [redacted] became an administrator of a chat where CARR members coordinated cyberattacks.

Overt Act No. 10: On January 20, 2024, defendant [redacted] created a private chat on Telegram for CARR's "DDoS squad" and invited defendant [redacted] to join the group.

Overt Act No. 11: Prior to June 24, 2024, defendant DUBRANOVA managed a paid subscription to a social media marketing service

designed to amplify CARR's public Telegram profile.

Overt Act No. 12: On July 20, 2024, defendant [redacted] sent a message to CARR co-conspirators instructing them to work faster toward an unidentified CARR cyberattack.

Overt Act No. 13: Between September 4, 2024, and October 31, 2024, defendant [redacted] and co-conspirators referred to defendant CYBER_ICE as "Commander" and characterized defendant CYBER_ICE as a Russian government operative.

Overt Act No. 14: On September 10, 2024, defendant [redacted] instructed co-conspirators regarding effective coding methods to circumvent network security protocols.

Overt Act No. 15: On September 27, 2024, defendant DUBRANOVA created a private Telegram chat called "Besedka" and included defendants [redacted], where these defendants and other CARR members shared exploits, discussed victim targeting, and coordinated cyberattacks against dozens of victims.

Overt Act No. 16: On September 30, 2024, defendant [redacted] directed co-conspirators to focus CARR cyberattacks on "all countries unfriendly to the Russian Federation," including Taiwan, Finland, Poland, and the United States, but to avoid attacking Serbia and Hungary.

Overt Act No. 17: On an unknown date before October 17, 2024, defendant [redacted] sent money to defendant [redacted] to fund CARR's activities.

Overt Act No. 18: On October 20, 2024, defendant DUBRANOVA created a public account on X called "Z Pentest," where CARR regularly published photos and videos claiming credit for

cyberattacks.

Overt Act No. 19: On October 24, 2024, defendants [redacted] and DUBRANOVA researched fundraising to cover the cost of CARR's subscription with an illicit DDoS service.

Overt Act No. 20: On November 7, 2024, defendant [redacted] coached defendant DUBRANOVA regarding how to flee from Ukraine to Russia.

Overt Act No. 21: On November 7, 2024, defendant [redacted] provided defendant DUBRANOVA with the contact information, including name and phone number, of an FSB agent working in the "Anti-Terrorism Department" located in Krasnodar, Russia.

Overt Act No. 22: On November 7, 2024, defendant [redacted] sent a private message to defendant DUBRANOVA informing her that an FSB sanctioned travel paper had been sent to Belarussian border patrol officers to help facilitate defendant DUBRANOVA's flight to Russia through Belarus.

DDoS Targeting and Attacks

Overt Act No. 23: On November 8, 2022, defendant [redacted] and co-conspirators conducted a DDoS attack against the Secretary of State website of a U.S. state, causing the website to be periodically inaccessible for approximately ten hours on election day in the 2022 midterm election.

Overt Act No. 24: On February 2, 2023, and November 23, 2023, defendant [redacted] researched DDoS cyberattack methods and tools.

Overt Act No. 25: On June 21, 2023, defendant [redacted] saved login credentials to her personal email account for a CARR account on a DDoS subscription service called Stresser.tech.

Overt Act No. 26: On September 23, 24, and 26, 2023, defendant

[redacted] and co-conspirators conducted DDoS attacks against several Moldovan airport websites.

Overt Act No. 27: On September 29, 2023, defendants [redacted] and [redacted] coordinated a DDoS attack against a Ukrainian web portal designed to provide food, clothes, medicine, and other emergency services to Ukrainian citizens affected by the war.

Overt Act No. 28: On and between October 16-18, 2023, defendants [redacted], and co-conspirators conducted a series of DDoS attacks against Romanian websites.

Overt Act No. 29: On December 18, 2023, defendant CYBER_ICE informed co-conspirators [redacted], and others, that he was going to submit payment for CARR's DDoS account later that day.

Overt Act No. 30: On January 10, 2024, defendant [redacted] and co-conspirators conducted a DDoS attack against the website for the Northwest Missouri Regional Airport.

Overt Act No. 31: On February 2, 2024, defendant [redacted] and co-conspirators conducted research on the website for the U.S. Department of Veterans Affairs to assess a possible DDoS attack.

Overt Act No. 32: On February 6, 2024, defendant CYBER_ICE instructed co-conspirators not to "touch the stressor [DDoS service] until I give the command."

