USDS SDNY
DOCUMENT
ELECTRONICALLY FILED
[redacted]:
DATE FILED: July 30, 2019

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DEMOCRATIC NATIONAL COMMITTEE,

Plaintiff,

- against -

THE RUSSIAN FEDERATION et al.,

Defendants.

18cv3501 (JGK)

OPINION AND ORDER

JOHN G. KOELTL, District Judge:

The plaintiff, the Democratic National Committee ("DNC"), brings this action against Donald J. Trump For President, Inc. ("the Campaign"); Donald J. Trump, Jr. ("Trump Jr."); Paul J. Manafort, Jr.; Jared C. Kushner; George Papadopoulos; and Richard W. Gates, III (collectively, the "campaign defendants"); Roger J. Stone, Jr.; the Russian Federation; Aras Iskenerovich Agalarov; Emin Araz Agalarov; Joseph Mifsud; WikiLeaks; and Julian Assange.[1]

The action arises out of the alleged actions of the Russian Federation in unlawfully hacking into the DNC's computers in connection with the 2016 presidential election and thereafter distributing stolen materials from those computers, particularly

[1] In the original complaint, the DNC also named as defendants the General Staff of the Armed Forces of the Russian Federation, the Russian operative using the pseudonym Guccifer 2.0, and 10 John Doe defendants. (Dkt. No. 1.) Those defendants were not named in the Second Amended Complaint. (Dkt. No. 217.)

through WikiLeaks, who in turn made those materials publicly available. While there are no plausible allegations that the remaining defendants participated in the unlawful hacking or in the dissemination of the materials by WikiLeaks, the DNC alleges that the dissemination of those materials furthered the prospects of the Trump Campaign and that the remaining defendants "welcomed" the assistance in various ways.

In the Second Amended Complaint, the DNC asserts claims under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962 ("RICO"); Wiretap Act, 18 U.S.C. §§ 2510-22; Stored Communications Act, 18 U.S.C. §§ 2701-12; Digital Millennium Copyright Act, 17 U.S.C. § 1201 et seq.; Defend Trade Secrets Act, 18 U.S.C. § 1831 et seq.; Washington, D.C. Uniform Trade Secrets Act, D.C. Code Ann. §§ 36-401 to 46-410; and Virginia Computer Crimes Act, Va. Code Ann. § 18.2-152.5 et seq. The DNC also asserts claims under Washington, D.C. common law for trespass and conversion and claims under Virginia common law for conversion, trespass to chattels, and conspiracy to commit trespass to chattels.

The primary wrongdoer in this alleged criminal enterprise is undoubtably the Russian Federation, the first named defendant in the case and the entity that surreptitiously and illegally hacked into the DNC's computers and thereafter disseminated the

results of its theft. But, as explained below, under the Foreign Sovereign Immunities Act, 28 U.S.C. § 1602 et seq. ("FSIA"), the Russian Federation cannot be sued in the courts of the United States for governmental actions, subject to certain limited exceptions not present in this case, just as the United States government generally cannot be sued in courts abroad for its actions. The remedies for hostile actions by foreign governments are state actions, including sanctions imposed by the executive and legislative branches of government.

The DNC seeks to hold the second-level participants in this alleged activity -- the Campaign, the Campaign defendants, WikiLeaks, Assange, the Agalarovs, Mifsud, and Stone -- liable for dissemination of the stolen materials. But, as also explained below, the First Amendment prevents such liability in the same way it would preclude liability for press outlets that publish materials of public interest despite defects in the way the materials were obtained so long as the disseminator did not participate in any wrongdoing in obtaining the materials in the first place. The plausible allegations against the remaining defendants are insufficient to hold them liable for the illegality that occurred in obtaining the materials from the DNC. Therefore, for the reasons explained below, the defendants' motion to dismiss the Second Amended Complaint is **granted.**

Additionally, the Campaign has moved for sanctions against the DNC and its attorneys pursuant to Federal Rule of Civil Procedure 11. For the reasons explained below, the Campaign's motion is **denied.**

I.

In deciding a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6), the allegations in the complaint are accepted as true, and all reasonable inferences must be drawn in the plaintiff's favor. McCarthy v. Dun & Bradstreet Corp., 482 F.3d 184, 191 (2d Cir. 2007). The Court's function on a motion to dismiss is "not to weigh the evidence that might be presented at a trial but merely to determine whether the complaint itself is legally sufficient." Goldman v. Belden, 754 F.2d 1059, 1067 (2d Cir. 1985). The Court should not dismiss the complaint if the plaintiff has stated "enough facts to state a claim to relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). While courts should construe the factual allegations in the light most favorable to the plaintiff, "the tenet that a court must accept as true all of

the allegations contained in the complaint is inapplicable to legal conclusions." Id.

