IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	Case No.: 24-mj-1395
	)	
v.	)	**Filed Under Seal**
	)	
CERTAIN DOMAINS	)	

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [redacted] being duly sworn, hereby declare as follows:

INTRODUCTION

1. I make this affidavit in support of a warrant for the seizure of 32 internet domains (the "SUBJECT DOMAINS") that have been used by the Russian government and Russian government-sponsored actors to engage in foreign malign influence campaigns colloquially referred to as "Doppelganger," in violation of U.S. money laundering and criminal trademark laws. As set forth below, since at least 2022, under the direction and control of the Russian Presidential Administration, and in particular Sergei Vladilenovich Kiriyenko ("KIRIYENKO"), the Russian companies Social Design Agency ("SDA"), Structura National Technology ("STRUCTURA"), ANO Dialog, have used, among others, the SUBJECT DOMAINS, which include "cybersquatted" domains[1] impersonating legitimate news entities and unique media brands created by Doppelganger, to covertly spread Russian government propaganda. As reflected in SDA's notes from strategy meetings with KIRIYENKO and other Presidential Administration officials, SDA project proposals, and other SDA records obtained during the course of the investigation, some of which are attached as exhibits hereto, these actors designed the content of

[1] Based on my training and experience, I know that cybersquatting is a method of registering a domain intended to mimic another person or company's domain. Cybersquatting is used to trick Internet users into believing they are visiting the legitimate person or company's website.

such propaganda to, *inter alia*, reduce international support for Ukraine, bolster pro-Russian policies and interests, and influence voters in the U.S. and foreign elections without identifying, and in fact purposefully obfuscating, the Russian government or its agents as the source of the content. Among the methods Doppelganger used to drive viewership to the cybersquatted and unique media domains were the deployment of "influencers" worldwide, paid social media advertisements (in some cases created using artificial intelligence tools), and the creation of fake social media profiles posing as U.S. (or other non-Russian) citizens to post comments on social media platforms with links to the cybersquatted domains, all of which attempted to trick viewers into believing they were being directed to a legitimate news media outlet's website.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I became a Special Agent in January 2017 when I was assigned to the Philadelphia Division's Counterintelligence Squad. As part of the Counterintelligence Squad, my duties include, among other things, the investigation of foreign malign influence, espionage, and foreign intelligence activities against the United States. I have successfully completed the Counterintelligence Operations Course offered by the FBI Counterintelligence Training Center, where I was exposed to a variety of counterintelligence techniques, cases, and exercises. I have participated in the execution of numerous search warrants involving electronic evidence, among other investigative techniques.

3. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under authority of the United States. I have attended multiple training courses related to managing counterintelligence and espionage investigations. I have also been involved in various types of electronic and physical surveillance, the execution of search warrants, and interviews of crime victims, witnesses, and subjects. Where I assert that an

event took place on a particular date or at a particular time, I am asserting that it took place on or about the date or at or near the time asserted. Similarly, where I assert that an event took place a certain number of times, I am asserting that the event took place approximately the number of times asserted. Likewise, when I assert that a transaction involved a certain amount of money, I am asserting that the transaction involved approximately that amount of money.

4. The facts in this affidavit come from my personal observations, my training and experience, records seized pursuant to search warrants or obtained through legal process, and information learned from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. As set forth below, there is probable cause to believe that the SUBJECT DOMAINS,[2] *see* Attachments A-1 through A-9, are property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956(a)(2)(A) (international promotional money laundering) and 1956(h) (conspiracy to commit same) and/or property used, or intended to be used, in any manner or part to facilitate violations of § 2320(a)(1) (trafficking in counterfeit goods or services) (collectively, the "SUBJECT OFFENSES"). In particular, the investigation has revealed that the SUBJECT DOMAINS have been purchased from U.S. registries or registrars by individuals abroad who are working under the direction and control of the Russian government, and in particular KIRIYENKO, including Ilya Gambashidze ("GAMBASHIDZE"), SDA, Nikolai Tupikin ("TUPIKIN"), and STRUCTURA, which have been sanctioned by the U.S. government and designated as SDNs, along with ANO Dialog, TABAK, and others, to advance their interests and the interests of the Russian government, thereby causing U.S. persons to unwittingly provide

[2] References to the individual SUBJECT DOMAINS in this affidavit will be denoted by **bolded** text.

goods and services to and for the benefit of one or more of the aforementioned SDNs, in violation of the International Emergency Economic Powers Act ("IEEPA"). As noted above, the foreign malign influence effort described herein and carried out by SDA, STRUCTURA, and ANO Dialog is colloquially referred to as "Doppelganger."

6. Because the SUBJECT DOMAINS represent property involved in a scheme to violate U.S. money laundering laws, they are subject to seizure, and therefore subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1).

7. In addition, as a secondary basis for seizure and forfeiture, a subset of the SUBJECT DOMAINS represent property used, or intended to be used, to commit or facilitate the commission of Trafficking in Counterfeit Goods or Services (e.g., trademark infringement), in violation of 18 U.S.C. § 2320, and therefore are subject to forfeiture pursuant to 18 U.S.C. § 2323(a)(1)(B) and (b)(1).

8. The procedure by which the government will seize the SUBJECT DOMAINS is described in Attachments A-1 through A-9 hereto and below.

TECHNICAL INFORMATION

9. Based on my training and experience and information learned from others, I am aware of the following:

10. Internet Protocol Address: An Internet Protocol ("IP") address is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address—it enables computers connected to the Internet to properly route traffic to

each other. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers ("ISP").

11. Domain Name: A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (*e.g.*, "justice.gov"). Domain names are composed of one or more parts, or "labels," delimited by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the "top-level domain" ("TLD") (e.g., ".com" or ".gov"). To the left of the TLD is the "second-level domain" ("SLD"), which is often thought of as the "name" of the domain. The SLD may be preceded by a "third-level domain," or "subdomain," which often provides additional information about various functions of a server or delimits areas under the same domain. For example, in "www.justice.gov," the TLD is ".gov," the SLD is "justice," and the subdomain is "www," which indicates that the domain points to a web server.

12. Domain Name System: The Domain Name System ("DNS") is the way that Internet domain names are located and translated into IP addresses. DNS functions as a phonebook for the Internet, allowing users to find websites and other resources by their names while translating them into the IP addresses that their computers need to locate them.

13. Domain Name Servers: Domain Name Servers ("DNS servers") are devices or programs that convert, or resolve, domain names into IP addresses when queried by web browsers or other DNS "clients."

14. Registrar: A registrar is a company that has been accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN") or a national country code top-level domain (such as .uk or .ca) to register and sell domain names. Registrars act as intermediaries

between registries and registrants. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

15. Registry: A domain name registry is an organization that manages top-level domains, including by setting usage rules and working with registrars to sell domain names to the public. For example, the registry for the ".com" and ".net" top-level domains is VeriSign, Inc., which is headquartered at 12061 Bluemont Way, Reston, Virginia.

16. Registrant: A registrant is the person or entity that holds the right to use a specific domain name sold by a registrar. Most registrars provide online interfaces that can be used by registrants to administer their domain names, including to designate or change the IP address to which their domain name resolves. For example, a registrant will typically "point" their domain name to the IP address of the server where the registrant's website is hosted.

17. Virtual Private Network: "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network ("WAN") link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

18. Virtual Private Server: "VPS" means a virtual private server. A VPS acts as an isolated, virtual environment on a physical server operated by a provider. VPS hosting providers

use virtualization technology to split a single physical machine into multiple private server environments that share resources. Hosting companies maintain server computers connected to the Internet. A server is a computer that provides services to other computers. Customers may use those servers for various functions, depending on the services offered by the hosting company. Some hosting companies offer simple cloud storage, which allows users to store files, much like an external hard drive, and share or edit those files with other persons. Other hosting companies allow users to operate and host websites on the Internet. Other hosting companies enable users to operate a virtual private server, which allows the customer to run virtualized operating systems from their computer over the Internet. Each VPS runs on a physical server but has its own self-contained disk space, bandwidth, processor allocation, memory, and operating system. Multiple VPS's can run on one physical server. A hosting company can offer any combination of the above. In the case of a VPS, each subscriber to a hosting company's services has full administrative control over the subscriber's VPS, which enables the subscriber to choose to install software from a menu the hosting company offers or store and run the subscriber's own software.

19. Who.is: A "Who.is" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Who.is record for a particular IP address or domain name will list a range of IP addresses that the particular IP address falls within and the entity responsible for that IP address range and domain name. For example, a Who.is record for the domain name XYZ.COM might list an IP address range of 12.345.67.0-12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0-12.345.67.99.

INTERNATIONAL MONEY LAUNDERING AND IEEPA

20. Title 18, United States Code, Section 1956(a)(2)(A) (international promotional money laundering) prohibits, in relevant part, the transportation, transmission, or transfer of funds or monetary instruments from or through a place outside of the United States to a place within the United States, with the intent to promote the carrying on of specified unlawful activity. Pursuant to 18 U.S.C. § 1956(c)(7)(D), specified unlawful activity includes violations of IEEPA, which is codified at 50 U.S.C. § 1701 *et seq.* In addition, any person who "conspires to commit any offense defined in [Section 1956]" shall also be subject to criminal prosecution. *See* 18 U.S.C. § 1956(h).

IEEPA

21. IEEPA authorizes the President of the United States to impose economic sanctions in response to an unusual and extraordinary threat to the national security, foreign policy, or economy of the United States. Pursuant to that authority, the President may declare a national emergency through an Executive Order to deal with that threat.

22. IEEPA makes it a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any order, license, regulation, or prohibition issued pursuant to IEEPA. 50 U.S.C. § 1705(a), (c).

23. In 2014, pursuant to his authorities under IEEPA, the President issued Executive Order 13660, which declared a national emergency with respect to the situation in Ukraine. To address this national emergency, the President blocked all property and interest in property that were then or thereafter came within the United States or the possession or control of any United States person, of individuals determined by the Secretary of the Treasury to meet one or more enumerated criteria. These criteria include, but are not limited to, individuals determined to be responsible for or complicit in, or who engage in, actions or policies that threaten the peace,

security, stability, sovereignty, or territorial integrity of Ukraine; or who materially assist, sponsor, or provide financial, material, or technological support for, or goods or services to individuals or entities engaging in such activities. Executive Order 13660 prohibits, among other things, transferring, paying, exporting, withdrawing, or otherwise dealing in any interest in property in the United States owned by a person whose property and interests in property are blocked (a "blocked person"), as well as the making of any contribution or provision of funds, goods, or services by a United States person, to, or for the benefit of a blocked person, and the receipt of any contribution or provision of funds, goods, or services by a United States person from any such blocked person.

24. The President on multiple occasions has expanded the scope of the national emergency declared in Executive Order 13660, including through: (1) Executive Order 13661, issued on March 16, 2014, which addresses the actions and policies of the Russian Federation with respect to Ukraine, including the deployment of Russian Federation military forces in the Crimea region of Ukraine; and (2) Executive Order 13662, issued on March 20, 2014, which addresses the actions and policies of the Government of the Russian Federation, including its purported annexation of Crimea and its use of force in Ukraine. Executive Orders 13660, 13661, and 13662 are collectively referred to as the "Ukraine-Related Executive Orders." On February 21, 2022, the President again expanded the scope of the national emergency, finding that the Russian Federation's purported recognition of the so-called Donetsk People's Republic and Luhansk People's Republic regions of Ukraine contradicts Russia's commitments under the Minsk agreements and threatens the peace, stability, sovereignty, and territorial integrity of Ukraine.

25. The Ukraine-Related Executive Orders authorized the Secretary of the Treasury to take such actions, including the promulgation of rules and regulations, and to employ all powers

granted to the President under IEEPA, as may be necessary to carry out the purposes of those orders. The Ukraine-Related Executive Orders further authorized the Secretary of the Treasury to redelegate any of these functions to other offices and agencies of the United States Government.

26. To implement the Ukraine-Related Executive Orders, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued certain Ukraine-Related Sanctions Regulations. These regulations incorporate by reference the prohibited transactions set forth in the Ukraine-Related Executive Orders. *See* 31 C.F.R. § 589.201. The regulations also provide that the names of persons designated directly by the Ukraine-Related Executive Orders, or by OFAC pursuant to the Ukraine-Related Executive Orders, whose property and interests are therefore blocked, are published in the Federal Register and incorporated into the SDNs and Blocked Persons List (the "SDN List"), which is published on OFAC's website. *Id. at* note 2.

27. Among other things, E.O. 13661 prohibits United States persons from transferring, paying, exporting, withdrawing, or otherwise dealing in the property or interests in property of a designated person identified on the SDN List. E.O. 13661 § 1. These prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of, a designated person identified on the SDN List. E.O. 13661 § 4. Any transaction that evades or avoids, or has the purpose of evading or avoiding, or causes a violation of E.O. 13661 is further prohibited. *Id*. § 5. "United States person" is defined as a United States citizen, permanent resident alien, entity organized under the law of the United State or any jurisdiction within the United States (including foreign branches), or any person in the United States. 31 C.F.R. § 6(c).

28. On March 2, 2021, OFAC announced sanctions designating seven Russian government officials, including First Deputy Chief of Staff of the Presidential Executive Office Sergei KIRIYENKO, pursuant to E.O. 13661 for serving as officials of the Russian government.

In so doing, OFAC noted that KIRIYENKO "is reported to be President Putin's 'domestic policy curator.'"

29. On April 15, 2021, pursuant to his authorities under IEEPA, the President issued E.O.14024, which declared a national emergency with respect to:

> [H]armful foreign activities of the Government of the Russian Federation—in particular, efforts to undermine the conduct of free and fair democratic elections and democratic institutions in the United States and its allies and partners; to engage in and facilitate malicious cyber-enabled activities against the United States and its allies and partners; to foster and use transnational corruption to influence foreign governments; to pursue extraterritorial activities targeting dissidents or journalists; to undermine security in countries and regions important to United States national security; and to violate well-established principles of international law, including respect for the territorial integrity of states—constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

Similar to the Ukraine-Related Executive Orders, E.O. 14024 blocked the property and interests in property of persons determined by the Secretary of the Treasury or the Secretary of State to meet one or more enumerated criteria and prohibited, among other things, the provision of funds, goods, or services by, to or for the benefit of such a designated person. To implement E.O. 14024, OFAC issued the "Russian Harmful Foreign Activities Sanctions Regulations," 31 C.F.R. Part 587. Persons designated pursuant to E.O. 14024 are identified on the SDN List. *Id.* at note 1.

30. On February 22, 2022, OFAC announced additional sanctions against KIRIYENKO pursuant to E.O. 14024. With respect to KIRIYENKO, OFAC again described KIRIYENKO as "the First Deputy Chief of Staff of the Presidential Office" and reportedly "Putin's domestic policy curator." OFAC noted KIRIYENKO had previously "served as the Prime Minister of the Russian Federation and as the General Director of Rosatom State Atomic Energy Corporation" and had been previously designated pursuant to E.O. 13661 in March 2021. Pursuant to E.O. 14024, OFAC redesignated KIRIYENKO for being or having been a leader, official, senior executive officer, or member of the board of directors of the Russian government.