Overt Act No. 33: On February 23, 2024, defendant [redacted] and co-conspirators conducted a DDoS attack against the website for a University in Alaska.

Overt Act No. 34: On March 27, 2024, defendant CYBER_ICE instructed defendant [redacted] that his organization would no longer fund CARR's DDoS efforts and that defendant [redacted] should instead focus CARR on getting "information for the war, namely, to destroy

the information resources and systems of the enemy."

Overt Act No. 35: On March 28, 2024, defendant CYBER_ICE instructed defendant [redacted] that DDoS "was closed" for CARR "because it does not cause any damage," and because "[i]f we hit Kyiv with missiles, we won't need DOS."

Overt Act No. 36: On April 6, 2024, defendant [redacted] sent a private message to the administrator of Stresser.tech, an illicit DDoS service, coordinating payment and conversion from Rubles for CARR's account on Stresser.tech.

Overt Act No. 37: On April 12, 2024, defendant [redacted] and co-conspirators conducted research on the website for the U.S. embassy in Ljubljana to assess a possible DDoS attack.

Overt Act No. 38: On an unknown date prior to April 13, 2024, defendant [redacted] developed a DDoS script called CA_DDoS and also known as "Killweb," which a co-conspirator later posted to CARR's public Telegram channel and shared privately among CARR members as a tool to conduct DDoS attacks against victims selected by CARR members.

Overt Act No. 39: On April 21, 2024, defendant [redacted] and co-conspirators conducted a DDoS attack against the website of an energy company located in Pennsylvania.

Overt Act No. 40: On May 5, 2024, defendant [redacted] and co-conspirators conducted a DDoS attack against the websites for U.S. nuclear regulatory institutes.

Overt Act No. 41: On August 21, 2024, defendant [redacted] conducted a DDoS attack against a Ukrainian government website, circulating evidence of the attack to co-conspirators and proposing text to accompany a public post claiming credit for the cyberattack

on CARR's public Telegram channel.

Overt Act No. 42: On August 22, 2024, defendant [redacted] instructed co-conspirators regarding how to install "Killweb," CARR's DDoS script.

Overt Act No. 43: On August 22, 2024, defendant [redacted] and co-conspirators conducted DDoS attacks against websites of several blood donation organizations in Ukraine.

Overt Act No. 44: On August 30, 2024, defendant [redacted] conducted a DDoS attack against a Ukrainian news website.

Overt Act No. 45: On September 17, 2024, defendant [redacted] instructed co-conspirators regarding DDoS attack methods, including Layer 4 and Layer 7 DDoS attacks, and CARR's DDoS script "CA_DDoS."

Overt Act No. 46: On September 27, 2024, defendant [redacted] instructed co-conspirators to conduct DDoS attacks against six Austrian financial and transportation websites.

Overt Act No. 47: On September 27, 2024, defendant [redacted] and co-conspirators conducted a DDoS attack against the website of a Ukrainian government institution.

Overt Act No. 48: On September 29, 2024, defendant [redacted] and co-conspirators conducted DDoS attacks against the website and server hosting the mobile application of an Uzbekistani airline.

Overt Act No. 49: On October 1, 2024, co-conspirators conducted a DDoS attack against websites for a Taiwanese news outlet, the Taiwanese military, and the city council of a Ukrainian city.

Overt Act No. 50: On October 2, 2024, defendant [redacted] and co-conspirators conducted DDoS attacks against an application for cryptocurrency investing.

Overt Act No. 51: On October 7, 2024, defendant [redacted]

provided detailed instructions to co-conspirators regarding how to use a virtual private network to conduct DDoS attacks.

Overt Act No. 52: On October 7, 2024, co-conspirators conducted a DDoS attack against a Ukrainian robotics website.

Overt Act No. 53: On October 8, 2024, defendant [redacted] instructed co-conspirators to identify targets for DDoS attacks in Belgium and Japan.

Overt Act No. 54: On October 9, 2024, defendant [redacted] instructed co-conspirators to conduct DDoS attacks against targets in Moldova because of upcoming Moldovan elections.

Overt Act No. 55: On October 9, 2024, defendant [redacted] conducted a DDoS attack against a Ukrainian government website.

Overt Act No. 56: On October 9, 2024, defendant [redacted] conducted a DDoS attack against the citizen portal for citizens of Brussels, Belgium.

Overt Act No. 57: On October 18, 2024, defendant [redacted] researched the website for the United States Department of Defense as a possible target for a CARR DDoS attack.