In deciding a motion to dismiss, a court may consider documents of which judicial notice may be taken. Chambers v. Time Warner, Inc., 282 F.3d 147, 153 (2d Cir. 2002). A court may also consider documents incorporated by reference in the complaint as well as documents the plaintiff either had in the plaintiff's possession or had knowledge of and upon which the plaintiff relied in bringing suit. See Cortec Indus., Inc. v. Sum Holding L.P., 949 F.2d 42, 48 (2d Cir. 1991).

II.

The following facts are taken from the Second Amended Complaint and are accepted as true for purposes of this motion to dismiss.

In the run up to the 2016 United States presidential election, Russian intelligence services hacked into the DNC's computers, penetrated its phone systems, and stole tens of thousands of documents. (SAC ¶ 1.) The DNC claims that the Trump Campaign welcomed the Russian Federation's help and was prepared to use the stolen information with the intent of hurting Hillary Clinton's presidential campaign and helping Donald Trump win the presidency. (Id. ¶¶ 1-2.)

A.

Over a year before the 2016 United States presidential election, on June 16, 2015, Donald Trump announced his candidacy for President of the United States. (Id. ¶ 84.) Soon after, in July of 2015, a Russian intelligence agent -- codenamed "Cozy Bear"[2] -- used stolen credentials to access the DNC's computer systems in Washington, D.C. and Virginia (the "2015 hack"). (Id. ¶¶ 81, 115.) Once in the system, Cozy Bear focused on collecting information from the DNC systems that were used primarily for communications, such as the systems providing email, email support, backup servers, voiceover internet protocol, and chat. (Id. ¶ 116.) Cozy Bear maintained access in the DNC system for almost a year. (Id. ¶ 81.)

On April 18, 2016, members of Russia's military intelligence agency, the General Staff of the Armed Forces of the Russian Federation ("GRU"), engaged another cyberattack on the DNC's Washington, D.C. and Virginia computer servers (the "April 2016 hack"). (Id. ¶ 101.) The agents that participated in the hack were part of two GRU units, Units 26165 and 74455, based in Moscow. (Id. ¶ 48.) At least ten GRU agents from Units 26165 and 74455 prepared for or participated in the hack. (Id. ¶ 49.) The DNC alleges that these agents were acting

---

[2] Cozy Bear is also referred to in the Second Amended Complaint as "Advanced Persistent Threat 29" or "APT 29." (SAC ¶ 114.)

pursuant to military orders. (Id. ¶¶ 49, 101.) To prepare for the hack, the GRU agents developed a malware -- "software that damages, disables, or spies upon computer systems" -- called "X-Agent." (Id. ¶ 49.) X-Agent allowed the GRU agents to monitor target computers in real time -- meaning they could see the screens and keystrokes of target computers as they were being used. (Id. ¶ 103.) On April 18, 2016, GRU agents accessed the DNC system and installed X-Agent onto the computer network. (Id. ¶¶ 101, 103.) Once X-Agent was installed on the DNC's computers, it was always on; the software captured the contents of communications going to and from the affected computers as they were being sent. (Id. ¶ 129.)[3]

---

[3] The DNC alleges that Viktor Borisovich Netyksho was the Russian military officer in command of GRU Unit 26165 in 2016. (SAC ¶ 49(a).) Boris Alekseyevich Antonov was a major in the Russian military in 2016 and the head of a department within Unit 26165 that was dedicated to computer intrusion activity. (Id. ¶ 49(b).) Antonov supervised other GRU officers who hacked the DNC's computer systems. (Id.) Dmitriy Sergeyevich Badin was the assistant head of Antonov's department within Unit 26165 in 2016 and worked with Antonov to supervise other GRU officers. (Id. ¶ 49(c).) Ivan Sergeyevich Yermakov was a Russian military officer who participated in an operation to hack a DNC email server and steal DNC emails. (Id. ¶ 49(d).) Sergey Aleksandrovich Morgachev was a lieutenant colonel in the Russian military assigned to Unit 26165 in 2016 who oversaw a department within Unit 26165 that developed and managed malware. (Id. ¶ 49(e).) Morgachev supervised the GRU officers who placed and monitored X-Agent on the DNC's computer network. (Id.) Nikolay Yuryevich Kozachek was a lieutenant captain in the Russian military and developed, customized, and monitored X-Agent. (Id. ¶ 49(f).) Pavel Vyacheslavovich Yershov was a Russian military officer who helped Kozachek and other GRU officers test and customize X-Agent before it was placed on the DNC's network. (Id. ¶ 49(g).) Artem Andreyevich Malyshev was a second lieutenant in the Russian military who monitored X-Agent on the DNC's computer network. (Id. ¶ 49(h).) Aleksandr Vladimirovich Osadchuk was a colonel in the Russian military and the commanding officer of GRU Unit 74455 in 2016. (Id. ¶ 49(i).) Aleksey Aleksandrovich Potemkin was an officer in the Russian military assigned to Unit 74455 in 2016. (Id. ¶ 49(j).) Potemkin supervised a department within Unit 74455 that created