31. On March 20, 2024, OFAC designated GAMBASHIDZE and TUPIKIN, as well as SDA and STRUCTURA, pursuant to Executive Order 14024 for "being or having been a leader, official, senior executive officer, or member of the board of directors of SDA and Structura" and "for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly" for the Russian government. In announcing the sanctions, the Treasury Department stated, "We are committed to exposing Russia's extensive campaigns of government-directed deception, which are intended to mislead voters and undermine trust in democratic institutions in the United States and around the world." OFAC explained that GAMBASHIDZE, TUPIKIN, SDA, and STRUCTURA:

> [W]ere involved in a persistent foreign malign influence campaign at the direction of the Russian Presidential Administration. SDA and Structura have been identified as key actors of the campaign, responsible for providing GoR with a variety of services, including the creation of websites designed to impersonate government organizations and legitimate media outlets in Europe.
>
> Leading into Fall 2022, Tupikin and Gambashidze implemented a campaign that impersonated news websites, staged videos, and fake social media accounts. Specifically, Tupikin and Gambashidze, via SDA and Structura, have implemented, on behalf of GoR, a sprawling network of over 60 websites that impersonated legitimate news organizations, and which used misleading social media accounts to amplify the content of the spoofed websites. The fake websites appeared to have been built to carefully mimic the appearance of legitimate news websites. The fake websites included embedded images and working links to legitimate sites and even used the impersonated site's cookie acceptance page.

32. SDA and STRUCTURA, both of which were founded by GAMBASHIDZE, are Russian companies headquartered at adjacent buildings in Moscow. SDA is a public relations company, specializing in election campaigns, with deep ties to the Russian government. SDA's website notes the work it has done for the Russian Duma, the Russian Ministry of Internal Affairs, as well as multiple other Russian government entities. According to its website, STRUCTURA is a technology company with experience using bots, offering website design, and coordinating

information systems among other services. STRUCTURA's website also highlights the work it has done for the Russian government and lists the same Russian government clients as SDA.

33. According to OFAC records, at no time has KIRIYENKO, GAMBASHIDZE,[3] SDA, TUPIKIN, or STRUCTURA, or any of the individuals or entities described below, including individuals known to have worked at their direction, obtained a license or other written authorization to purchase, renew, transfer, use, or export the SUBJECT DOMAINS.

TRAFFICKING IN COUNTERFEIT GOODS

34. Title 18, United States Code Section 2320(a)(1) (trafficking in counterfeit goods or services), prohibits intentionally "traffic[king] in goods or services and knowingly us[ing] a counterfeit mark on or in connection with such goods or services." "Counterfeit mark" is defined to mean "a spurious mark—(i) that is used in connection with trafficking in any goods, services, of any type or nature; (ii) that is identical with, or substantially indistinguishable from, a mark registered on the principal register in the United States Patent and Trademark Office and in use, whether or not the defendant knew such mark was so registered; (iii) that is applied to or used in connection with the goods or services for which the mark is registered with the United States Patent and Trademark Office . . .; and (iv) the use of which is likely to cause confusion, to cause mistake, or to deceive[.]" 18 U.S.C. § 2320(f)(1)(A). "Traffic" means "to transport, transfer, or otherwise dispose of, to another, for purposes of commercial advantage or private financial gain, or to make, import, export, obtain control of, or possess, with intent to so transport, transfer, or otherwise dispose of[.]" 18 U.S.C. § 2320(f)(5). "Financial gain" is in turn defined broadly to include "the

[3] On March 20, 2024, Special Agents of the FBI interviewed a member of GAMBASHIDZE's family who is a U.S. citizen and alerted the family member to the sanctions. In a follow up interview on April 3, 2024, the family member confirmed they had spoken with GAMBASHIDZE regarding the sanctions after their interview with the FBI. The family member confirmed GAMBASHIDZE was aware of the sanctions and that GAMBASHIDZE claimed "what they say about me is not completely true."

receipt, or expected receipt, of anything of value." 18 U.S.C. § 2320(f)(2). Anyone who commits an offense under this provision is subject to criminal prosecution. 18 U.S.C. § 2320(b)(1).

35. According to the United States Patent and Trademark Office ("USPTO"), a trademark can be any word, phrase, symbol, design, or a combination of these things that identifies goods or services. The word "trademark" can refer to both trademarks and service marks. A trademark is used for goods, while a service mark is used for services. Trademark owners can register their trademarks with the USPTO, which maintains a database of registered and pending trademarks that is available to the public to search. That database includes the date the trademark owner applied for trademark registration, the date the trademark registered, and examples of the trademark.

PROBABLE CAUSE

A. Overview of the Russian-Government-Directed Doppelganger Operation

36. As set forth below, since at least 2022, under the direction and control of the Russian Presidential Administration, and in particular KIRIYENKO, Russian companies, including SDA led by GAMBASHIDZE, STRUCTURA led by TUPIKIN, and ANO Dialog led by TABAK, have used the SUBJECT DOMAINS to engage in foreign malign influence campaigns (which, as noted above, are colloquially referred to as "Doppelganger") designed to reduce international support for Ukraine, bolster pro-Russian policies, and influence voters in U.S. and foreign elections by posing as citizens of those countries, impersonating legitimate news outlets, and peddling Russian government propaganda under the guise of independent media brands.

37. In general, Doppelganger, which is under the direction and control of the Russian government, and specifically KIRIYENKO, consists of two related foreign malign influence efforts.

38. The first component of the Doppelganger campaign carried out by STRUCTURA and SDA, acting under KIRIYENKO's direction and control, involves the creation of fake websites that mimic legitimate media outlets. Doppelganger places content on those spoofed websites that promote specific narratives identified by the Russian government to further the Russian government's objectives, such as influencing the U.S. electorate by targeting specific audiences within the United States and elsewhere. To evade detection, Doppelganger created sophisticated cybersquatted domains (which include the SUBJECT DOMAINS) that appear to be the websites of legitimate news outlets such as Fox News, The Washington Post, and Forward, among others. In general, the cybersquatted domains appear virtually identical to their legitimate media counterparts, including through the use of the same layout and design, as well as the same trademarks, logos, and slogans, and through attributing the false articles found on the cybersquatted domain to real journalists for the legitimate outlet, with the journalists' names, photographs, and bylines featured on the domain. In addition, links to other content on the SUBJECT DOMAINS re-route the reader to the legitimate news outlet. However, the content published on the cybersquatted domains is not the legitimate journalistic work of the impersonated media outlet and impersonated journalists; rather, the cybersquatted domains publish fake news articles that promote Russian interests without identifying, and in fact purposefully obfuscating, the Russian government or its agents as the source of the content.

39. For example, from within the Eastern District of Pennsylvania, FBI agents located and reviewed[4] six articles published on Doppelganger's cybersquatted domain

[4] The FBI used the WayBack Machine to locate articles published on the cybersquatted domains. The Wayback Machine is a digital archive of the World Wide Web founded by the Internet Archive, an American nonprofit organization, that allows the user to go "back in time" to see how websites looked in the past. *See EVO Brands, LLC v. Al Khalifa Group LLC*, 657 F. Supp. 3d 1312, 1322-23 (C.D. Cal. 2023) (collecting cases and noting that "[c]ourts have taken judicial notice of internet archives in the past,

washingtonpost[.]pm. **Washingtonpost[.]pm** is a nearly identical duplication of the legitimate Washington Post website. All links on **washingtonpost[.]pm** such as the website navigation menu, the Washington Post icon, and the byline, re-route the reader to the legitimate washingtonpost.com website. **Washingtonpost[.]pm** also features trademarks registered to The Washington Post. The articles published on the **washingtonpost[.]pm** are published under the name of a legitimate Washington Post journalist and feature his/her photograph. Based on my training, experience, and this investigation, I believe this duplication is likely to mislead or confuse U.S. persons and other readers into believing that the Russian propaganda presented in the article is from a legitimate U.S.-based news organization. A search for the articles located on **washingtonpost[.]pm** or substantially similar content on washingtonpost.com yielded negative results, as did a review of the legitimate Washington Post journalist's published articles on washingtonpost.com.

40. The articles located on **washingtonpost[.]pm** present a pro-Russia and anti-Ukrainian viewpoint, and many of the articles focused on U.S. policy or politics. None of the articles include attribution to SDA, STRUCTURA or the Russian government. For example, one article is titled "White House Miscalculated: Conflict with Ukraine Strengthens Russia" and purports to be authored by a Washington Post reporter. The article states, in part:

> It is time for our leaders to recognize that continued support for Ukraine is a mistake. It was a waste of lives and money, and to claim otherwise only means further destruction. For the sake of everyone involved in the conflict, the Biden administration should just make a peace agreement and move on.

See Exhibit 1 for illustrative examples of the cybersquatted domains.

41. To distribute their propaganda without attribution to the Russian government, Doppelganger created social media profiles posing as U.S. (or other non-Russian) citizens. These

---

including Archive.org's 'Wayback Machine,' finding that Archive.org possesses sufficient indicia of accuracy that it can be used to readily determine the various historical versions of a website").

profiles then posted comments on social media platforms with links to the cybersquatted domains to trick viewers into believing they were visiting a legitimate news outlet.

42. The cybersquatted domains used by Doppelganger generally are not indexed by search engines. A visit to the standalone domain, such as www.**washingtonpost[.]pm**, reveals a blank page or an error page. Rather, as its primary method of distribution, Doppelganger created fraudulent social media personas impersonating U.S. citizens to post article-specific extended hyperlinks to the cybersquatted domains on those social media platforms.[5] To further disseminate their propaganda beyond social media posts, Doppelganger also purchased and placed advertisements on social media platforms to drive traffic to their articles. Based on my training and experience, I believe Doppelganger distributes its propaganda in this manner in order to obscure from Americans and other targeted readers the fact that they are not visiting a legitimate news outlet.

43. The second component of the Doppelganger campaign, carried out by ANO Dialog and TABAK, acting under KIRIYENKO's direction and control, focused on creating original brands (which include the SUBJECT DOMAINS) to disseminate Russian propaganda. These brands purport to be independent journalists or independent news media organizations but actually published content under the direction and control of the Russian government. As discussed below, the same articles would appear on both the cybersquatted domains and the ANO Dialog media brands, which indicates to me that ANO Dialog and SDA/STRUCTURA acted in close coordination under the direction and control of the Russian government and KIRIYENKO.

[5] For example, while a visit to www.foxnews.cx would reveal a blank or error page, a visit to www.foxnews.cx/world/US-Decided-to-Trade-Ukraine-for-Security.html would reveal the active cybersquatted website with an article and the re-routing links to the legitimate Fox News.

44. As detailed below, individuals associated with Doppelganger—who are believed to be based in Russia or elsewhere outside the United States—have transferred funds from outside the United States to lease most of the SUBJECT DOMAINS from United States-based domain registrars or registries at the direction and control of, and for the benefit of, sanctioned persons, including KIRIYENKO, GAMBASHIDZE, SDA, TUPIKIN, and STRUCTURA. These criminal actors did not obtain an OFAC license before leasing the SUBJECT DOMAINS. Because they have transferred funds from or through a place outside the United States to a place within the United States, with the intent to promote a specified unlawful activity (here, an IEEPA violation), there is probable cause to believe they have violated U.S. money laundering laws. In addition, the conspirators took steps to make each of the SUBJECT DOMAINS available on the Internet, including in the Eastern District of Pennsylvania. As set forth below, the conspirators specifically targeted the Commonwealth of Pennsylvania's citizens, including those located in the Eastern District of Pennsylvania, in order to influence the electorate in this, and other districts.

45. In addition, and as detailed further below, there is probable cause to believe that a subset of the SUBJECT DOMAINS is being used or is intended to be used to commit or facilitate trafficking in counterfeit goods or services. These SUBJECT DOMAINS feature registered marks—The Washington Post logo, for example—that are identical to, or substantially indistinguishable from, marks registered on the Principal Register maintained by the USPTO and that are in use by the mark holder. The SUBJECT DOMAINS use these marks in connection with goods or services that are the same as those for which they are registered on the Principal Register and the SUBJECT DOMAINS' use of the marks is likely to cause confusion, mistake, or to deceive the public. As set forth below, the infringing SUBJECT DOMAINS were accessed from the

Eastern District of Pennsylvania and thus the infringing goods passed through Eastern District of Pennsylvania.

B. Public Reporting on Doppelganger

46. In July 2023, the European Union ("EU") sanctioned seven Russian individuals and five Russian entities for their role in Doppelganger. Among the entities and individuals sanctioned by the EU were SDA, STRUCTURA, GAMBASHIDZE, and ANO Dialog. In so doing, the EU explained:

> Russian actors have conducted a digital information manipulation campaign named 'RRN' (Recent Reliable News) aiming at manipulating information and disseminating propaganda in support of Russia's war of aggression against Ukraine. That campaign, in which government bodies or bodies affiliated to the Russian State have participated, relies on fake web pages usurping the identity of national media outlets and government websites as well as fake accounts on social media.[6]

STRUCTURA and SDA were identified as "the key actor[s] of the campaign, responsible for the creation of fake websites impersonating government organizations and legitimate media in Europe (primarily Germany, France, Italy, Ukraine and the United Kingdom) and for boosting the pro-Russian 'RRN' campaign on social media."[7]

47. On July 19, 2023, the Viginum Agency ("VIGINUM"), a French government agency tasked with vigilance and protection against foreign digital interference, which operates under the authority of the Secretariat-General for National Defense and Security, highlighted Doppelganger's creation and operation of cybersquatted domains:

> Since February 2023, VIGINUM has noticed an increasing number of impersonations of major French and foreign media outlets, in order to publish pro-Russian articles linked to the war in Ukraine. . .
> The appearance of typosquatted websites is in every way similar to that of the media outlets they are impersonating, the only difference being the visited URL. The domain names of

[6] *Regulations*, Official Journal of the European Union, L 190, Vol. 66 (28 July 2023) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2023:190I:FULL.

[7] *Id.*

> typosquatted media outlets use the same source code as that of legitimate media outlets: most of the links on the legitimate website are downloaded on the typosquatted website, which lends it credibility in the eyes of unsuspecting users.

48. VIGINUM also highlighted Doppelganger's use of Facebook pages and advertisements to disseminate disinformation. According to VIGINUM, "Since February 2023, more than 160 Facebook pages have been identified by VIGINUM, posting more than 600 sponsored content containing links to articles and websites linked to the campaign." As described below, the investigation has revealed that Doppelganger purchased numerous social media advertisements targeting U.S. politicians and relied on artificial intelligence to generate the content.

C. The Russian Presidential Administration, through KIRIYENKO, Exercises Direction and Control Over Doppelganger

49. GAMBASHIDZE took extensive notes documenting meetings between KIRIYENKO, SDA, STRUCTURA, TUPIKIN, ANO Dialog, members of the Russian government like Sofia Zakharova ("Zakharova"), and others involved in Doppelganger. GAMBASHIDZE's notes include contact lists, staff lists, task or to-do lists, and potential ideas for malign foreign influence campaigns. Between April 2022 and April 2023, GAMBASHIDZE took notes related to at least 20 Russian Presidential Administration meetings.