Overt Act No. 58: On October 24, 2024, defendant DUBRANOVA created a video defendant [redacted] later posted to CARR's public Telegram channel that described how CARR was going to engage in a campaign of DDoS attacks against U.S. election-related websites in advance of the November 2024 U.S. elections.

Overt Act No. 59: On October 25, 2024, defendant [redacted] and co-conspirators conducted DDoS attacks against the website for a Ukrainian academic institution.

Overt Act No. 60: On October 25, 28, and 29, 2024, defendant [redacted] and co-conspirators conducted DDoS attacks against

election-related government websites in Florida.

Overt Act No. 61: On October 26, 2024, defendant [redacted] proposed potential cyberattack targets, including targets in the Bahamas, to defendant [redacted] and other co-conspirators.

Overt Act No. 62: On October 27, 2024, co-conspirators conducted a DDoS attack against a Bahamian government website.

Overt Act No. 63: On October 28, 2024, co-conspirators conducted a DDoS attack against the government website of a county in Florida.

Overt Act No. 64: On October 30, 2024, co-conspirators conducted a DDoS attack against the website of a Texas government agency.

Overt Act No. 65: On November 29, 2024, defendant [redacted] and co-conspirators conducted a DDoS attack against a Ukrainian military logistics company.

Overt Act No. 66: On December 4, 2024, defendant [redacted] and co-conspirators conducted a DDoS attack against the website for a public toll road in the United Kingdom.

Overt Act No. 67: On November 5, 2024, defendant [redacted] and co-conspirators conducted DDoS attacks against the websites of South Korean government agencies.

SCADA Targeting and Attacks

Overt Act No. 68: In September and October 2023, defendant [redacted] researched SCADA attack strategies and drafted a document entitled "Manual," in which defendant [redacted] provided detailed instructions to teach other CARR members how to conduct cyberattacks against SCADA systems.

Overt Act No. 69: On November 23, 2023, defendant [redacted]

and co-conspirators compromised a dairy processing facility in California, tampering with fans and misters, and altering passwords.

Overt Act No. 70: On January 18, 2024, defendant [redacted] and co-conspirators compromised a public water system in Texas, tampering with the set points of the water storage tanks and triggering 22 wells, causing an unknown volume of drinking water to overflow.

Overt Act No. 71: On January 18, 2024, defendant [redacted] and co-conspirators compromised another public water system in Texas, changing passwords, tampering with storage settings, and causing an unknown volume of drinking water to overflow.

Overt Act No. 72: In February 2024, defendant [redacted] and co-conspirators compromised a car wash facility in Florida, tampering with the position of the car wash components.

Overt Act No. 73: On April 21, 2024, defendant [redacted] and co-conspirators attempted to hack a victim oil and gas facility in Texas. The hack was not successful.

Overt Act No. 74: On April 23, 2024, defendant [redacted] posted links on CARR's public Telegram channel to news reports describing CARR's cyberattack against a water facility in Texas, and claimed credit for these attacks.

Overt Act No. 75: On July 24, 2024, defendant [redacted] and co-conspirators compromised a landfill water treatment installation in Pennsylvania, tampering with pumps and the levels of parasitic acid contamination.

Overt Act No. 76: On and between August 14-17, 2024, defendant [redacted] and co-conspirators compromised an oil facility in Oklahoma.

Overt Act No. 77: On and between August 28-30, 2024, defendant [redacted] and co-conspirators compromised another public water system in Texas, altering pump set points and shutting down the system, causing approximately 200,000 gallons of water to overflow.

Overt Act No. 78: On September 18, 2024, defendant [redacted] and co-conspirators compromised a victim public water system in Indiana, activating all pumps and tampering with settings.

Overt Act No. 79: On September 27, 2024, defendant [redacted] sent co-conspirators a password associated with a CARR SCADA victim.

Overt Act No. 80: On September 28, 2024, defendant [redacted] instructed co-conspirators to turn off a sensor and turn on a pump during an attempted cyberattack against a SCADA system.

Overt Act No. 81: On October 3, 2024, defendant [redacted] sent co-conspirators login credentials for a victim server he had hacked.

Overt Act No. 82: On October 7, 2024, defendant [redacted] sent co-conspirators an IP address and corresponding password for another victim server.

Overt Act No. 83: On October 10, 2024, defendant [redacted] watched training videos defendant [redacted] had sent him regarding how to conduct cyberattacks against SCADA victims.