Four days after the hack, on April 22, 2016, GRU agents prepared several gigabytes of DNC data for exfiltration. (Id. ¶ 104.) The GRU used another malware that it had developed, called "X-Tunnel," to transfer the data through encrypted channels to a GRU-leased computer in Illinois. (Id. ¶¶ 104, 121.) The Russian GRU agents remained in the DNC system for over a month, stealing documents and data until at least June 2016. (Id. ¶¶ 81, 105.)[4] Between May 25 and June 1, 2016, the GRU gained access to the DNC's email server and stole thousands of emails from the accounts of DNC employees. (Id. ¶ 123.)

During the April 2016 hack, GRU agents gained access to at least thirty-three of the DNC's computers. (Id. ¶ 105.) The GRU agents also accessed the DNC's "Voice-over Internet Protocol" transfers, which allowed the hackers to monitor voice-based communications, such as phone calls and voicemail, in real time. (Id. ¶ 128.) By June 2016, the Russian operatives had stolen thousands of documents from the DNC, including documents

---

computer infrastructure and social media accounts that were used in the dissemination of stolen DNC materials through Guccifer 2.0. (Id.)

These allegations in the Second Amended Complaint mirror allegations in the indictment brought by Special Counsel Robert Mueller, III, against these Russian defendants. See United States v. Netyksho, No. 18cr215 (D.D.C. July 13, 2018) (Dkt. No. 1.).

[4] The DNC detected another Russian agent -- referred to as "Fancy Bear" -- in its computer system on April 28, 2016. (SAC ¶ 118.) Like Cozy Bear, Fancy Bear used stolen credentials to gain access to the system. (Id. ¶ 127.) Fancy Bear is also referred to as "Advanced Persistent Threat 28" or "APT 28." (Id. ¶ 114.) The DNC alleges that Fancy Bear was acting as an agent of the GRU. (Id. ¶ 118.)

containing donor information, financial and economic information, proprietary opposition research compiled from multiple sources, information regarding planned political activities, and emails. (Id. ¶ 105.)

The DNC discovered that it had been hacked on April 28, 2016. (Id. ¶ 109.) Thereafter, the DNC hired a cybersecurity technology firm called CrowdStrike to investigate the attack, assess the damage done to the DNC's computers and servers, assist the DNC in its remediation efforts, set up a system for monitoring the current cyberattack, and alert the DNC to future attacks. (Id. ¶¶ 110, 112.)

On June 10, 2016, GRU agents launched a third -- but unsuccessful -- attack on the DNC's computers. This time, the GRU unsuccessfully attempted to hack the DNC's backup server -- nicknamed, "Raider" -- located in Virginia. (Id. ¶¶ 143-44.) The GRU placed X-Agent onto the backup server but the DNC discovered the intrusion before the agents were able to steal any information. (Id. ¶ 144.)

A fourth attack came in September 2016 (the "September 2016 hack"). On September 20, 2016, CrowdStrike discovered that GRU agents had gained access to the DNC's cloud-computing service. (Id. ¶ 180.) The Russian operatives exfiltrated a large amount of the DNC's data from the DNC's cloud to their own cloud-based account on the same service. (Id.) During this hack, the GRU

accessed and stole confidential information from servers housing voter contact information, DNC email lists, proprietary data such as the number of times internet users click on DNC advertisements, the number of times internet users click on links embedded in DNC emails, and volunteer information. (Id. ¶ 182.) The GRU also stole computer code created by DNC computer engineers, including Vertica and Tableau queries. (Id. ¶¶ 180, 182-86, 189.) The Second Amended Complaint does not allege that any materials from the September 2016 hack were disseminated to the public and counsel for the DNC acknowledged at the argument of the current motions that there is no such allegation.