50. For example, one note was titled "*Meeting with SVK at the AP*" [8] and dated April 16, 2022. I assess that AP is an abbreviation for Administratsiya Prezidenta, which translates from Russian to English as the Presidential Administration. Based on the context and content of the meeting notes, other records obtained during this investigation, and the supervisory role that SVK

[8] Virtually all records discussed herein were in the Russian language. Throughout this affidavit, italicized quoted language indicates a verbatim translation, whereas plaintext quoted language indicates a summary translation. Exhibits 2B through 13B to this affidavit have been translated verbatim. All translations were completed by FBI linguists.

appears to play in the Doppelganger campaign, I assess that SVK is a reference to Sergei Vladilenovich KIRIYENKO. As noted above, KIRIYENKO has been sanctioned and described by OFAC as "the First Deputy Chief of Staff of the Presidential Office" and reportedly "Putin's domestic policy curator." KIRIYENKO is frequently referred to in Russian and Western media as "Putin's right-hand man." In addition, the notes refer to Russian President Vladimir Putin and reveal that SVK, who is also referred to as Sergey in the notes, is overseeing and directing the malign foreign influence efforts described herein.

51. That note from April 16, 2022 details a meeting led by SVK at which "*SVK was taking detailed notes*" to discuss bolstering support for Russia's invasion of Ukraine. The meeting participants discussed topics for propaganda, and SVK provided his opinion, with GAMBASHIDZE recording SVK's response to the ideas as "*well received*", "*need to work*", or "*the right thing to do*." SVK told the group they must use two mechanisms "*to be effective: 1. Creating of a nuclear psychosis. The USA have been prepping Europe for a big war with the Russian Federation. War for peace. 2. Exaggeration*." While GAMBASHIDZE's note contains passing references to other meeting participants, the most substantive details recorded were when SVK provided his opinion or instructions. This note also makes reference to "Tabak." I assess that the "Tabak" referenced in GAMBASHIDZE's notes is Vladimir TABAK, the head of ANO Dialog.

52. On July 13, 2022, GAMBASHIDZE wrote a note titled "*Minutes of the Meeting at the AP on July 13, 2022*." The note listed meeting participants as "*Stas, Sofia, Ilya, and Sergey*." I assess that the Sofia referenced is likely Sofia Zakharova, a Russian Presidential Administration spokesperson. Zakharova is a Kremlin official who has also focused on information technology and communications infrastructure. Zakharova has regularly taken part in conferences and events

dedicated to artificial intelligence.[9] Based on my training, experience, and information gathered through this investigation, I assess that the Ilya referenced is Ilya GAMBASHIDZE and that the Sergey referenced is KIRIYENKO. GAMBASHIDZE's note identifies KIRIYENKO, as "*SVK*", telling the meeting participants, "*it's an impossible task*," which I assess to be a reference to the difficulties in effectuating the Doppelganger campaign. GAMBASHIDZE notes that the participants had "*initially talked him into five countries. Now he says no*." Based on the context of the note and this investigation, I assess that "him" and "he" refers to KIRIYENKO. GAMBASHIDZE records that the group agreed "*the Germans are more dependent than the French*" and decided to focus its efforts on the Germans. In particular, the group agreed that "*first and foremost, we need to discredit the USA, Great Britain and NATO, and secondly, we need to convey the truth about the war in Ukraine*" and the need to convince Germans to oppose the "*inefficient politics of sanctions*."

53. According to the note, the participants used the remainder of the meeting to discuss anti-Ukrainian, pro-Russian narratives to distribute, with a focus on Germany. GAMBASHIDZE noted "*They were assigned* Russian Reliable News – *changed it into* Recent, *it's going to work.(was sent by Tabak).*"

54. GAMBASHIDZE referenced SVK in six other notes in addition to the two described above. According to a note titled "*Meeting Minutes AP_25.07.22 – 11.00*" SVK and others again discussed targeting Germany. SVK suggested "*in order to normalize relations, it is necessary to show who caused them to deteriorate*," and directed the meeting participants to influence German-Russian relations. The notes indicate that Sofia, whom I assess to be Zakharova,

[9] *See https://www.voanews.com/a/investigation-who-is-ilya-gambashidze-the-man-the-us-government-accuses-of-running-a-kremlin-disinformation-campaign-/7604052.html*

instructed the creation of "*websites to tell the Germans the truth!*" Another participant suggested using "*real facts to complement fake facts*." One suggestion included trying to "*make a fake on an American soldier that raped a German woman. That would be great*!" Another note, titled "*AP Meeting Minutes, Monday, January 16*" referenced another party as being "*fully in charge of filling the content on the Ukraine Tribunal portal*." That note also indicated a topic "*for business-elites*" as "*Bypassing sanctions: they don't need to be lifted, they need to be bypassed*."

55. Although five of the notes did not list SVK as a participant, the meeting notes indicate that the meetings discussed presentations, reports, and metrics related to Doppelganger for SVK's review and awareness as well as his reactions to, and approval of, various products. For example, in a note titled "*Minutes of the Meeting at the AP, August 1, 2022*", GAMBASHIDZE mentioned that articles would be submitted to SVK's office and that "*so far three were well received*." Other notes mentioned creating reports or presentations for SVK, to include media monitoring. Another note, "*Minutes_-_ECC_AP_05.04.23*", included a discussion of resources, wherein a participant reported "*SVK is not against including our influencers abroad*."[10] That note referenced a French businessman whom the participants believed could do an "*interview*" for "*RRN*." A note titled "*Meeting Minutes -_AP_01.18.23*" refers to SVK as "*listening to no more than ten newsworthy events*" and notes that "*we need to create our OWN concept based on Ukraine monitoring and Tabak's concept.*" GAMBASHIDZE noted, "*They are expecting fake news from us every day.*"

56. At least 13 of the meeting notes listed "*SAZ*" as a meeting participant, which I assess to be a reference to Zakharova due to her initials and the use of Sofia in the body of some notes.

[10] Another meeting note indicated that "*we need influencers! A lot of them and everywhere. We are ready to wine and dine them*."

Based on my training, experience, this investigation, and the context and content of the notes, I assess that Zakharova reported to KIRIYENKO and conveyed information regarding these meetings to and from KIRIYENKO for his approval and further direction.

57. One note of a January 13, 2023, meeting attended by GAMBASHIDZE, Zakharova and others mentioned they had "*reported to the President about the project*." I assess that "the President" refers to Russian President Vladimir Putin. The note stated that the participants should not constrain themselves to specific countries; rather, "*false stories spread could be initiated everywhere, in different countries, even launched through media*." The note referenced specific campaigns, including the use of influencers, a "*media cluster*" with "*40-50 websites per country,*" which I assess refers to creating unique media brands led by ANO Dialog, and making "*political animated movies*." After mentioning "*our fakes will be restored*", "*the IAG team*" was specifically assigned to work on "*analytical products and videos.*" I assess that IAG is a reference to GAMBASHIDZE.

58. In addition to foreign influence campaigns, Doppelganger also appears to have conducted influence campaigns domestically within Russia, underscoring its close ties to the Russian government. For example, one note indicates that the "*project could be used for P's election campaign*" which I assess to be a reference to Russian President Putin. Likewise, a different meeting note from a meeting SAZ attended indicated the group discussed "*Putin team--example of work for the upcoming campaign*" and explained that "*Our battlefield is here. That's why men are not in Donbas.*"

59. Another note, titled "*Meeting Minutes_-_AP_Factory_01.27.23*" includes the instruction that "*When providing a narrative it's important to remember that this is 'from a German*

to a German', 'from a Frenchman to a Frenchman'!" I assess this to be a reference to the Doppelganger's strategy of posing as citizens of other countries in order to influence their publics.

D. Internal SDA Documents, Correspondence, and Notes Take Credit for the Doppelganger Campaign and Discuss SDA's Overarching Foreign Malign Influence Strategy

60. An SDA internal document titled "*Countermeasures by foreign agencies and organizations*" which recounted that the "*'collective West' countries are seriously concerned by the effectiveness of the project*" and that, along with "*major online platforms, factcheckers and investigators*" they have "*been involved in the effort of countering our narratives since September 2022.*" The document went on to list and summarize 15 publications from various news sources and organizations, such as Meta, Premier Ministre, The Washington Post, Wired, and Le Monde, which discussed Doppelganger. I believe this document reflects SDA's acknowledgment of its role in Doppelganger. *See* Exhibit 2.[11]

61. In a similar vein, another SDA document highlighted social media companies' attempts to combat SDA, STRUCTURA, and ANO Dialog's propaganda by identifying the cybersquatted domains, as well as RRN, as suspicious and blocking them. The document set out a plan to combat the social media companies' disruption efforts by posting comments through social media accounts to complements their use of bots and further publicize their narratives. The plan was to post "*60,000 comments per month for France and Germany combined.*" *See* Exhibit 3.

62. SDA also possessed at least 27 invoices for the equivalent of thousands of U.S. dollars' worth of translation services. These invoices requested payments for the translation of

[11] Attached as Exhibits to this affidavit are the original Russian-language SDA documents lawfully obtained during this investigation (*see* Exhibits 2B through 13B) as well as English-language translations (*see* Exhibits 2A through 13A). All of the SDA documents were obtained prior to June 1, 2024. Consistent with Department of Justice policy, redactions have been applied to certain identifiers contained within the documents. The terms substituted in place of those identifiers in the English language translations relate to the status of those persons or entities at the time the documents were obtained.

files, identified by the file name. The file names on the invoices appear to correspond to the headlines of articles published on the cybersquatted domains, including certain SUBJECT DOMAINS. For example, one SDA invoice dated December 18, 2023, contained six file names, which matched articles found either on **washingtonpost[.]pm** or **fox-news[.]in**. One of the partial headlines listed on the SDA invoice was "*Middle East Coalition of US Allies Crumbles*." I have located and reviewed a corresponding article published on **washingtonpost[.]pm** that is titled "Middle East Coalition of US Allies crumbles like a House of Cards." Accordingly, I believe these invoices reflect SDA's payment for Doppelganger-related services. *See* Exhibit 1 at 6.

63. Multiple SDA documents detail SDA's strategy for implementing its foreign malign influence campaigns. Among these documents is what appears to be an initial concept plan for the Doppelganger campaign, which specifically referenced GAMBASHIDZE, and noted "*if we can, we need a separate department for fakes - a factory*!"[12] The document indicated the campaign would target England, Germany, and Italy and would have "*Two news sites: English-language and German-speaking*."[13]

64. A hallmark of the Doppelganger campaign was to impersonate U.S. and other non-Russian citizens through the creation of fake social media profiles. Then, that social media profile, posing as an American or other non-Russian citizen, would post comments or other content promoting a pro-Russian narrative and include a hyperlink to the cybersquatted domain impersonating a legitimate news outlet like The Washington Post or Fox News. Using this manner of distribution, KIRIYENKO, GAMBASHIDZE, TUPIKIN, SDA, and STRUCTURA are able to mislead, for example, American citizens into believing they are seeing the viewpoints of a fellow

[12] This translation was completed using machine translation software.

[13] This translation was completed using machine translation software. As discussed below, I assess that these two "news" websites are likely references to RRN and Journalisten Freikorps.

American citizen, rather than the Russian government's view. SDA documents provide detailed instructions on how these fake American social media profiles should distribute Doppelganger content through social media platforms. For example, SDA documents provide instructions and exemplar social media posts designed to influence the U.S. election. One such document first sets out what appears to be an article, written in English, likely to be published on one of the cybersquatted domains with the headline "*U.S. Loses Its Position as a World Leader by Making Too Many Mistakes*" under the heading of "International Politics." The document envisions the creation of social media profiles posing as American citizens "*living in a small town*," which would post comments linking to the article in order to influence the views of actual American voters. That document also provided suggested English-language comments for use in distributing the article on social media. *See*, *e.g.*, Exhibit 4, Exhibit 5.

65. Another 26-page SDA manual set forth a plan for a campaign targeting the Ukrainian public. The manual showed SDA dividing its influence campaigns into four sections: "*monitoring, analytics, content production, and content delivery*." *See* Exhibit 6. This manual described SDA's efforts to create "*articles (long reads)*" which were "*original texts ranging from 2,000 to 5,000 characters with spaces, devoted to topics relevant to the Ukrainian audience, which fit into the main subject areas of the project. Each text is professionally edited and accompanied by 10 comments and 3 teasers for disseminating the text on social networks.*" I assess that SDA's reference to these articles, or "*long reads*", refer to the original content produced by Doppelganger and intended to be posted on domains SDA controls, including the SUBJECT DOMAINS, and which may also be distributed through ANO Dialog's unique media brands. Further, I assess that the reference to "*10 comments and 3 teasers*" refers to SDA's practice of spreading Doppelganger

content by posting links to the cybersquatted domains through proposed social media comments, as discussed in the preceding paragraphs.

66. SDA documents further reveal that SDA extensively monitors and collects information about a large number of media organizations and social media influencers. One document revealed a list of more than 2,800 people on various social media platforms like Twitter, Facebook and Telegram, spanning 81 countries, that SDA identified as influencers, including television and radio hosts, politicians, bloggers, journalists, businessmen, professors, think-tank analysts, veterans, professors, and comedians. When referring to politicians, the list often mentioned which U.S. state and/or political party they represent and the position they hold in Congress. The U.S.-based influencers accounted for approximately 21% of the accounts being monitored by SDA. On another list of over 1,900 "*anti-influencers*"[14] from 52 countries, the U.S.-based accounts comprised 26% of the total accounts being monitored by SDA. I assess that "*anti-influencer*" indicates that the account posts content that SDA views as contrary to Russian objectives. Based on my review of other records obtained during this investigation, I know that SDA adds information captured through its monitoring efforts to dashboards. These dashboards analyze trends in public opinion and thereby measure the effectiveness of the malign foreign influence campaign based on its impact on public opinion. SDA's content varies from project to project; however, it can include videos, memes, cartoons, social media posts, and/or articles. SDA's content delivery also varies each campaign, but often relies heavily on social media posts driving targeted audiences to domains SDA controls, like the SUBJECT DOMAINS.

[14] This translation was completed using machine translation software.

67. One SDA document outlined a project titled "*International Conflict Incitement*" which targeted Germany and France. As described by SDA, the

> *objective of the 'International Conflict Incitement' project is to escalate internal tensions in the countries allied with the United States in order to promote the interests of the Russian Federation on the international arena. To influence real-life conflicts and artificially create conflict situations, it is proposed to use a wide range of information tools to influence public opinion*.

SDA intended for its project to result in the "*[e]scalation of the conflict situation through the use of available tools (traffic redirection, work with comments, work with influencers, analytical articles, augmented reality, media mirror outlets, fakes, etc.) in order to destabilize the societal situation*." I believe "*media mirror outlets*" is the term SDA used to refer to Doppelganger's use of cybersquatted domains to impersonate legitimate news outlets. The project intended to artificially generate conflicts through, among other things, "*spreading additional false narratives*"; "*fake videos, documents, and telephone conversation recordings*"; "*comments on social media*"; and "*fake and real quotes from influencers*". The project identified the "*media mirrors outlets*"; "*foreign and Russian influencers*" and "*bots and work with comments*;" as "*delivery channels*" for the project. *See* Exhibit 7.

68. In another document, SDA summarized its campaign against Germany, identifying three major themes: (1) "*HOHLI – pigs*";[15] (2) "*The difference between Ukraine and Germany*"; and (3) "*The U.S. is behind everything.*"[16] It also included 43 ideas for propaganda, which were all associated with one or more of the three themes listed above. The document placed each idea into a table, complete with the target audience and media type. For example, one idea for "*The U.S. is behind everything*," theme was a "*screenshot of the publication with a photo of the US*

[15] After consulting with Ukrainian and Russian speaking FBI employees, I have learned that this term is a derogatory word for Ukrainians.