Overt Act No. 84: On October 18, 2024, defendant [redacted] asked defendant [redacted] to share access to a tool defendant [redacted] used to identify potential SCADA victims.

Overt Act No. 85: On October 31, 2024, defendants [redacted] and [redacted] compromised a victim oil and gas company in Colorado, depleting onsite chemical supplies by increasing chemical injection rates into oil wells.

Overt Act No. 86: On October 31, 2024, defendant [redacted]

instructed defendant [redacted] to raise a temperature and disarm alarm settings at the victim oil and gas company so that the "probability of a real accident will be higher."

Overt Act No. 87: On October 31, 2024, defendant DUBRANOVA created a video defendant [redacted] later posted to CARR's public Telegram channel, depicting defendant [redacted] intrusion of the victim oil and gas company.

Overt Act No. 88: On November 1, 2024, defendant [redacted] sent co-conspirators the website for the Victim Meat Packing Facility.

Overt Act No. 89: On November 1, 2024, defendant [redacted] compromised the Victim Meat Packing Facility, shutting off refrigeration and spoiling more than two thousand pounds of meat, and triggering an ammonia leak, requiring the facility to be evacuated for more than four hours, resulting in more than $5,000 in damages.

Overt Act No. 90: On November 1, 2024, defendant [redacted] sent defendant DUBRANOVA video files depicting his intrusion of the Victim Meat Packing Facility.

Overt Act No. 91: On November 1, 2024, defendant [redacted] sent defendant DUBRANOVA a message in reference to the intrusion of Victim Meat Packing Facility stating, "alarm blue code," to which defendant DUBRANOVA replied that she would generate a video of the cyberattack within 40 minutes.

Overt Act No. 92: On November 1, 2024, defendant DUBRANOVA edited the video file depicting defendant [redacted] intrusion of the Victim Meat Packing Facility (the "Meat Packing Video") and claiming credit for damaging the victim's system and spoiling "tons of finished meat products."

Overt Act No. 93: On November 1, 2024, defendant [redacted] posted the Meat Packing Video to CARR's public Telegram channel.

Overt Act No. 94: On and between November 3-4, 2024, defendant [redacted] compromised a children's water park in the Netherlands, tampering with temperature and other control settings including chlorination levels.

Identity and Data Theft

Overt Act No. 95: On September 14, 2023, defendant CYBER_ICE sent defendant [redacted] a list of 30 usernames and corresponding passwords belonging to Ukrainian victims and instructed her to post the data on CARR's Telegram channel.

Overt Act No. 96: On April 21, 2024, defendant DUBRANOVA conducted pre-operational reconnaissance by visiting the website of an American contracting company in Virginia. CARR later accessed, without authorization, that American contracting company, exfiltrating confidential documents from the victim's system and posting them to CARR's public channel and targeting the victim's website with DDoS attacks.

Overt Act No. 97: On September 23, 2024, defendant DUBRANOVA sold defendant [redacted] stolen database information containing personal identifying information, including driver's licenses, phone numbers, emails, and passwords, belonging to thousands of victims in Ukraine, Romania, and Moldova.

Overt Act No. 98: On October 11, 2024, defendant [redacted] sent co-conspirators a list of 23 IP addresses with passwords corresponding to computer systems that defendant [redacted] and co-conspirators could access without authorization.

Overt Act No. 99: On December 3, 2024, defendant [redacted]

publicly posted dozens of account credentials, including emails and passwords, for accounts on various services, including Disney Plus.

COUNT TWO

[18 U.S.C. §§ 1030(a)(5)(A), (b), (c)(4)(B)(i), (c)(4)(A)(i)(I), (IV), 2(a)]

[DEFENDANTS DUBRANOVA, [redacted] CYBER ICE, [redacted]]

On or about November 1, 2024, in Los Angeles County, within the Central District of California, and elsewhere, defendants VICTORIA EDUARDOVNA DUBRANOVA, also known as ("aka") "Vika," aka "Sovasonya"; [redacted] FNU LNU, aka "Cyber_1ce_Killer," aka "Commander"; [redacted] each aiding and abetting the others, knowingly caused the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally and without authorization caused damage and attempted to cause damage by impairing the integrity and availability of data, programs, systems, and information on protected computers, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), belonging to a meat packing and processing company located in Vernon, California, and did aid, abet, counsel, command, induce, or procure others to do so, thereby causing and attempting to cause loss to one or more persons during a one-year period aggregating at least $5,000 in value, and

causing and attempting to cause a threat to public health or safety.