B.

The DNC does not allege that any of the non-Russian Federation defendants actually participated in any of the hacks on the DNC's computer systems. Rather, the DNC argues that the Campaign, the Campaign defendants, Stone, the Agalarovs, Mifsud, Assange, and WikiLeaks actively supported and approved the Russian operation. (Id. ¶ 82.) The DNC points to various meetings between the defendants and individuals alleged to be connected to the Russian Federation and argues that the meetings are circumstantial evidence that the defendants conspired with the Russian Federation to steal the DNC's materials and publish them.

Before the April 2016 hack, in March 2016, Papadopoulos was notified that he would become a foreign policy adviser to the Campaign. (Id. ¶ 92.) Soon thereafter, Papadopoulos began meeting with Joseph Mifsud, a London-based Maltese academic who the DNC alleges acted as an unofficial agent of the Russian government. (Id. ¶ 93.) On March 14, Papadopoulos met with Mifsud in Italy. (Id. ¶ 94.) On March 24, Papadopoulos met with Mifsud and "a Russian national who was introduced as a relative of Putin." (Id.) The DNC does not offer any allegation about what was discussed at these meetings. On April 18, 2016, the day that the GRU agents hacked into the DNC's computers, Mifsud introduced Papadopoulos to an individual who Mifsud said had connections to the Russian Ministry of Foreign Affairs. (Id.) On April 26, 2016, four days after the GRU exfiltrated documents from the DNC system, Papadopoulos met Mifsud in London. (Id. ¶ 13.) Mifsud informed Papadopoulos that the Russians "have dirt" on Hillary Clinton in the form of "thousands of emails." (Id.) Papadopoulos reported back to superiors at the Campaign, stating that there were "interesting messages coming in from Moscow." (Id.)

On May 26, 2016, Donald Trump clinched the Republican presidential nomination. (Id. ¶ 132.) A week later, on June 3, 2016, Aras and Emin Agalarov contacted Donald Trump's son and political advisor, Trump Jr., through the Agalarovs' publicist,

Rob Goldstone. (Id. ¶¶ 133 & n.96, 137.) Aras Agalarov is an Azeri-born oligarch who is a Russian real estate mogul and "close ally" of Russian president Vladimir Putin. (Id. ¶ 50.) Emin Agalarov is a pop singer and executive at the Agalarov's real estate company. (Id. ¶ 51.) In an email to Trump Jr. on June 3, Goldstone stated that Emin Agalarov offered to provide damaging information about Hillary Clinton as "part of Russia and its government's support for Mr. Trump." (Id. ¶¶ 14, 133.) Seventeen minutes later, Trump Jr. responded to Goldstone's email, stating, "if it's what you say I love it especially later in the summer." (Id. ¶¶ 14, 134 (emphasis omitted).) On June 6 and 7, 2016, Trump Jr. and Emin Agalarov spoke on the phone several times and began planning an in-person meeting. (Id. ¶ 135.) In a June 7, 2016 email to Goldstone, Trump Jr. confirmed plans for a meeting, stating, "It will likely be Paul Manafort (campaign boss) my brother in law [Kushner] and me." (Id. ¶ 136 & n.100.)

On June 9, 2016, the meeting that Emin Agalarov and Trump Jr. had been planning took place in Trump Tower in New York City. (Id. ¶ 14.) Trump Jr., Manafort, and Kushner met with Goldstone, Russian lawyer Natalia Veselnitskaya, Agalarov business associate Irakyl Kaveladze, lobbyist Rinat Akhmestshin, and a translator. (Id. ¶¶ 15, 137.) Manafort was the Trump Campaign's convention manager from March to May 2016 and the

Campaign's chairman from May 2016 to August 2016. (Id. ¶ 57.) Kushner is Donald Trump's son-in-law and was a senior advisor to the Trump Campaign. (Id. ¶ 59.) Veselnitskaya is alleged to have been "closely connected to the Kremlin" and to have had "a history of acting as an agent of the Russian government." (Id. ¶ 138.) The DNC does not allege what specifically was discussed at the Trump Tower meeting but reiterates that the Russians had offered "damaging information about the Democratic presidential nominee" to the Campaign. (Id. ¶ 141.)

The day after the Trump Tower meeting, on June 10, 2016, GRU agents unsuccessfully attempted to hack the DNC's backup server, Raider. (Id. ¶ 143.)