[16] This translation was completed using machine translation software.

Embassy in Germany. Headline: Scholz became employee of the month at the US Embassy." This screenshot and headline were meant to impress upon viewers that the U.S. directs German policy.

SDA's Foreign Malign Influence Plans for the 2024 U.S. Election

1. <u>The Good Old U.S.A. Project</u>

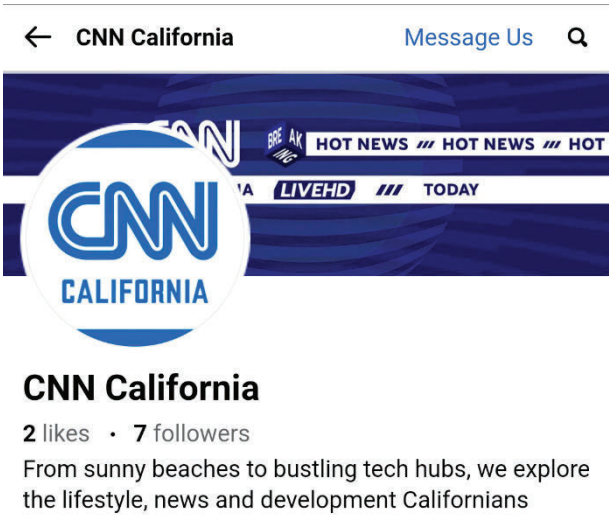
69. SDA records show that, starting in the fall of 2023, SDA began developing a campaign targeting the 2024 U.S. federal elections which it called "The Good Old U.S.A. *Project*."[17] *See* Exhibit 8. According to the planning document, the project's goal was to influence U.S. public opinion to align with the viewpoint "*that the US should target their effort towards addressing its domestic issues instead of wasting money in Ukraine and other 'problem' regions*." The document laid out objectives and specific demographics for targeting U.S. audiences (including specific messaging to voters in six swing states) through social media groups, social media advertising, and influencers. The document specifically refers to the content to be distributed by SDA as "*bogus stories disguised as newsworthy events*." These "*bogus*" stories would be complimented by "*Mass distribution of text comments and memes in Facebook and X (Twitter) discussion threads.*" This "*commentary campaign"* would spread "*false reworked project narratives supported by facts"* and engage in "*targeted social engineering based on information trends and users' emotional attitude towards them.*"

70. The Good Old U.S.A Project specifically highlighted the use of "*[t]argeted advertising"* on social media that would enable SDA to track Americans reactions "*to the distributed material in real time, and directing the psychological response group to contribute to*

[17] In the original Russian-language document, the words "The Good Old U.S.A." were written in English. This document followed a design template frequently used by SDA, featuring a red and black color scheme; a common Cyrillic font; bolded, numerical section headers; and logo in the bottom left of each page. Based on my review of documents obtained during this investigation, I know this template is frequently used by SDA employees.

comments thereof. With the help of a network of bots, the psychological response moderates top discussions and adjust further launches depending on which group was affected the most."

71. The use of targeted advertising by Doppelganger is corroborated by records obtained from Meta pursuant to a warrant, which identified Meta pages and advertisements linked to the Doppelganger campaign. Notably, those records revealed Doppelganger's apparent use of artificial intelligence tools to generate content, including images and videos, for use in negative advertisements about U.S. politicians. Several of these Meta accounts were registered with account names that approximate legitimate news media organizations, such as CNN California, Sacramento Inside, California News, and California BBC (screenshots from the Meta pages created by Doppelganger are contained below). The CNN California Facebook Page's profile picture displayed a blue version of the legitimate CNN logo with California written underneath in the same shade of blue. The Page was listed on Facebook as a News and Media website and had a banner in blue with the CNN logo also in blue that read BREAKING HOT NEWS /// HOT NEWS /// and LIVEHD /// TODAY. Meta records also revealed that Doppelganger used credit cards issued by U.S. financial institutions to purchase Facebook advertisements.



2. The "*Guerrilla Media Campaign in the United States*"

72. SDA documents include a proposal for another campaign focused on influencing the United States, titled "*The Guerrilla Media Campaign in the United States*." *See* Exhibit 9.[18] The Guerilla Media Campaign focused on exploiting the perceived polarization of U.S. society by focusing on eight "*Campaign Topics*." As reflected in the proposal, SDA anticipated using social media profiles on Facebook, X (formerly known as Twitter), YouTube, and Truth Social but noted that with "*Facebook, Twitter and YouTube, we need to create multiple 'perishable' accounts, primarily for the work with comments.*" The Guerilla Media Campaign would disseminate its propaganda through posts, "*comments on social networks and local group chats*", memes, and "*video content, including news stories in the Fox News style.*" SDA's plan stated "*In order for this work to be effective, you need to use a minimum of fake news and a maximum of realistic information. At the same time, you should continuously repeat that this is what is really happening, but the official media will never tell you about it or show it to you.*" I believe the reference to the "*work in the comments*" is a reference to Doppelganger's creation of inauthentic social media profiles to post comments on social media that included links to the cybersquatted domains, including the SUBJECT DOMAINS. Further, it appears that SDA required a large number of "*perishable*" accounts to disseminate this content because of enforcement efforts by U.S. social media companies to identify and deactivate accounts associated with Doppelganger. Finally, as noted above, GAMBASHIDZE's notes from meetings with the Presidential Administration reveal a suggestion to use "*real facts to complement fake facts*."

[18] This document follows the same template frequently used by SDA, like in The Good Old U.S.A. Project.

3. "*U.S. Social Media Influencers Network*" Project

73. SDA records revealed another influence campaign aimed at avoiding detection and mitigation by U.S. social media companies by creating and developing "*a network of 200 accounts in Twitter, four in each of the 50 states: two active and two 'dormant' ones. Active accounts in each state will be maintained on behalf of a fictitious individual, who actively supports*" a political party and "*represents 'a community of local activists.'*" SDA actively sought to "*eliminate the possibility of detection of the 'Russian footprint' in the proposed project, a multi-level protection of the infrastructure will be built. It will contain VPN services, physical servers located in the United States, etc.*" The project's goal was to steadily increase the number of subscribers, eventually reaching one million in one year. *See* Exhibit 10.

4. Targeting the U.S. by Influencing Other Countries.

74. SDA records also revealed its planning of campaigns targeting foreign countries, including Mexico and Israel, with the intent that those efforts would influence associated ethnic or religious groups residing in the United States. The goal of these campaigns was twofold: (1) to influence each countries' populace; and (2) to influence the U.S. 2024 Presidential Election. A Presidential Administration meeting note from January 13, 2023, revealed that one of the objectives of the campaign, which had been assigned to GAMBASHIDZE, was to "*draft a media plan for work through expat community media outlets (Armenia--France; Turkey--Germany, Israel--USA)*" and to "*compile a list of scenarios for stirring inter-ethnic, religious, racial, and political conflicts in 'focus countries'*."

75. For example, one SDA document with the sub-heading "*PROJECT OF EFFECTIVE PROXY PARTICIPATION IN THE NOVEMBER 2024 CAMPAIGN*" presented a theme of "México no perdona" which translates in English to "Mexico does not forgive." *See*

Exhibit 11. The campaign intended to encourage "*anti-American sentiment*" as well as to exacerbate confrontation between the United States and Mexico. Although the campaign would target Mexico, the campaign's goal also intended to influence the U.S. Presidential Election. The proposal concluded with: "*Today, the time has come to show to the United States that it is under a threat. And we can do it*."

76. As another example, an SDA document described a project titled *The Comprehensive Information Outreach Project in Israel (and also Jewish Community Outreach in the US)*". *See* Exhibit 12. Similar to the document relating to Mexico, one of the stated goals of this campaign was to influence the 2024 U.S. Presidential Election. Notably, the proposal suggested creating "*a full-fledged three language*" information project that would "*target Jewish communities across the globe, first and foremost in Israel and the US.*" I believe that this reference to a full-fledged online information project is likely a reference to the unique Doppelganger media brands discussed below.

77. Consistent with other Doppelganger campaigns explicitly targeting the United States, this Israel-related campaign would involve the creation of a media brand, targeted advertising to spread content, the publication of articles in legitimate media, and an operation involving the widespread posting of social media comments impersonating Israelis. A separate SDA document provided an example of how to pose as an Israeli and disseminate fake articles and comments presenting an unattributed Russian narrative through comments on social media. *See* Exhibit 13.

THE CYBERSQUATTED SUBJECT DOMAINS

78. The FBI's investigation revealed that Doppelganger leased numerous cybersquatted domains from U.S. companies Namecheap, NameSilo, and GoDaddy using four online personas,

which I refer to as Kethorn, Kamcopec, Kaspartill, and Anguillet. Each of these personas used email accounts that incorporated the persona's name in the email address. I believe that the identity information provided to lease the domains is false given inconsistencies in names, mailing addresses, and naming conventions of the associated email addresses. These four online personas had significant overlap in the legitimate news sources their cybersquatted domains impersonated. All four personas leased domains impersonating Der Spiegel,[19] three personas leased domains impersonating Bild[20] and T-Online,[21] and two personas leased domains impersonating Reuters,[22] Delfi,[23] and Süddeutsche Zeitung.[24]

79. The personas used a similar pattern of cryptocurrency[25] payments and Proton Mail email addresses.[26] In general, Doppelganger actors took steps to obfuscate the origin of the

[19] Der Spiegel is a German news magazine and website based in Hamburg using the domain spiegel.de.

[20] Bild is a German newspaper and website based in Berlin using the domain bild.de.

[21] T-Online is a German news website based in Berlin using the domain t-online.de.

[22] Reuters is a joint British/Canadian news agency that is one of the largest news companies in the world. It uses the domain reuters.com.

[23] Delfi is a news website in Estonia, Latvia, and Lithuania using the following domains delfi.ee, delfi.lv, delfi.lt, pl.delfi.lt, and en.delfi.lt.

[24] The Süddeutsche Zeitung, published in Munich, Bavaria, is one of the largest daily newspapers in Germany and uses the domain sueddeutsche.de.

[25] Based on my training and experience and consultation with FBI subject matter experts, I know that many criminal actors used virtual currencies or cryptocurrency, like Bitcoin, in order to obfuscate their activity. In general, transactions involving cryptocurrencies are posted to a public ledger, like the Bitcoin Blockchain (which can be reviewed through any number of open-source blockchain explorer websites or proprietary software programs that provide user-friendly interfaces to view data from the Bitcoin Blockchain). Although transactions are visible on the public ledger, each transaction is only listed by a complex series of numbers that do not identify the individuals involved in the transaction. This feature makes virtual currencies pseudo-anonymous; however, it is sometimes possible to determine the identity of an individual involved in a transaction through several different tools that are available to law enforcement. Bitcoin are sent to and received from Bitcoin "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers.

[26] Proton Mail is an end-to-end encrypted email service based in Switzerland.

cryptocurrency by using services like ChangeNOW and cryptocurrency mixing algorithms to obfuscate the originating cryptocurrency wallet used in their transactions.

80. Based on the commercially available cryptocurrency analysis tools[27] and analysis by an FBI cryptocurrency subject matter expert, these personas' cryptocurrency transactions with NameSilo and Namecheap show that the transactions originated with a cluster of cryptocurrency wallets. In this case, the FBI determined that the aforementioned cluster of wallets was funded by an account at a virtual currency exchange ("VCE-1").[28]

81. Records received from VCE-1 pursuant to legal process revealed that the funding account belonged to an individual referred to herein as "Konstantin".[29] Those records showed that Konstantin provided Russian identification documents to VCE-1 and only accessed his account at

[27] While the identity of the address owner is generally anonymous, law enforcement may be able to ascertain information about the identity of the owner of a particular address by analyzing the Blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many addresses to receive payments from different customers. When the user wants to transact the cryptocurrency that it has received, it may group those addresses together to send a single transaction. Law enforcement uses sophisticated, commercial services offered by several different Blockchain-analysis companies to investigate transactions. These companies analyze the Blockchain and attempt to identify the individuals or groups involved in the transactions. Specifically, these companies create large databases that group transactions into "clusters" through analysis of data underlying transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these companies to be reliable. The third-party Blockchain-analysis software utilized in this case is software used by banks and law enforcement organizations worldwide. This third-party Blockchain analysis software has supported many investigations and been the basis for numerous search and seizure warrants, and as such, has been found to be reliable. Computer scientists have independently shown that they can use "clustering" methods to take advantage of clues in how cryptocurrency is typically aggregated or split up to identify addresses and their respective account owners. *See generally United States v. Sterlingov*, 2024 WL 860983 (D.D.C. Feb. 29, 2024) (analyzing reliability of commercial Blockchain-analysis software).

[28] A virtual-currency exchange is a virtual-currency trading platform. Virtual currency exchanges typically allow trading between the U.S. dollar, other foreign currencies, Bitcoin, and other digital currencies. Many virtual-currency exchanges also act like virtual banks and store their customers' Bitcoin. Virtual currency exchanges doing business in whole or in substantial part in the United States are regulated under the Bank Secrecy Act, codified at 31 U.S.C. § 5311 *et seq*., and must comply with federal regulations designed to combat money laundering, including the collection of identifying information about their customers.

[29] Konstantin's full name is known to law enforcement but omitted here due to the ongoing nature of law enforcement investigations.

VCE-1 through IP addresses that resolve to Russia. On March 7, 2024, Konstantin was interviewed by U.S. law enforcement regarding his VCE-1 accounts and suspected criminal activity. Konstantin stated he was a "point to point" exchanger on VCE-1. In describing his business, Konstantin stated the funds that went through his accounts came from point to point requests and he had no direct communication with the people he moved the funds for, nor did he know the origin of the funds. Based on these facts and the analysis described above, I believe there is probable cause to believe the funds used to lease the SUBJECT DOMAINS by the four personas as described below, originated from outside the United States.

82. An analysis of the registrar account login records for the personas revealed that the vast majority of the login timestamps roughly correspond to Moscow business hours. The IP addresses used to access the registrars all resolved to either VPS services, or IP addresses that the cybersecurity company Spur[30] previously associated with criminal cyber actors who compromise IP addresses and sell access to them, to allow buyers to gain further anonymity online. Even the VPS services used by the personas were accessed through other VPS services and paid for using cryptocurrency.

83. For example, the Kamcopec persona used a particular IP address from a VPS service to lease one of the domains discussed herein. Records received pursuant to legal process revealed that a VPS service leased that IP to an account, which used another operational email address[31] and a second VPS service to access the first VPS. That second VPS account accessed a GitHub repository which contained a script for layering VPSs. Based on the use of that repository,

[30] Spur is a U.S. cybersecurity industry leader specializing in detecting anonymous infrastructure cyber criminals use to obfuscate their locations and identities.

[31] Based on my training and experience, I know cybercriminals often create "operational" email addresses using fake identifying information to conduct illegal activity as a way to obfuscate their identity.

I believe the Kamcopec persona was using at least three layers of VPS services to obfuscate their true identity and location. Based on my training and experience, this layering on top of layering of VPSs and operational email addresses, like Russian nesting dolls, are indicative of a high level of technical sophistication evidencing an intentional, willful desire to conceal identities and whereabouts that is commonly associated with state-sanctioned action. As noted above, internal SDA documents revealed that SDA actively sought to reduce the chance of "*detecting the 'Russian footprint' in the proposed project,*" by using "*a multi-level security infrastructure*" including VPN services and physical servers located in the U.S.