COUNT THREE

[18 U.S.C. § 1029(a)(3)]

[DEFENDANT DUBRANOVA]

On or about November 9, 2024, in Los Angeles County, within the Central District of California, and elsewhere, defendant VICTORIA EDUARDOVNA DUBRANOVA, also known as ("aka") "Vika," aka "Sovasonya" ("DUBRANOVA") knowingly and with intent to defraud, possessed at least fifteen unauthorized access devices, as defined in Title 18, United States Code, Sections 1029(e)(1) and (3), namely, more than fifteen victim business website credentials and individual email account credentials, all belonging to persons other than defendant DUBRANOVA, with said possession affecting interstate and foreign commerce.

COUNT FOUR

[18 U.S.C. § 1028A(a)(1)]

[DEFENDANT DUBRANOVA]

On or about November 9, 2024, in Los Angeles County, within the Central District of California, and elsewhere defendant VICTORIA EDUARDOVNA DUBRANOVA, also known as ("aka") "Vika," aka "Sovasonya" ("DUBRANOVA") knowingly transferred, possessed, and used, and willfully caused to be transferred, possessed, and used, without lawful authority, a means of identification that defendant DUBRANOVA knew belonged to another person, during and in relation to the offense of access device fraud, a felony violation of Title 18, United States Code, Section 1029, as charged in Count Three of this Indictment.

COUNT FIVE

[redacted]

FORFEITURE ALLEGATION ONE

[18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c)]

1. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), in the event of any defendant's conviction of the offense set forth in Count One of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds traceable to the offenses; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), any defendant so convicted shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph or any portion thereof (a) cannot be located upon the exercise of due diligence; (b) has been transferred, 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 divided without difficulty.

FORFEITURE ALLEGATION TWO

[18 U.S.C. §§ 982 and 1030]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Sections 982(a)(2) and 1030, in the event of any defendant's conviction of the offenses set forth in either of Counts Two or Three of this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

a. All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense;

b. Any property used or intended to be used to commit the offense; and

c. To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i), any defendant so convicted shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence;

//

(b) has been transferred, 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 divided without difficulty.

FORFEITURE ALLEGATION THREE

[18 U.S.C. §§ 982 and 1029]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Sections 982(a)(2) and 1029, in the event of the defendant's conviction of the offense set forth Count Four of this Indictment.

2. The defendant, if so convicted, shall forfeit to the United States of America the following:

(a) All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense;

(b) Any personal property used or intended to be used to commit the offense; and

(c) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1029(c)(2), the defendant, if so convicted, shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of the defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence;

//

(b) has been transferred, 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 divided without difficulty.

A TRUE BILL

/S/
Foreperson

BILAL A. ESSAYLI
United States Attorney

DAVID T. RYAN
Assistant United States Attorney
Chief, National Security Division

KHALDOUN SHOBAKI
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section

AARON FRUMKIN
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section

ANGELA MAKABALI
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section

ALEXANDER GORIN
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section

Exhibit A

VICTORIA EDUARDOVNA DUBRANOVA

aka "Vika"

aka "Sovasonya"

[redacted]

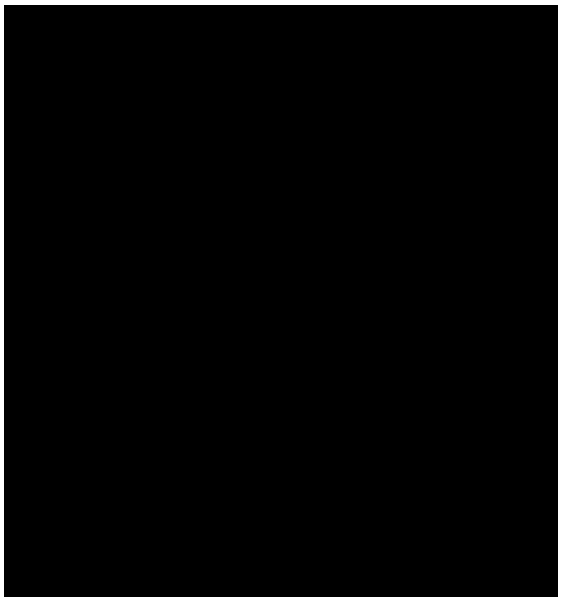
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]



FNU LNU

aka “Cyber 1ce Killer”

aka “Commander”