On June 12, 2016, Julian Assange -- the founder and publisher of WikiLeaks -- appeared on a British television show and stated that WikiLeaks had obtained "leak materials concerning the Democratic presidential candidate" and would be releasing them soon. (Id. ¶ 145.) WikiLeaks is an international news organization of "unknown structure" that operates a website, WikiLeaks.org, on which it publishes leaked or stolen confidential and classified information. (Id. ¶ 54.)

On June 14, 2016, the DNC announced publicly for the first time that it had been hacked by Russian intelligence agents. (Id. ¶ 146.) The next day, June 15, Russian intelligence agents began releasing stolen DNC documents to the public. (Id. ¶ 16.)

The DNC alleges that these documents were released systematically from June through October 2016 at times that were favorable to the Trump Campaign. (Id. ¶ 160.) Documents were first disseminated through "Guccifer 2.0,"[5] a fictitious online persona created by Russian intelligence agents. (Id. ¶ 16.)[6] On June 22, 2016, WikiLeaks contacted Guccifer 2.0 and asked Guccifer 2.0 to send some of the stolen DNC documents to WikiLeaks. (Id. ¶ 17.) In that communication, WikiLeaks noted that Donald Trump's chances of winning the presidency might improve if WikiLeaks were allowed to disseminate some of the stolen documents. (Id.) On July 14, 2016, Guccifer 2.0 sent WikiLeaks an email with instructions on how to access stolen DNC documents in an online depository. (Id. ¶ 154.) Between July 14 and 18, 2016, GRU agents transmitted to WikiLeaks documents that were stolen in the April 2016 hack. (Id. ¶¶ 19, 126.) WikiLeaks promised to release the documents ahead of the Democratic National Convention with the intention of creating conflict among the potential Democratic nominees for president. (Id. ¶¶ 17, 19.)

---

[5] Guccifer 2.0 published the documents on www.guccifer2.wordpress.com. (SAC ¶ 125.)

[6] The DNC states that Guccifer 2.0 publicly took responsibility for the hacks on the DNC but claimed to be a Romanian hacker with no relationship with the Russian Federation. (SAC ¶ 48.) The DNC claims, however, that upon information and belief, Guccifer 2.0 is a Russian-created persona that only claimed to be Romanian to hide the Russian Federation's role in cyberattacks on the DNC. (Id.)

As promised, on July 22, 2016, three days before the start of the Democratic Convention, WikiLeaks began publishing stolen DNC documents to the public. (Id. ¶ 20.) WikiLeaks released over 20,000 emails and other documents that had been stolen from the DNC. (Id. ¶ 156.)

On July 25, 2016, Roger Stone, a "long-time confidant" of Donald Trump's who served as an "informal advisor" during the presidential campaign, directed his associate, Jerome Corsi[7] -- who is described only as an associate of Stone's -- to connect with Assange and WikiLeaks to gather information about what kind of documents WikiLeaks possessed. (Id. ¶¶ 58, 162.) Corsi reported back to Stone in August that WikiLeaks planned to publish more documents in October 2016. (Id. ¶ 162.) However, it appears that many or all of the documents about which Stone communicated with WikiLeaks (through Corsi) were documents that had not been stolen from the DNC's servers. (See id. ¶¶ 161, 164-65.) Stone is also alleged to have communicated with Guccifer 2.0 about information it had in its possession that could damage Hillary Clinton's presidential campaign. (Id. ¶ 161.) On August 17, 2016, a GRU operative sent Stone a private message on Twitter, stating, "please tell me if i can

[7] Corsi is not named as a defendant in this case but is alleged to have been a coconspirator. (SAC ¶ 62.)

help u anyhow. it would be a great pleasure to me." (Id. ¶ 167.)

The DNC alleges that throughout the summer and fall of 2016, Trump's associates continued to communicate secretly with Russian agents and WikiLeaks who disseminated strategically the stolen DNC information. (Id. ¶ 21.)[8] The DNC asserts that some of Stone's public statements show that he must have been communicating with Russian operatives, WikiLeaks, or both, because he had access to nonpublic information. For example, on August 21, 2016, Stone tweeted that "it will soon [be] the Podesta's time in the barrel" -- referring to John Podesta, chairman of the 2016 Hillary Clinton presidential campaign. (Id. ¶ 22.) Weeks later, WikiLeaks began releasing Podesta's emails. (Id.) Podesta's emails had been stolen in a different cyberattack -- there is no allegation that they were taken from the DNC's servers. (Id. ¶ 161.)