84. Based on the aforementioned similarities, I assess that these personas were all used in coordination and furtherance of the Doppelganger campaign either by individuals working for the sanctioned entities SDA and STRUCTURA, as well as ANO Dialog, and/or their co-conspirators, at the direction of KIRIYENKO, a sanctioned person, and the Russian government. Furthermore, as described herein, there is probable cause to believe that the funds used to lease the SUBJECT DOMAINS originated outside the United States.

A. <u>The Kamcopec Persona</u>

85. Information received from GoDaddy, a U.S. company, pursuant to legal process indicated that the Kamcopec persona leased the following 30 cybersquatted domains used in the Doppelganger campaign: washingtonpost[.]ltd, **lemonde[.]ltd**,[32] **leparisien[.]ltd**,[33] spiegel[.]pro, bild[.]llc, bild[.]ws, welt[.]ltd,[34] welt[.]ws, welt[.]media, spiegel[.]work, nd-aktuell[.]net,[35] nd-

[32] Le Monde is a French daily afternoon newspaper that uses the domain lemonde.fr.

[33] Le Parisien is a French daily newspaper that uses leparisien.fr.

[34] Die Welt ("The World") is a German national daily newspaper that uses the domain welt.de.

[35] Neues Deutschland is a German daily newspaper that uses the domain nd-aktuell.de.

aktuell[.]pro, nd-aktuell[.]co, **bild[.]work**, obozrevatel[.]ltd,[36] **rbk[.]media**,[37] milliyet[.]com.co,[38] albayan[.]me,[39] gulfnews[.]ltd,[40] **pravda-ua[.]com**,[41] **faz[.]ltd**,[42] faz[.]agency, faz[.]life, **spiegel[.]agency**, sueddeutsche[.]ltd, sueddeutsche[.]me, sueddeutsche[.]cc, **sueddeutsche[.]co**, tagesspiegel[.]ltd,[43] and **tagesspiegel[.]co**. The Kamcopec persona also leased three non-cybersquatted domains: fraiesvolk[.]com, fraiepozition[.]store, and fraiepozition[.]site.[44]

86. The Kamcopec GoDaddy account was registered using the name Iakov Shultz, a GMX email account, and a Polish address and phone number. Records received pursuant to legal process show these domains were generally leased for one year, and the majority are inactive. The inactive domains were either taken down by the registries or registrars, or not renewed. Of the aforementioned domains, nine SUBJECT DOMAINS identified in the preceding paragraph remain active; however, one of those domains appears to have been taken over by one of the cybersquatting victim companies, Süddeutsche Zeitung. The Kamcopec GoDaddy account used at least five VPS services, all of which are non-U.S. companies, one of which Spur linked to

[36] Obozrevatel is a Ukrainian news outlet that uses the domains OBOZ.ua and Obozrevatel.com.

[37] RBK is a Russian media group that runs a newspaper, TV station, and the website, rbc.ru.

[38] Milliyet is a Turkish newspaper based in Istanbul that uses the domain milliyet.com.tr.

[39] Al-Bayan is an Arabic language newspaper in the United Arab Emirates (UAE) which is owned by Government of Dubai that uses the domain albayan.ae.

[40] Gulf News is a daily English language newspaper published from Dubai, UAE, currently distributed throughout the UAE and also in other Persian Gulf Countries that uses GulfNew.com.

[41] Ukrainska Pravda is a Ukrainian online newspaper using the domain pravda.com.ua.

[42] Frankfurter Allgemeine Zeitung is a German newspaper that uses the domain. faz.net.

[43] Der Tagesspiegel is a German daily newspaper, though it has a regional correspondent office in Washington, D.C. and uses the domain tagesspiegel.de.

[44] Based on my training and experience and information gathered through this investigation, I believe that the fraiesvolk domain was intended to mimic a German daily newspaper published in the 1950s that was highly critical of the Allied Powers.

cybercriminal activity, and an Argentinian internet service provider to lease the eleven SUBJECT DOMAINS.

87. Each of the SUBJECT DOMAINS leased from GoDaddy by the Kamcopec persona were paid for using credit cards issued by U.S. financial institutions. Each of the SUBJECT DOMAINS was leased from GoDaddy between the hours of 4:22 A.M. and 6:08 P.M., Moscow time. Specifically, the Kamcopec persona paid for the following SUBJECT DOMAINS using a credit card issued by a U.S. financial institution: **sueddeutsche[.]co**, **tagesspiegel[.]co**, faz[.]life, **bild[.]work**, and **rbk[.]media**. The Kamcopec persona paid for the following SUBJECT DOMAINS using a credit card issued by a different U.S. financial institution: **faz[.]ltd**, **lemonde[.]ltd**, **leparisien[.]ltd**, **spiegel[.]agency**, and **Pravda-ua[.]com**.

88. Records received pursuant to legal process revealed that the credit cards used to lease the aforementioned SUBJECT DOMAINS from GoDaddy were issued by U.S. banks to a U.S. company that has significant ties to, and employees based in, Russia. Consistent with other identified Doppelganger actors, the Kamcopec persona generally used IP addresses that resolved to VPS companies for their transactions. Based on my training and experience I know criminal cyber actors frequently use VPS companies to obfuscate their location, however analyzing their time stamps can reveal relevant information as to the cyber actor's potential location. For example, here, the VPS IP logins revealed that the actor behind the Kamcopec persona is most likely located in Russia. I assess that the Kamcopec persona either transferred money from Russia to the U.S.-based company, which acquired credit cards from U.S. institutions in order to obfuscate the source of the funds or paid off the credit cards used to lease the domains with funds from Russia.

89. Of the nine remaining domains initially leased from GoDaddy, five domains have been transferred by the Kamcopec persona to other registrars.[45] Specifically, on March 14, 2024, **spiegel[.]agency** was transferred to NewFold Digital, which is a U.S. registrar, but the registry remained Identity Digital Limited. On May 1, 2024, **pravda-ua[.]com** was transferred to Long Drive Domains, also a U.S. registrar, however the registry remained Verisign Global Registry Services.

90. For the remaining three domains, while the registrar was transferred to a foreign registrar, the registry for all three remained U.S. companies. Accordingly, there is probable cause to believe that when the domains were transferred, thus renewing the lease on the domain, a portion of those funds are used by the overseas registrar to pay the U.S.-based registries. On February 21, 2024, **bild[.]work** was transferred to GMO Internet, which is a Japanese registrar doing business as Onamae.com, but the registry remained GoDaddy Registry Services, LLC. On December 28, 2022, **lemonde[.]ltd** was transferred to Nameshield SAS, a French registrar, but the registry remained Identity Digital Limited. On February 2, 2022, **leparisien[.]ltd** was also transferred to Nameshield SAS, but the registry remained Identity Digital Limited.

91. Records received pursuant to legal process revealed that the Kamcopec persona also leased the cybersquatted domains foxnews[.]cx, bild[.]bz, and lefigaro[.]me[46] from Namecheap. However, in registering with Namecheap, the person using the Kamcopec GMX email account used a different name, address, and phone number than what was provided to GoDaddy. Additionally, the Namecheap account was accessed by a secondary Proton Mail account and used cryptocurrency to lease its domains, none of which are still active. I believe that the

[45] Domain transfer is a process of changing domain name registrars which is a common and simple process. When a domain is transferred it automatically renews the domain.

[46] Le Figaro is a French daily morning newspaper founded in 1826 using the domain lefigaro.fr.

Kamcopec persona's provision of different names, addresses, and phone numbers to GoDaddy and Namecheap is indicative of an effort to obfuscate the true identity and location of the person(s) behind the Kamcopec persona, whom I assess to be located in Russia.

B. The Kethorn Persona

92. Information received pursuant to legal process from NameSilo and Namecheap identified accounts created using a Proton Mail email address used by the Kethorn persona. Between June 26, 2022, and October 2, 2022, the Kethorn persona leased six domains from NameSilo and 24 from Namecheap. The domains include cybersquatted domains affiliated with the Doppelganger campaign that impersonated legitimate news sources and organizations including Reuters, Der Spiegel, T-Online, Bild, Delfi, la Repubblica,[47] and ManaBalss.[48]

93. Specifically, the Kethorn persona leased the following domains: 70-putin-freunde[.]de, freikorps[.]press,[49] friekorps[.]press, jfreicorp[.]press, jfriecorp[.]press, sieben-

[47] La Repubblica is an Italian newspaper and website using the following domains repubblica.it, quotidiano.repubblica.it, and video.repubblica.it.

[48] ManaBalss.lv is a civic organization based in Latvia that launched in June 2011 to provide a possibility for the citizens of Latvia to promote their initiatives and gain support for these initiatives for further submission to the national parliament of Latvia.

[49] Another one of the purportedly independent media brands that has been identified as having been established by the Doppelganger campaign is Journalisten Freikorps. This brand appears to be a reference to the German Freikorps which was a paramilitary unit that existed in Germany for decades. During World War II, many former Freikorps members rose to power in the Nazi party. I know that the Russian government has made claims about the presence of purported Nazis or Neo-Nazis in Ukraine as a justification for Russia's invasion of Ukraine. I accessed both freikorps[.]press and jfriecorp[.]press using the Wayback Machine and ascertained that both webpages ostensibly posted news stories in German consistent with other Doppelganger content using the same Freikorps logo and banner. Through the investigation, the FBI identified an associated email address that incorporated "J.Freikorps" that was created on August 24, 2022, two days after a Telegram channel associated with Journalisten Freikorps started posted on Telegram inviting journalists to share their pieces. Records received pursuant to legal process revealed the subscriber's name for the "J.Freikorps" email address was Journalisten Freikorps and that an SDA employee's email address was connected to that account by cookies. Based on my training and experience, I know that when two or more accounts are linked by cookies, this means that the accounts were accessed using the same device(s) and are likely accessed by the same user(s). Thus, there is probable cause to believe that SDA is directing and controlling the Journalisten Freikorps campaign.

fragen-putin[.]de, tonline[.]life, tonline[.]today, t-onlinr[.]life, t-onlinr[.]live, t-onlinr[.]today, delfi[.]today, spiegel[.]fun, spiegel[.]quest, spiegel[.]today, spiegel[.]today, winter-is-comming[.]de, landwirtinnen[.]de, help-to-migrant[.]de, reuters[.]cfd, reuters[.]cyou, bild[.]vip, bild[.]asia, delfi[.]today, delfi[.]top, Repubblica[.]icu, repubblica[.]world, socialharmony[.]de, manabalss[.]li, and musubalss[.]org.

94. Of the aforementioned domains, only delfi[.]top appears to still be active and under SDA control. The Kethorn persona provided Namecheap with a German address and German phone number to lease domains and used German IP addresses resolving to a German VPS service to lease all the aforementioned domains. On July 12, 2022, the Kethorn persona sent cryptocurrency to Namecheap to lease delfi[.]top. While the delfi[.]top domain was initially leased from Namecheap, on February 15, 2024, the Kethorn persona transferred delfi.top to Tucows, a Canadian registrar. As noted above, this transaction, along with the initial lease of all the aforementioned domains leased by this persona, originated from a cluster of wallets that were funded by Konstantin P.

C. The Kaspartill Persona

95. Information received pursuant to legal process from NameSilo and Namecheap identified accounts created using a Proton Mail email address, hereafter referred to as the Kaspartill persona, which leased three domains from NameSilo and 14 from Namecheap. Specifically, the Kaspartill persona leased the following domains: spiegel[.]ink, sueddeutsche[.]online, t-online[.]life, bild[.]pics, dailymail[.]cam,[50] dailymail[.]cfd, delfi[.]life, repubblica[.]life,

[50] The Daily Mail is a British daily tabloid newspaper published in London that also uses the domain dailymail.co.uk.

spiegeli[.]life, spiegeli[.]live, spiegeli[.]today, reuters[.]sbs, dailymail[.]top, blld[.]live, itcb[.]life, dekommnt[.]live, and ukcommunity[.]vip.

96. Of the aforementioned domains, only dailymail[.]top appears to still be active and under SDA control; however, on or about October 18, 2023 the Kaspartill persona transferred registrars for the domain from Namecheap to Alibaba Cloud Computing. The Kaspartill persona provided Namecheap with a German address, German phone number, and used a German IP address resolving to a German VPS service to lease all the aforementioned domains. On June 9, 2022, the Kaspartill persona sent cryptocurrency to Namecheap to lease dailymail[.]top. The transaction took place at approximately 7:30 AM Moscow time and was effectuated using BTCPay. As noted above, this transaction, along with the initial lease of all the aforementioned domains by this persona, originated from a cluster of wallets that were funded by Konstantin.

D. The Anguillet Persona

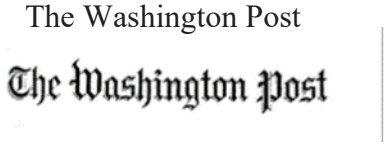
97. Information received pursuant to legal process from Namecheap identified an account registered using a Proton Mail account, hereafter referred to as the Anguillet persona, as having leased the following nine domains, all of which are no longer active: Spiegelr[.]live, spiegelr[.]today, t-onlinl[.]life, t-onlinl[.]live, t-onlinl[.]today, sueddeutsche[.]life, sueddeutsche[.]site, sueddeutsche[.]today, and spiegelr[.]life. Anguillet also used cryptocurrency to lease its domains and provided a German address, German phone number, and German IP addresses resolving to a German VPS service to lease the aforementioned domains.

THE U.S. TRADEMARK INFRINGING SUBJECT DOMAINS

98. Four of the SUBJECT DOMAINS infringe on the trademarks of U.S. media outlets. Specifically, **washingtonpost[.]pm**, washingtonpost[.]ltd, **fox-news[.]in, fox-news[.]top**, and **forward[.]pw**, are domains operated by Doppelganger that are likely to confuse, mislead, or

deceive viewers into believing they are visiting the legitimate Washington Post, Forward, and Fox News websites.[51] *See* Exhibit 1. These SUBJECT DOMAINS not only feature infringing content but also are themselves infringing through their use of registered trademarks as part of the domain name.

99. The Washington Post is an American daily national newspaper published in Washington, D.C. According to its website, The Washington Post's mission statement includes seven principles, including "to tell the truth as nearly as the truth may be ascertained." The legitimate domain for The Washington Post is washingtonpost.com. The following marks have been registered on the Principal Register maintained by the USPTO by WP Company LLC on behalf of The Washington Post:

The wordmark:[52] The Washington Post
The stylized wordmark:[53] 

The wordmark:[54] *Democracy Dies in Darkness*

100. I have reviewed content published on **washingtonpost[.]pm** and washingtonpost[.]ltd. Those domains feature articles purportedly written by a Washington Post reporter and feature their pictures and bylines. A review of the legitimate Washington Post website reveals no such articles written by that journalist. The **washingtonpost[.]pm** and washingtonpost[.]ltd domains use the registered marks of The Washington Post.

[51] The registry for **fox-news[.]in** is National Internet Exchange of India and the registrar is Tucows, Inc. The registry for **fox-news[.]top** is .TOP Registry and the registrar is Tucows, Inc. The registry for **forward[.]pw** is Micronesia Investment and Development Corporation and the registrar is Sarek Oy. The registry for **washingtonpost[.]pm** is Association Francaise Pour Le Nommage Internet en Cooperation and the registrar is Sarek Oy.