In mid-September 2016, Stone said that he expected "Julian Assange and the WikiLeaks people to drop a payload of new

[8] The DNC alleges that in early July 2016, Manafort, who was then the chairman of the campaign, emailed Kilimnik, "his longtime aide with ties to the GRU, offering private briefings on the presidential campaign to Russian oligarch and Putin ally Deripaska." (SAC ¶ 152.) At some time during the presidential campaign, Manafort also provided Kilimnik with "polling data." (Id. ¶ 91.) The DNC also alleges that Gates -- "a longtime employee and business partner of Manafort" and senior advisor to the campaign -- was in contact with Kilimnik during the campaign. (Id. ¶ 67.) However, the DNC does not allege that Manafort and Gates ever discussed the DNC's stolen information with Kilimnik.

documents on Hillary [Clinton] on a weekly basis fairly soon." (Id. ¶ 22.) Beginning on October 7, 2016, WikiLeaks began releasing "stolen emails" at least once a week, although the Second Amended Complaint does not say whether these emails were Clinton's emails or if they were stolen from the DNC. (See id. ¶ 22.)

In or around September 2016, Trump Jr. was also in communication with WikiLeaks. (Id. ¶ 24.) WikiLeaks provided Trump Jr. with a password to an anti-Trump website, and in exchange WikiLeaks asked that Donald Trump retweet a link to the website where WikiLeaks had posted the stolen DNC emails. (Id.) Fifteen minutes later, Donald Trump sent out a tweet noting the media's lack of attention to WikiLeaks. (Id.)

On November 6, 2016, days before the presidential election, WikiLeaks released additional hacked DNC emails. (Id. ¶ 203.) Donald Trump was elected President of the United States in the election held on Tuesday, November 8, 2016. (See id. ¶ 204.)

C.

The DNC asserts that after the presidential election the individual defendants and the Campaign attempted to cover up their coordination with the Russian Federation through criminal obstruction of justice and witness tampering.

In 2017, Stone denied having contact with any Russians during the 2016 campaign, testifying before the House

Intelligence Committee that he "never had any communications with any Russians or individuals fronting for Russians[] in connection with the 2016 presidential election," and telling the Washington Post that he "didn't talk to anybody who was identifiably Russian during the two-year run-up to this campaign." (Id. ¶ 214.)

Trump Jr. allegedly lied about his communications with Russia. In March 2017, he told CNN, "Did I meet with people that were Russian? I'm sure, I'm sure I did. But none that were set up. None that I can think of at the moment. And certainly none that I was representing the campaign in any way, shape or form." (Id. ¶ 216 & n.196.) Trump Jr. also allegedly lied about the June 2016 Trump Tower meeting, stating in July 2017 to the media that the meeting was primarily about the adoption of Russian children. (Id. ¶ 217.)

On November 26, 2018, Special Counsel Robert Mueller, III, submitted a status report to the United States District Court for the District of Columbia, explaining that Manafort had breached Manafort's plea agreement with the Government by "lying to the Federal Bureau of Investigation and the Special Counsel's Office on a variety of subject matters." (Id. ¶ 231.) Subsequent filings clarified that Manafort lied about his repeated interactions with Kilimnik and about sharing polling data with Kilimnik related to Trump's 2016 campaign. (Id.)

Corsi is alleged to have deleted all of his email correspondence that predated October 11, 2016, including an email chain in which Stone instructed Corsi to get in touch with Assange and WikiLeaks to discuss documents stolen from Democratic targets. (Id. ¶ 215.)

On July 24, 2017, Kushner is alleged to have misrepresented to Congress that he did not know what the Trump Tower meeting was going to be about. (Id. ¶ 219.)

The DNC alleges that, on September 7, 2017, Trump Jr. testified falsely to the Senate Judiciary Committee that no attendee of the Trump Tower meeting requested additional meetings or communications with members of the Campaign. (Id. ¶ 222.)

On October 5, 2017, Papadopoulos pleaded guilty to lying to the FBI about his contacts with Mifsud and other Russian agents during a January 27, 2017 interview. (Id. ¶ 223.)

D.

The DNC filed this action on April 20, 2018. The Court granted leave to file an amended complaint, and on October 3, 2018 the DNC filed its First Amended Complaint. After several of the defendants moved to dismiss that complaint, the DNC filed the Second Amended Complaint.[9]

[9] "On May 17, 2017, Deputy Attorney General Rod J. Rosenstein -- then serving as Acting Attorney General for the Russia investigation . . . -- appointed [Robert Mueller, III, as] Special Counsel to investigate Russian

III.