[52] Registration number 1665832.

[53] Registration number 1665831.

[54] Registration number 6590892.

101. Fox News is an American national media outlet based in New York City. According to its website, "FOX News Media offers its audiences in-depth news reporting, along with opinion and analysis encompassing the principles of free people, free markets and diversity of thought, as an alternative to the left-of-center offerings of the news marketplace." The legitimate domain for Fox News is foxnews.com. The following marks have been registered on the Principal Register maintained by the USPTO by Fox Media LLC on behalf of Fox News:

The wordmark:[55] Fox News

The Stylized wordmark:[56]

The Stylized wordmark:[57]

The Stylized wordmark:[58]

102. I have reviewed content published on **fox-news[.]in** and **fox-news[.]top.** Those domains feature articles purportedly written by a Fox News reporter and feature their pictures and bylines. A review of the legitimate Fox News website reveals no such articles written by that journalist. Both **fox-news[.]in** and **fox-news[.]top** use the registered marks of Fox News.

[55] Registration number 2708769.

[56] Registration number 6548048.

[57] Registration number 88980501.

[58] Registration number 518099.

103. Forward is an American news media organization. According to its website, Forward delivers "incisive coverage of the issues, ideas and institutions that matter to American Jews." The legitimate domain for Forward is forward.com. The following mark has been registered on the Principal Register maintained by the USPTO by The Forward Fund, Inc., on behalf of Forward:

The Stylized wordmark:[59] 

104. I have reviewed content published on **forward[.]pw** and have been unable to find the same or similar articles on forward.com. The **forward[.]pw** domain uses the registered mark of The Forward Fund, Inc.

105. Records received from Cloudflare Inc. pursuant to legal process, revealed that two Proton Mail email accounts purchased Cloudflare services for washingtonpost[.]pm, **fox-news[.]in**, and **fox-new[.]top**. The Cloudflare accounts associated with these two Proton Mail email accounts were each accessed from the same Netherlands IP address which resolves to a British VPS server leased by Doppelganger with an address ending in 11.27 (the "11.27 Server"). On January 2, 2024, a search warrant was authorized for the 11.27 Server. The 11.27 Server had been identified as having been created by the same user who created two other VPS servers from the same provider that were used by the Kamcopec persona to register foxnews[.]cx from Namecheap, Spiegel[.]ltd, fax[.]ltd, and welt[.]ltd from GoDaddy, and to access a Cloudflare account associated with Sueddeutsche[.]ltd.

[59] Registration number 5243694.

106. The true IP address[60] for **forward[.]pw** resolves to a Hostinger VPS IP address. Records received from Hostinger pursuant to legal process, reveal that the Hostinger VPS was leased by adampalmer1973[@]proton.me on May 18, 2023 using cryptocurrency. The account accessed the Hostinger VPS using all three of the Doppelganger Servers leased from the British provider, including the 11.27 Server.[61] Based on my training and experience, I know that when a person leases a VPS server, like the 11.27 Server, only that person or individuals they grant access to, can use that VPS server. Accordingly, I assess that any account or domain accessed from the 11.27 VPS server is a member of the Doppelganger conspiracy.

107. As described further above, the SUBJECT DOMAINS were used by Doppelganger as part of a foreign malign influence campaign carried out at the behest of the Russian government. SDA and STRUCTURA are Russian companies that list various Russian government entities as clients and that perform work for the Russian government.

The Unique Media Brand SUBJECT DOMAINS

108. As noted above, in addition to impersonating legitimate news outlets, Doppelganger, led by ANO Dialog and TABAK, under the direction and control of KIRIYENKO, a sanctioned person, also created original media brands (which are included among the SUBJECT DOMAINS). These brands purport to be independent journalists or news media organizations but are actually under the direction and control of the Russian government. The investigation has

[60] A true IP address for a domain is the server where the actual information that comprises the website or webpage resides. Accordingly, a True IP address for a domain is leased or purchased by the individual in control of the domain.

[61] As noted above, records received pursuant to legal process revealed that Doppelganger leased three servers from the Provider who provided the 11.27 Server in three-month intervals before switching to a new server from the same Provider.

revealed that as ANO Dialog created the domains for its purportedly unique media brands, it also registered email addresses that correspond to those domains.

A. RRN, War on Fakes, and the RovGeneral Persona

109. As discussed above, GAMBASHIDZE's notes from Presidential Administration meetings with KIRIYENKO document the use of Reliable Recent News ("RRN") by TABAK and ANO Dialog to further the malign influence campaign, noting "*They were assigned* Russian Reliable News – *changed it into* Recent, *it's going to work.(was sent by Tabak).*" RRN was hosted at rrn[.]world and published in numerous languages. As the Meta coordinated inauthentic behavior reports[62] note, RRN "maintain[ed] accounts on Twitter and Telegram, which were amplified by the operation's Facebook Pages. The Facebook Pages of the Russian diplomatic missions in Malaysia, Sweden, Hungary, Slovakia and Bangladesh shared links to the site." According to Meta, Doppelganger articles would often appear on RRN after they were posted on the cybersquatted domains: "For example, the same article about Bucha was published on the same day in English on the spoofed Guardian site, in Italian on the spoofed ANSA site, and in German on the spoofed Spiegel site. It also appeared in English, French, German, Italian, Spanish and Chinese on rrn[.]world."[63]

110. Information received from NameSilo, a U.S. company, pursuant to legal process revealed that the domain rrn[.]world was registered on June 6, 2022, by an identified individual,

[62] Starting on September 27, 2022, Meta released a series of reports regarding Doppelganger. These reports are available to the public on Meta's website.

[63] During the Russian occupation of Bucha, Ukraine, numerous reports of Russian war crimes were alleged. After the Russian military retreated from the town, independent journalists confirmed significant atrocities largely against the civilian population. *See* https://www.hrw.org/news/2022/04/21/ukraine-russian-forces-trail-death-bucha. "The Russian Defense Ministry denied allegations that its forces killed civilians in Bucha, stating in a Telegram post on April 3, [2022] that 'not a single local resident has suffered from any violent action' while Bucha was "under the control of the Russian armed forces,' and claiming instead that the evidence of crimes was a 'hoax, a staged production and provocation" by authorities in Kyiv." On July 7,

using a Moscow address, with email address reliablerecentnews[@]gmail.com. The individual applied for and received visas from the State Department to enter the United States from Russia in 2008, 2012, 2015, and 2019. Information received from Google pursuant to legal process revealed that reliablerecentnews[@]gmail.com was created on July 14, 2023, with the name Reliable Recent News, a recovery email of rrussianews[@]gmail.com and recovery telephone number that matched the number provided by the individual on her State Department applications.

111. I determined that rrn[.]world continued to post Doppelganger content until approximately July 10, 2024, when it appears ANO Dialog lost control of the domain. At some point shortly thereafter, unknown actors took over the domain and renamed it Rotten Reliable News and used the domain to publish information regarding Doppelganger's methods and activities, much of which I know to be accurate.

112. Records received pursuant to legal process from Namecheap, revealed that on July 26, 2023, a week after the VIGINUM report was published identifying rrn[.]world as part of Doppelganger, RoyGeneral[@]proton.me was used to register an account with Namecheap and lease **rrn[.]media** and **vip-news[.]org**. In registering that Namecheap account, the RoyGeneral persona provided a Beaverton, Oregon address and what appeared to be an incomplete U.S. phone number. Law Enforcement and open-source records checks indicate the name and home address provided are not correlated. Additionally, as further discussed below, the RoyGeneral persona also created an account with NameSilo to lease three more Doppelganger domains and provided a New York City address and Canadian phone number.

2022, RRN published an article titled "Video: False Staging in Bucha Revealed!" which falsely alleged the atrocities were staged by Ukraine.

113. On July 26, 2023, the RoyGeneral persona accessed Namecheap with an Estonian VPS IP address ending in 77.25 (the "77.25 Server") and deposited $55.00 with BitPay.[64] That same day, the RoyGeneral persona used $42.90 of the $55 deposited to lease **rrn[.]media**. Like the 11.27 Server, given the frequent use of the 77.25 Server by Doppelganger actors, I assess that the 77.25 Server was leased by Doppelganger and only accessible to persons involved in Doppelganger.

114. As discussed further below, the RoyGeneral, Goodbye, Levinaigrenet, Holylandherald, and Artichocio personas used the 77.25 Server to access their Namecheap accounts between February 27, 2023 and July 12, 2024. On at least four occasions, more than one Doppelganger persona accessed their Namecheap accounts at approximately the same times using this same IP address. This was not the only shared IP address. Between May 11, 2024 and July 1, 2024, the RoyGeneral, Levinaigrenet, Holylandherald, and Artichocio personas each accessed their Namecheap accounts on at least two occasions from the same Dutch IP address resolving to the same Russian VPS ending in 76.173 (the "76.173 Server"). Based on my training and experience, I know that unlike VPNs, which tend to be used once and discarded, when cyber-criminals lease a VPS they will frequently make use of that particular server for a period of time until the lease ends. For example, records received pursuant to legal process revealed that Doppelganger leased servers from the Provider who provided the 11.27 Server in three-month intervals before switching to a new server from the same Provider.

[64] As noted below, the persona responsible for leasing **levinaigre[.]net**, **warfareinsider[.]us**, and **meisterurian[.]io** also accessed Namecheap from the 77.25 Server. Likewise, the individual responsible for leasing **holylandherald[.]com**, **grenzezank[.]com**, and **lexomnium[.]com** also accessed Namecheap from the 77.25 Server.

115. On July 1, 2024, the RoyGeneral persona accessed Namecheap via three IP addresses, including a British IP address resolving to a Russian VPS that Spur has linked to a cybercriminal network, a Moscow IP address that Spur has linked to a cybercriminal network, and from the 76.173 Server. That same day, the RoyGeneral persona deposited $300.00 with BitPay and used $42.90 to renew the lease for **rrn[.]media** and $7.66 to lease **vip-news[.]org.** I reviewed materials posted on **rrn[.]media** and discovered that it uses the same logo and branding as the original rrn[.]world and continues to post content consistent with the malign influence campaign previously posted on rrn[.]world.

116. In addition, records received from OpenAI, a U.S.-based artificial intelligence research organization, revealed the purchase of multiple artificial intelligence program accounts, like ChatGPT, to generate and edit articles and comments specifically for rrn[.]media and other Doppelganger-linked domains. There were five email accounts used to register for OpenAI services linked to Doppelganger. Records received pursuant to legal process revealed one of those email accounts was connected by cookies to reliablerecentnews[@]gmail.com. Based on my training and experience, I know that when two or more accounts are linked by cookies, this means that the accounts were accessed using the same device(s) and are likely accessed by the same user(s). One of the other email accounts used to register for OpenAI was connected by cookies to 37 other email accounts. Almost all of these connected email accounts used naming conventions that corresponded to domains used by Doppelganger as part of their unique media branding operation, including some of the SUBJECT DOMAINS, as discussed further below.

117. One of the SUBJECT DOMAINS, **waronfakes[.]com,** was discussed in length in the VIGINUM report:

> The first articles published on RRN website were identical copies of articles previously published on the fake Russian fact-checking website War on Fakes,

> launched a few hours after Russia invaded Ukraine. Quickly identified for its role in legitimizing the Russian 'special military operation' and discrediting the Ukrainian State, War on Fakes has also been amplified by at least 65 official Facebook pages and official Twitter accounts of the Russian diplomatic network. Moreover, War on Fakes the administrator's login page has been set up to redirect traffic to rrussianews.com, thereby establishing a technical link between the two websites. The domain name **waronfakes[.]com** was registered on 1 March 2022 and was updated a year later by Timofey VASILIEV a Russian citizen known for having worked for ANO Dialog. Dialog is an organization created in 2019 under the supervision of the Russian Presidential Administration and the Department of Information Technologies of Moscow city. In charge of a portion of the public relations and communication strategy of Moscow, ANO Dialog has been accused of conducting online propaganda activities on behalf of the Russian State.[65]

118. As noted in the VIGINUM report, the administrator's login page for **waronfakes[.]com** redirected traffic to rrussianews.com. The corresponding email address for rrussianews.com, rrussiannews[@]gmail.com was the recovery email for the above-described Russian citizen's reliablerecentnews[@]gmail.com account, which in turn was used to register the rrn[.]world domain. In addition, SDA records revealed that GAMBASHIDZE had the resume of an individual assessed to be working for Doppelganger, who described their experience from October 2022 to present as a writer for the Telegram channel war on fakes, with duties including writing posts for the channel war on fakes and war on fakes analytics, and working on translations and open-source research. **Waronfakes[.]com** is leased from an overseas registrar which leases the domain from the U.S. registry, VeriSign Global Registry Services ("VeriSign"). Accordingly, there is probable cause to believe that when ANO Dialog renews the lease on the domain, a portion of those funds are used by the overseas registrar to pay VeriSign in the United States for the benefit of sanctioned persons.

[65] Available at https://www.sgdsn.gouv.fr/files/files/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN1.pdf

B. Other Doppelganger Media Brands

119. Based on records received pursuant to legal process, open-source research, the content of articles published on the domains, and information obtained throughout this investigation, I assess that each of the SUBJECT DOMAINS listed below is part of Doppelganger.

1. *The Demon Accounts*

120. As noted above in paragraph 116, five email accounts were identified as using OpenAI services in furtherance of Doppelganger. Records received from Google pursuant to legal process revealed that one of those accounts (the "Demon Account") was subscribed in the name of "White Seo." When it was registered, the Demon Account selected Russian as its language, listed a Russian recovery email ending in .ru with the same naming convention, namely "Demon" followed by a string of numbers, and provided a Russian phone number. The Demon Account was linked by cookies to 37 other email accounts with naming conventions that correspond to domains connected to Doppelganger's unique media branding operation, including some of the SUBJECT DOMAINS, such as:

Email Account Linked by Cookies to the Demon Account	**Corresponding SUBJECT DOMAIN**
holylandheraldcom[@]gmail.com	**holylandherald[.]com**
mypride.press[@]gmail.com	**mypride[.]press**
liesofwallstreet.com[@]gmail.com	**liesofwallstreet[.]io**
50statesoflie.com[@]gmail.com	**50statesoflie[.]media**
ukrlm.info[@]gmail.com	**ukrlm[.]info**
meisteruiancom[@]gmail.com	**meisterurian[.]io**
Acrosstheline.press[@]gmail.com	**acrosstheline[.]press**
Electionwatch.live[@]gmail.com	**electionwatch[.]io**

Honeymoney.infonow[@]gmail.com	**honeymoney.press**
Uschina.press.now[@]gmail.com	**uschina[.]online**
Spicyconspiracy.info[@]gmail.com	**spicyconspiracy[.]io**
Levinaigre.net[@]gmail.com	**levinaigre[.]net**

2. *The Goodbye Persona Leased the **Acrosstheline[.]press, ukrlm[.]info**, and **mypride[.]press** Domains Linked to the Demon Account*

121. Two Proton Mail email accounts, Aurevourmail[@]proton.me and Buenasnochesmail[@]proton.me, (collectively, the "Goodbye persona"), leased domains from Namecheap for use in the Doppelganger campaign, including **acrosstheline[.]press**,[66] **ukrlm[.]info**,[67] and **mypride[.]press**.[68] Given that these Proton Mail addresses included derivations of a phrase roughly translated into two languages: Au Revoir and Buenas Noches, I assess that the Namecheap accounts were created using operational email addresses by ANO Dialog employees or agents acting on their behalf and will refer to them collectively as the Goodbye persona.

122. Records received from Namecheap pursuant to legal process revealed that the Goodbye persona leased **acrosstheline[.]press**, **ukrlm[.]info**, and **mypride[.]press** using the 77.25 Server and paid for them using a U.S.-based payment provider, called BitPay, which allows

[66] Across the Line presents itself as a website focused on migration and forced displacement issues, often presenting only an adverse perspective as it relates to the U.S. Its website footer notes, "Join us in tackling the problems of refugees across the globe and at the US border. Let's cross the line to support those who didn't ask to leave their homes and face uncertainty."

[67] UKRLM is an English language website that describes itself as "Bringing you the latest updates, analysis, and insights from war-torn Ukraine. Stay informed on the ongoing Russia-Ukraine conflict with us."

[68] My Pride Press is an English language website that focuses on the LGBTQ community, with topics including trans youth, athletes, health, woke wars, LGBT.

users to make payments via Bitcoin. Records received pursuant to legal process from Namecheap and BitPay revealed the following:

a. On February 27, 2023, the Goodbye persona, using the 77.25 Server, sent 0.002612 BTC, equivalent to $60.46, from a Bitcoin address ending in -MiP6T to Namecheap. The same day, Namecheap credited the Goodbye persona account with $60.00 and the account used $53.12 to lease **acrosstheline[.]press**, **ukrlm[.]info**, and **mypride[.]press** which included a $38.64 monthly subscription for EasyWP, a Namecheap product for managing websites.

b. On March 21, 2023, the Goodbye persona, using the 77.25 Server, sent 0.001486 BTC, equivalent to $40.84, from a Bitcoin address ending in -JPrHF to Namecheap. The same day, Namecheap credited the Goodbye persona account with $40.00, which prevented the previously mentioned subscription from overdrawing the account.

c. On April 20, 2023, the Goodbye persona, using the 77.25 Server, sent 0.003881 BTC, equivalent to $110.62, from a Bitcoin address ending in -mhtcF to Namecheap. The same day, Namecheap credited the Goodbye persona account with $110.00, which prevented the previously mentioned subscription from overdrawing the account.

d. On July 23, 2023, the Goodbye persona, using a German IP address that Spur has linked to a cybercriminal network, sent 0.006791 BTC, equivalent to $202.51, from a Bitcoin address ending in -Z2my to Namecheap. The same day, Namecheap credited the Goodbye persona account with $200.00, which prevented the previously mentioned subscription from overdrawing the account.

e. On December 15, 2023, the Goodbye persona, using a German IP address that Spur has linked to a cybercriminal network, sent 0.002147 BTC, equivalent to $89.99, from a Bitcoin address ending in – qpwW to Namecheap. The same day, Namecheap credited the Goodbye persona account with $70.00, which prevented the previously mentioned subscription from overdrawing the account.

f. On July 23, 2023, the Goodbye persona, using a German IP address that Spur has linked to a cybercriminal network, sent 0.004861 BTC, equivalent to $206.86, from a Bitcoin address ending in -Z2my to Namecheap. The same day, Namecheap credited the Goodbye persona account with $205.00 and the account used $89.48 to renew their lease of **acrosstheline[.]press**, **ukrlm[.]info**, and **mypride[.]press**.

123. Based on these BitPay transactions, the IP addresses, and my training and experience, there is probable cause to believe the funds used to lease these three SUBJECT DOMAINS originated from outside the United States.

3. *The Levinaigrenet Persona Leased the **Levinaigre[.]net**, and **Meisterurian[.]io** Domains Linked to the Demon Account and **Warfareinsider[.]us**.*

124. Records received from Namecheap pursuant to legal process revealed that a user with the email address levinaigrenet[@]proton.me leased **levinaigre[.]net**,[69] **meisterurian[.]io**,[70] and **warfareinsider[.]us**.[71] The Levinaigrenet persona provided Namecheap with a name of Jay Rom and a Broken Bow, Nebraska mailing address. All payments were made using funds transferred from BitPay. Law enforcement records checks reveal no association between a Jay

[69] Levinaigre is a French language website that focuses on French scandals.

[70] Meisterurian is a German language website that purports to publish German news stories.

[71] Warfareinsider is an English language website that describes itself as reporting on "Latest military news. Stay sharp to look at it from the different perspective."

Rom and the physical mailing address in Nebraska provided to Namecheap. In addition, despite indicating a U.S. mailing address, on June 16, 2023, the Levinaigrenet persona accessed Namecheap via the 77.25 Server and, using BitPay, deposited $72.00. On June 19, 2023, the Levinaigrenet persona used the 77.25 Server to access Namecheap and used $25.04 to lease **levinaigre[.]net** and purchase a monthly subscription of EasyWP. Then, on July 5, 2023, the Levinaigrenet persona accessed Namecheap via a French IP address that Spur linked to a cybercriminal network and, using BitPay, deposited $120.00. The same day the Levinaigrenet persona used $70.22 to lease **warfareinsider[.]us** and **meisterurian[.]io** and purchase monthly subscriptions of EasyWP for both. On June 4, 2024, the Levinaigrenet persona accessed Namecheap via the 76.173 Server. and, using BitPay, deposited $200.00. The same day the account used $10.48 to renew the lease for **warfareinsider[.]us** and **meisterurian[.]io.**

125. As discussed below, on both June 16 and 19, 2023, another Doppelganger linked Namecheap account also used the 77.25 Server to access their Namecheap account. Accordingly, although the Levinaigrenet persona provided Namecheap with a U.S. address, I assess that the individual accessing and paying for the account is actually located overseas.

4. *The Holylandherald Persona Leased the **Holylandherald[.]com** Domain Linked to the Demon Account and **Grenzezank[.]com**, and **Lexomnium[.]com***

126. Records received from Namecheap pursuant to legal process revealed that a user with the email address holylandheraldcom[@]proton.me leased **holylandherald[.]com**,[72] **grenzezank[.]com**,[73] and **lexomnium[.]com**.[74] The Holylandherald persona provided Namecheap

[72] Holyland Herald poses as an Israeli based English language news website focused on Israel-US relations, the war in Gaza, and other Middle East issues, however it also posted articles related to Ukraine, such as an article titled "Ukraine Interferes in Russian Presidential Elections."

[73] Grenzezank is a German language website that focuses on international news, including U.S. politics.

[74] Lex omnium, which translates to The Law of All in Latin, is a French language website that appears to focus on French news with a legal perspective.

with a first name of holyland, a last name of herald, and a mailing address in Kansas City, Missouri that indicated the country of residence to be Germany. All payments for the domains were made using funds transferred from BitPay.

127. Specifically, on June 16, 2023, the Holylandherald persona accessed Namecheap via the 77.25 Server and, using BitPay, deposited $65.00. On June 19, 2023, the Holylandherald persona accessed their Namecheap account using the 77.25 Server and used $22.64 to lease **holylandherald[.]com** and purchase a monthly subscription of EasyWP. As referenced above, records received from Namecheap revealed that the account used to lease **Levinaigre[.]net**, **meisterurian[.]io**, and **warfareinsider[.]us** accessed Namecheap from the same server at approximately the same time. On April 16, 2024, the Holylandherald persona accessed Namecheap via a U.S. IP address that Spur has linked to a cybercriminal network and, using BitPay, deposited $104.00. On May 20, 2024, Namecheap charged the account $16.06 to renew the lease for **holylandherald[.]com.**

128. On July 5, 2023, the Holylandherald account accessed Namecheap via a German IP address that Spur has linked to a cybercriminal network and, using BitPay, deposited $120.00. The same day the account used $45.28 to lease **grenzezank[.]com** and **lexomnium[.]com** and purchase monthly subscriptions of EasyWP for both. On May 31, 2024, the account accessed Namecheap via the 76.173 Server. and, using BitPay, deposited $100.00. The same day the account used $32.12 to renew the lease for **grenzezank[.]com** and **lexomnium[.]com**.

5. *The RoyGeneral Persona Leased the **50statesoflie[.]media**, **uschina[.]online**, and **HoneyMoney[.]press** Linked to the Demon Account*

129. As referenced above, the Doppelganger campaign created email addresses with a naming convention that correspond to **50statesoflie[.]media**,[75] **honeymoney[.]press**,[76]and **uschina[.]online**.[77] The registrar for all three of those domains was NameSilo and the domains were leased, from QHoster, a Uruguayan domain reseller,[78] using RoyGeneral[@]proton.me. Records received pursuant to legal process from NameSilo, revealed that the RoyGeneral persona created a QHoster account, using a New York, New York address and a Canadian phone number and leased the **50statesoflie[.]media**, **uschina[.]online**, and **honeymoney[.]press**. Law enforcement and open-source records checks indicate the name and home address provided are not correlated. As referenced above in paragraph 112, the RoyGeneral persona also leased **rrn[.]media** and **vip-news[.]org** but provided an Oregon address and an incomplete U.S. telephone number. At least one article published on **honeymoney[.]press** focused on the current U.S. Presidential administration's stance on Ukraine. Although the RoyGeneral persona provided NameSilo with a U.S. address, based on the RoyGeneral's use of VPSs with Namecheap, links to other Doppelganger actors, and leasing of **rrn[.]media** and **waronfakes[.]com**, I assess that the individual accessing and paying for the RoyGeneral account is actually located overseas.

130. Mandiant, an American cybersecurity firm and a subsidiary of Google, tracks the "Doppelganger Information Operations Campaign" and publishes a monthly report with updates

[75] 50 States of Lie describes itself as "Exposing the scandals that shape American politics and culture. We bring you the latest on corruption, cover-ups, and controversies in the land of the free."

[76] Honey Money Press is an English language website that focuses on U.S. consumer trends.

[77] US China Online on issues related to China's national interest, including U.S.-China relations, Taiwan, and U.S. trade and foreign policies.

[78] A reseller is a third-party company that offers domain name registration services through a registrar, in this case NameSilo, a U.S. company.

to the state of the campaign in a document Mandiant calls a "Narrative Tracker." In their April 2024 report, Mandiant noted in addition to the continued use of cybersquatted websites, the Doppelganger campaign had begun using the following domains to target American audiences: Election Watch (electionwatch[.]live), Spicy Conspiracy (spicyconspiracy[.]info), 50 States of Lie (50statesoflie[.]com), and Dragonfly Times (uschina[.]press). Of note, records received from Hostinger pursuant to legal process, showed that the Goodbye persona leased Electionwatch[.]live, 50statesoflie[.]com, and uschina[.]press on February 23, 2023, using cryptocurrency transferred using CoinGate, a Lithuanian cryptocurrency payment processor.

131. As noted above, the Demon Account created email addresses that correspond directly to spicyconspiracy[.]io[79] and electionwatch[.]io.[80] At present, electionwatch[.]live, spicyconspiracy[.]info, 50statesoflie[.]com, and uschina[.]press are no longer active. However, I have reviewed the active domains **50statesoflie[.]media, uschina[.]online,** spicyconspiracy[.]io, and electionwatch[.]io and have confirmed that they use the same branding and formatting as electionwatch[.]live, spicyconspiracy[.]info, 50statesoflie[.]com, and uschina[.]press, which leads me to conclude that the same person(s) are behind these domains.

6. *The Artichocio persona leased **truthgate[.]us, shadowwatch[.]us,**[81] and **artichoc[.]io,**[82]*

132. Records received from Namecheap revealed that an individual using the email address artichocio[@]proton.me leased **truthgate[.]us**, **shadowwatch[.]us**, and **artichoc[.]io**, and

[79] Spicy Conspiracy describes itself as "Uncovering the truth behind the veil. Your source for in depth coverage of conspiracies, secret agendas, and hidden realities."

[80] Election Watch focuses on U.S. elections, including the 2024 U.S. presidential election, political candidates, purported corruption, and polling results.

[81] Truth Gate and Shadow Watch are English language websites that focused on disseminating corruption and conspiracy disinformation targeting the U.S.

[82] Artichoc io is a French language website with a tagline that translates to "Art that Shocks." It purports to

provided the name Jason Kant with a French mailing address and a U.S. phone number. The domains were purchased using Bitcoin transferred through BitPay.

133. June 29, 2023, the Artichocio persona used the 77.25 Server to access Namecheap and deposit $120.00 using BitPay. As discussed above, given the frequent use of the 77.25 Server by Doppelganger actors, I assess that the 77.25 Server was leased by Doppelganger and only accessible to persons involved in Doppelganger. The same day, the Artichocio persona used $52.86 to lease **artichoc[.]io** and purchase a monthly subscription of EasyWP. On April 16, 2024, the artichocio account accessed Namecheap via a German IP address that Spur has linked to a cybercriminal network and, using BitPay, deposited $92.00. On May 30, 2024, Namecheap charged the artichocio account $48.98 to renew the lease for **artichoc[.]io**.

134. On July 5, 2023, the artichocio account accessed Namecheap via a U.S. IP address resolving to a British VPS service and, using BitPay, deposited $120.00. The same day, the artichocio account used $34.72 to lease **truthgate[.]us** and **shadowwatch[.]us** and purchase monthly subscriptions of EasyWP for both. On June 18, 2024, the artichocio account accessed Namecheap from the 76.173 Server and, using BitPay, deposited $220.00. The same day, the account used $20.96 to renew the lease for **truthgate[.]us** and **shadowwatch[.]us**.

7. *The Ukraine Domains*

135. As noted above, one of GAMBASHIDZE's notes from a meeting with the Presidential Administration referenced a participant as "*fully in charge of filling the content on the Ukraine Tribunal portal*." Two Doppelganger-linked domains, **tribunalukraine[.]info**,[83] and

focus on pop culture, art, and entertainment.

[83] Tribunal Ukraine is a German language website a focus on revealing the alleged truth about what is happening in Ukraine.

ukraine-inc[.]info,[84] were leased from Newfold Digital, a U.S. registrar. Records received from Newfold Digital revealed that ukraine-inc[.]info was registered on November 3, 2023. Those records also revealed that the email address trelelcalra1975[@]yahoo.com, was used to lease ukraine-inc[.]info**.** The trelelcalra1975[@]yahoo.com was only logged into five times, four times from German VPSs and once from a Russian IP address. The trelelcalra1975[@]yahoo.com user registered their Newfold Digital account in the name of Dennis Eggers with a German mailing address and German phone number. Subscriber records received from Yahoo Inc. revealed that the trelelcalra1975[@]yahoo.com account was registered using a Cyrillic first name and the last name Reddy and a Brazilian phone number, which does not match the information provided to Newfold Digital.

136. Records received from Newfold Digital revealed that **tribunalukraine[.]info** was registered on June 10, 2022. Those records revealed that the email address glennwallace9672[@]outlook.com was used to lease **tribunalukraine[.]info.** The glennwallace9672[@]outlook.com user registered their Newfold Digital account in the name of Glen Wallace with a Vienna mailing address and an Austrian phone number. Records received from Microsoft revealed that glennwallace9672[@]outlook.com was registered by Glenn Wallace from Austria. Notably, that Outlook account was only logged into twice, September 28, 2022, and October 5, 2022. According to records received from Newfold Digital, the Newfold Digital account for **tribunalukraine[.]info** was accessed from the 11.27 Server.