The DNC asserts each of its fourteen claims against the Russian Federation with the exception of Count 4, which alleges violation of the Wiretap Act. All of the remaining defendants are named in Counts 2 (RICO), 3 (RICO Conspiracy), 8 (Washington, D.C. Uniform Trade Secrets Act), 12 (Conspiracy to Commit Trespass to Chattels Under Virginia Common Law), and 14 (Virginia Computer Crimes Act). Count 4 (Wiretap Act) is

---

interference with the 2016 presidential election and related matters." Special Counsel Robert Mueller, III, Report on the Investigation into Russian Interference in the 2016 Presidential Election (the "Mueller Report"), Vol. I at 11 (Mar. 2019) (quotation marks omitted). The Special Counsel's investigation also included "any links and/or coordination between the Russian government and individuals associated with the campaign of President Donald Trump." Id. In March of 2019, the Special Counsel concluded his investigation and provided to the Attorney General a report detailing the Special Counsel's findings. Id. at 1. A redacted version of the Mueller Report was released publicly on April 18, 2019. The Report states that the Special Counsel found that although Russia "worked to secure" President Trump's election and the Campaign "expected it would benefit electorally" from the release of information Russia had stolen, the Special Counsel's "investigation did not establish that members of the Trump Campaign conspired or coordinated with the Russian government in its election interference activities." Id. at 1-2.

The Campaign argues that the Court can take judicial notice of the Mueller Report. The DNC argues that the Court cannot take such notice. The existence of the Mueller Report "is not subject to reasonable dispute because it[s existence] . . . can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). And there is not a hearsay issue because the Mueller Report could be admitted under the public records exception. See Fed. R. Evid. 803(8) ("A record or statement of a public office [is not excluded by the rule against hearsay] if . . . it sets out . . . in a civil case or against the government in a criminal case, factual findings from a legally authorized investigation[] and . . . the opponent does not show that the source of information or other circumstances indicate a lack of trustworthiness."). The DNC nevertheless objects to the Court's consideration of the Mueller Report because it was issued shortly before the DNC filed its response to the current motions and the DNC did not have an opportunity to incorporate the Report into its arguments. The Mueller Report is unnecessary to the decision of the current motions and, in view of the DNC's opposition, the Court will not rely upon it in deciding the current motions.

asserted only against defendants WikiLeaks, Assange, the Campaign, Trump Jr., Manafort, Stone, Kushner, Papadopoulos, and Gates. Count 7 (Defend Trade Secrets Act) is asserted only against the Russian Federation, WikiLeaks, and Assange.

Defendants Kushner, Gates, WikiLeaks, the Campaign, Aras and Emin Agalarov, Papadopoulos, Trump Jr.,[10] and Stone have moved to dismiss the Second Amended Complaint.[11] The Russian Federation has submitted a statement of immunity. Manafort and Assange were served with the Second Amended Complaint but have failed to respond by motion or answer.[12] Misfud has not yet been served. The Knight First Amendment Institute at Columbia University, the Reporters Committee for Freedom of the Press, and the American Civil Liberties Union submitted an amicus curiae brief in support of WikiLeaks's motion to dismiss.

---

10 Trump Jr. executed a waiver of service of the summons on June 4, 2018. (Dkt. No. 85.) Trump Jr. did not initially respond to the Second Amended Complaint. After the motions to dismiss were fully briefed, counsel for Trump Jr. submitted a letter to the Court requesting to join the Campaign's motion. (Dkt. No. 265.) Because Trump Jr. simply seeks to join the Campaign's motion and does not submit any additional arguments, there is no prejudice to the DNC. Therefore, the Court grants the application of Trump Jr. to join the motion to dismiss filed by the Campaign.

11 Gates and Trump Jr. joined the arguments of the other defendants but did not submit a memorandum of law in support of their motions. (Dkt. No. 223.) Kushner and WikiLeaks moved to dismiss the Second Amended Complaint and joined the Campaign's omnibus motion to dismiss. (Dkt. Nos. 222, 225.) Papadopoulos and Stone moved to dismiss the Second Amended Complaint and joined all of the other defendants' motions to dismiss. (Dkt. Nos. 234, 236.)

12 Manafort was served in mid-July 2018, (Dkt. No. 147), and Assange was served on August 1, 2018, (Dkt. No. 157). While those defendants have not responded to the Second Amended Complaint, the disposition of the current motions also applies to them.

IV.

The Russian Federation has not appeared in this case but has submitted a statement of immunity. (Dkt. No. 186.) In that statement, the Russian Federation argues that it is immune from the DNC's claims under the FSIA, that the DNC's claims are barred by the political question doctrine,[13] and that the Southern District of New York is an improper venue.