[84] Ukraine Inc is an English language website that features animated anti-Ukrainian videos. The videos contain anti-Semitic tropes that depict Ukrainian President Zelensky as an alcoholic and imply that the deaths of Ukrainians benefit him financially.

THE SUBJECT DOMAINS

137. As described above, the SUBJECT DOMAINS were used by individuals abroad who are working under the direction and control of the Russian government, and in particular KIRIYENKO, GAMBASHIDZE, SDA, TUPIKIN, and STRUCTURA, all of whom have been sanctioned by the U.S. Government, along with ANO Dialog, TABAK, and others, to advance their interests and the interests of the Russian government and to facilitate the violation of, or in violation of, the SUBJECT OFFENSES.

138. As set forth above and in Attachments A-1 through A-9, a search of publicly available Who.is domain name registration records revealed the dates that the SUBJECT DOMAINS were registered, with which registrar, the headquarters of that registrar, the registrant of each of the SUBJECT DOMAINS, and the top-level domain for each of the SUBJECT DOMAINS.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

139. Title 18, United States Code, Section 981(a)(1)(A) provides, in relevant part, that any property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956(a)(2)(A) (international promotional money laundering) and 1956(h) (conspiracy to commit the same) is subject to civil forfeiture.

140. Title 18, United States Code, Section 2323(a)(1)(B), provides, in relevant part, that any property used, or intended to be used, in any manner or part to commit or facilitate the commission of Trafficking in Counterfeit Goods or Services (e.g., trademark infringement), in violation of 18 U.S.C. § 2320, is subject to civil forfeiture to the United States government.

141. Title 18, United States Code, Section 981(b)(2) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause and "obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Forfeiture."

142. Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and such warrant may be executed in any district in which the property is found, and provides that the warrant may be executed in any district in which the property is found or transmitted to the central authority of a foreign state for service in accordance with any treaty or other international agreement.

143. Title 18, United States Code, Section 982(a)(1) provides, in relevant part, that when imposing sentence on a person convicted of an offense in violation of 18 U.S.C. § 1956(a)(2)(A) (international promotional money laundering) and 1956(h) (conspiracy to commit the same), a court shall order that person's property that was involved in the offense be forfeited to the United States.

144. Title 18, United States Code, Section 2323(b)(1), provides, in relevant part, that the court, in imposing sentence on a person convicted of Trafficking in Counterfeit Goods or Services (e.g., trademark infringement), in violation of 18 U.S.C. § 2320, an offense under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title, shall order, in addition to any other sentence imposed, that the person forfeit to the United States Government any property subject to forfeiture under 18 U.S.C. § 2323(a) for that offense.

145. Title 18, United States Code, Section 982(b)(1) incorporates by reference the procedures for seizure and forfeiture in 21 U.S.C. § 853. Title 21, United States Code, Section 853(f) provides in relevant part that a seizure warrant for property subject to forfeiture may be

sought "in the same manner in which a search warrant may be issued. A court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture."

146. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the SUBJECT DOMAINS for forfeiture. By seizing the SUBJECT DOMAINS and redirecting them to another website(s), the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the SUBJECT DOMAINS will prevent third parties from continuing to access the SUBJECT DOMAINS in their present form.

147. Title 18, United States Code, Section 2323(a)(1)(B), provides, in relevant part, that any property used, or intended to be used, in any manner or part, to commit or facilitate the commission of Trafficking in Counterfeit Goods or Services (e.g., trademark infringement), in violation of 18 U.S.C. § 2320, is subject to civil forfeiture. Title 18, United States Code, Section 2323(b)(1), provides, in relevant part, that the court, in imposing sentence on a person convicted of Trafficking in Counterfeit Goods or Services (e.g., trademark infringement), in violation of 18 U.S.C. § 2320, shall order, in addition to any other sentence imposed, that the person forfeit to the United States Government any property subject to forfeiture under 18 U.S.C. § 2323(a).

148. Title 18, United States Code, Section 981(h) provides that venue for civil forfeitures brought under this section lies in the district either where the defendant owning the property is located or in the judicial district where the criminal prosecution is brought.

149. Title 18, United States Code, Section 981(b)(3) provides that a seizure warrant may be issued in any district in which a forfeiture action against the property may be filed under 28 U.S.C. § 1355(b).

150. Title 28, United States Code, Section 1355(b)(1)(A), provides that a forfeiture action or proceeding may be brought in a district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred.

151. Title 21, United States Code, Section 853(l) provides that the district courts of the United States having jurisdiction to enter orders, including seizure warrants, without regard to the location of property which may be subject to criminal forfeiture under § 853.

152. As set forth above, there is probable cause to believe that the SUBJECT DOMAINS are subject to civil and criminal forfeiture because they are property involved in in the commission of violations of 18 U.S.C. § 1956(a)(2)(A) (international promotional money laundering) and 1956(h) (conspiracy to commit same). Specifically, the SUBJECT DOMAINS are property involved in transactions or attempted transactions that violate 18 U.S.C. § 1956(a)(2)(A) (international promotional money laundering) and 1956(h) (conspiracy to commit same), done with the intent to promote the carrying on of specified unlawful activity, specifically violations of IEEPA. Further, as set forth above, there is probable cause to believe that a subset of the SUBJECT DOMAINS are subject to civil and criminal forfeiture because they are property that facilitated the commission of Trafficking in Counterfeit Goods or Services (e.g., trademark infringement), in violation of 18 U.S.C. § 2320.

153. Venue for civil and criminal forfeiture is proper in this district pursuant to 18 U.S.C. § 981(b)(3) and (h), 28 U.S.C. § 1355(b)(1)(A), and 21 U.S.C. § 853(l), as set forth above, as the government has venue to charge the above described international promotional money laundering,

conspiracy to commit the money laundering, and trafficking in counterfeit goods or services offenses in the Eastern District of Pennsylvania. In addition, as part of the money laundering conspiracy to promote violations of IEEPA, the conspirators took steps to make the SUBJECT DOMAINS available on the internet, including in the Eastern District of Pennsylvania and the defendants used a subset of the SUBJECT DOMAINS to commit or facilitate the commission of Trafficking in Counterfeit Goods or Services, including in the Eastern District of Pennsylvania.

SEIZURE PROCEDURE

154. As detailed in Attachments A-1 through A-9, upon execution of the seizure warrant, the registry or registrar for the top-level domain or for each SUBJECT DOMAIN (collectively, the "PROVIDERS"), shall be directed to restrain and lock the SUBJECT DOMAINS pending transfer of all right, title, and interest in the SUBJECT DOMAINS to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAINS cannot be made absent court order or, if forfeited to the United States, without prior consultation with the Federal Bureau of Investigation or DOJ.

155. In addition, upon seizure of the SUBJECT DOMAINS by the Federal Bureau of Investigation, the PROVIDERS will be directed to associate the SUBJECT DOMAINS to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which the SUBJECT DOMAINS will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

REQUEST FOR SEALING

156. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the

targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

CONCLUSION

157. For the foregoing reasons, I submit that there is probable cause to believe that the SUBJECT DOMAINS are used in and/or intended to be used in facilitating and/or committing the SUBJECT OFFENSES. Accordingly, the SUBJECT DOMAIN NAMES are subject to seizure pursuant to 18 U.S.C. §§ 981(b), 982(b)(1), 2323(a)(2), 2323(b)(2), 21 U.S.C. § 853(f), and subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a), and 18 U.S.C. § 2323(a)(1)(B), (b)(1), and I respectfully request that the Court issue a seizure warrant for SUBJECT DOMAIN NAMES.

158. Because the warrant will be served on the PROVIDERS that control the SUBJECT DOMAINS, and the PROVIDERS, thereafter, at a time convenient to them, will transfer control of the SUBJECT DOMAINS to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

[redacted]

Special Agent, Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 30th day of August, 2024 at 9:34pm.

[redacted]
Digitally signed by [redacted]
Date: 2024.08.30 22:19:07 -04'00'

United States Magistrate Judge

ATTACHMENT A-1

With respect to **tribunalukraine.info**, **rrn.media**, **ukrlm.info**, **faz.ltd, spiegel.agency**, **lemonde.ltd**, **leparisien.ltd**, **rbk.media, 50statesoflie.media**, **meisterurian.io**, **artichoc.io** ("SUBJECT DOMAINS"), Identity Digital, located at 10500 NE 8th Street, Ste. 750 Bellevue, WA 98004, who is the domain registry for the SUBJECT DOMAINS, shall take the following actions to effectuate the seizure of SUBJECT DOMAINS:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the SUBJECT DOMAINS to the following authoritative name-server(s)**:**

    (a) Ns1.fbi.seized.gov;

    (b) Ns2.fbi.seized.gov; and/or

    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to Identity Digital Limited.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAINS pending transfer of all right, title, and interest in SUBJECT DOMAINS to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAINS cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAINS will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981(b), 982(b)(1), 2323(a)(2), 2323(b)(2), 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Pennsylvania as part of a law enforcement action by the Federal Bureau of Investigation."

ATTACHMENT A-2

With respect to **vip-news.org**, **acrosstheline.press**, **mypride.press, truthgate.us, warfareinsider.us, shadowwatch.us** ("SUBJECT DOMAINS"), NameCheap, located at 4600 East Washington Street Suite 300 Phoenix, AZ 85034, who is the domain registrar for the SUBJECT DOMAINS, shall take the following actions to effectuate the seizure of SUBJECT DOMAINS:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the SUBJECT DOMAINS to the following authoritative name-server(s)**:**

    (a) Ns1.fbi.seized.gov;

    (b) Ns2.fbi.seized.gov; and/or

    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to Namecheap.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAINS pending transfer of all right, title, and interest in SUBJECT DOMAINS to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAINS cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAINS will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981(b), 982(b)(1), 2323(a)(2), 2323(b)(2), 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Pennsylvania as part of a law enforcement action by the Federal Bureau of Investigation."

ATTACHMENT A-3

With respect to **pravda-ua.com**, **waronfakes.com**, **holylandherald.com**, **levinaigre.net**, **grenzezank.com**, **lexomnium.com** ("SUBJECT DOMAINS"), VeriSign Global Registry Services, located at 12061 Bluemont Way, Reston, VA 20190, who is the domain registry for the SUBJECT DOMAINS, shall take the following actions to effectuate the seizure of SUBJECT DOMAINS:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the SUBJECT DOMAINS to the following authoritative name-server(s)**:**

    (a) Ns1.fbi.seized.gov;

    (b) Ns2.fbi.seized.gov; and/or

    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to VeriSign Global Registry Services.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAINS pending transfer of all right, title, and interest in SUBJECT DOMAINS to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAINS cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAINS will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981(b), 982(b)(1), 2323(a)(2), 2323(b)(2), 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Pennsylvania as part of a law enforcement action by the Federal Bureau of Investigation."

ATTACHMENT A-4

With respect to **uschina.online**, **honeymoney.press** ("SUBJECT DOMAINS"), NameSilo, located at 1300 E Missouri Ave Ste A-110 Phoenix, AZ 85014-2362 who is the domain registrar for the SUBJECT DOMAINS, shall take the following actions to effectuate the seizure of SUBJECT DOMAINS:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the SUBJECT DOMAINS to the following authoritative name-server(s)**:**

    (a) Ns1.fbi.seized.gov;

    (b) Ns2.fbi.seized.gov; and/or

    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to NameSilo.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAINS pending transfer of all right, title, and interest in SUBJECT DOMAINS to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAINS cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAINS will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981(b), 982(b)(1), 2323(a)(2), 2323(b)(2), 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Pennsylvania as part of a law enforcement action by the Federal Bureau of Investigation."

ATTACHMENT A-5

With respect to **sueddeutsche.co**, **tagesspiegel.co** ("SUBJECT DOMAINS"), GoDaddy.com LLC., located at 100 S. Mill Ave Suite 1600 Tempe, AZ 85281 USA, who is the domain registrar for the SUBJECT DOMAINS, shall take the following actions to effectuate the seizure of SUBJECT DOMAINS:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the SUBJECT DOMAINS to the following authoritative name-server(s)**:**

    (a) Ns1.fbi.seized.gov;

    (b) Ns2.fbi.seized.gov; and/or

    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to GoDaddy.com LLC.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAINS pending transfer of all right, title, and interest in SUBJECT DOMAINS to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAINS cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAINS will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981(b), 982(b)(1), 2323(a)(2), 2323(b)(2), 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Pennsylvania as part of a law enforcement action by the Federal Bureau of Investigation."

ATTACHMENT A-6

With respect to **bild.work** ("SUBJECT DOMAIN"), GoDaddy Registry Services, LLC, located at 100 S. Mill Ave Suite 1600 Tempe, AZ 85281 USA, who is the domain registry for the SUBJECT DOMAIN, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the SUBJECT DOMAIN to the following authoritative name-server(s)**:**

    (a) Ns1.fbi.seized.gov;

    (b) Ns2.fbi.seized.gov; and/or

    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to GoDaddy Registry Services, LLC.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAIN pending transfer of all right, title, and interest in SUBJECT DOMAIN to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAIN will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981(b), 982(b)(1), 2323(a)(2), 2323(b)(2), 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Pennsylvania as part of a law enforcement action by the Federal Bureau of Investigation."

ATTACHMENT A-7

With respect to **fox-news.top**, **fox-news.in** ("SUBJECT DOMAINS"), Tucows Inc., 10400 NE 4th Street, 5th Floor, Suite 121, Bellevue, Washington 98004 who is the domain registrar for the SUBJECT DOMAINS, shall take the following actions to effectuate the seizure of SUBJECT DOMAINS:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the SUBJECT DOMAINS to the following authoritative name-server(s)**:**

    (a) Ns1.fbi.seized.gov;

    (b) Ns2.fbi.seized.gov; and/or

    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to Tucows Inc.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAINS pending transfer of all right, title, and interest in SUBJECT DOMAINS to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAINS cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAINS will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981(b), 982(b)(1), 2323(a)(2), 2323(b)(2), 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Pennsylvania as part of a law enforcement action by the Federal Bureau of Investigation."

ATTACHMENT A-8

With respect to **forward.pw** ("SUBJECT DOMAIN"), Micronesia Investment and Development Corporation, located at P.O. Box 1256 Koror 96940, Palau who is the domain registry for the SUBJECT DOMAIN, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the SUBJECT DOMAIN to the following authoritative name-server(s)**:**

    (a) Ns1.fbi.seized.gov;

    (b) Ns2.fbi.seized.gov; and/or

    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to Micronesia Investment and Development Corporation.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAIN pending transfer of all right, title, and interest in SUBJECT DOMAIN to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAIN will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981(b), 982(b)(1), 2323(a)(2), 2323(b)(2), 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Pennsylvania as part of a law enforcement action by the Federal Bureau of Investigation."

ATTACHMENT A-9

With respect to **washingtonpost.pm** ("SUBJECT DOMAIN"), Sarek Oy, located at Urho Kekkosen katu 4E 00100, HELSINKI, Uusimaa Finland, who is the domain registry for the SUBJECT DOMAIN, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the SUBJECT DOMAIN to the following authoritative name-server(s)**:**

    (a) Ns1.fbi.seized.gov;

    (b) Ns2.fbi.seized.gov; and/or

    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to Sarek Oy.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAIN pending transfer of all right, title, and interest in SUBJECT DOMAIN to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAIN will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981(b), 982(b)(1), 2323(a)(2), 2323(b)(2), 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Pennsylvania as part of a law enforcement action by the Federal Bureau of Investigation."