A.

A plaintiff may only sue a foreign sovereign in the United States if the suit is authorized under the FSIA. Republic of Argentina v. Weltover, 504 U.S. 607, 611 (1992) (The FSIA "provides the 'sole basis' for obtaining jurisdiction over a foreign sovereign in the United States." (quoting Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 434-39 (1989))). Under the FSIA, a "foreign state" -- such as the Russian Federation -- is "immune from the jurisdiction" of state and federal courts in the United States unless a statutory exception applies. 28 U.S.C. § 1604; see id. §§ 1605-07

---

[13] The Russian Federation and the Campaign argue that certain allegations in the Second Amended Complaint should be dismissed based on the political question doctrine. They argue that the DNC's allegations regarding policy decisions that Donald Trump has made as president -- for example, that President Trump "has continued to help the Russian Federation achieve its goals by adopting policies that inure to Russia's benefit," (SAC ¶ 243) -- cannot be second-guessed by the DNC or the Court. However, the DNC's allegations regarding President Trump's post-election decisions are not necessary to decide the issues before the Court. Therefore, the Court need not reach any issues raised by the political question doctrine.

(providing exceptions); see also Atlantica Holdings v. Sovereign Wealth Fund Samruk-Kazyna JSC, 813 F.3d 98, 106 (2d Cir. 2016) ("Federal courts have subject-matter jurisdiction over an action against a foreign state if, and only if, one of those exceptions applies."). The DNC asserts that two exceptions to the FSIA allow suit against the Russian Federation in this case: the "noncommercial tort" and "commercial activity" exceptions.

B.

The noncommercial tort exception to the FSIA applies in cases where (1) "money damages are sought against a foreign state" (2) "for personal injury or death, or damage to or loss of property, occurring in the United States" (3) that is "caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment." 28 U.S.C. § 1605(a)(5). This exception does not apply to "any claim based upon the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion be abused." Id. § 1605(a)(5)(A). Courts read this exception narrowly; indeed Congress's objective in enacting the noncommercial tort exception was to "eliminate a foreign state's immunity for traffic accidents and other torts committed in the United States, for which liability is imposed under domestic tort law." Amerada Hess Shipping Corp., 488 U.S. at 439-40.

The Russian Federation argues that the noncommercial tort exception does not apply in this case because, among other reasons, the entire tort did not take place in the United States. In Amerada Hess Shipping Corp., the Supreme Court held that the noncommercial tort exception is not applicable where a foreign sovereign commits a tort abroad, even if that tort results in "'direct effects' in the United States." Id. at 441. The Second Circuit Court of Appeals and other circuit courts have interpreted the statute to mean that the "entire tort" must have been committed in the United States. See In re Terrorist Attacks on Sept. 11, 2001, 714 F.3d 109, 115 (2d Cir. 2013) ("For this exception to apply, however, the 'entire tort' must be committed in the United States."); see also Doe v. Fed. Democratic Republic of Ethiopia, 851 F.3d 7, 10 (D.C. Cir. 2017) ("The phrase 'occurring in the United States' is no mere surplusage.' '[T]he entire tort' -- including not only the injury but also the act precipitating that injury -- must occur in the United States." (quoting Jerez v. Republic of Cuba, 775 F.3d 419, 424 (D.C. Cir. 2014))); O'Bryan v. Holy See, 556 F.3d 361, 382 (6th Cir. 2009) ("We join the Second and D.C. Circuits in concluding that in order to apply the tortious act exception, the 'entire tort' must occur in the United States.").

This case is a far cry from jurisdiction over a traffic accident involving a foreign diplomat, which is the paradigm for

the noncommercial tort exception. In this case, the DNC alleges that the Russian GRU agents who hacked the DNC computer system did so from Moscow. The DNC alleges that "GRU Unit 26165, located at 20 Komsomolskiy Prospekt, in Moscow, Russia, was primarily responsible for the cyberattacks on the DNC in 2016." (SAC ¶ 48.) The DNC alleges that a major and a lieutenant colonel in the Russian military supervised GRU officers in Unit 26165 as they "developed, customized, and monitored the X-Agent malware used on the DNC's computer network," placed the X-Agent malware on the DNC computer network, and "monitored the X-Agent malware" after the hack. (Id. ¶ 49(b), (e)-(h).) After the documents were taken from the DNC's servers, "GRU Unit 74455, located at 22 Khirova Street, Khimki, Moscow, helped disseminate . . . stolen DNC information through fictitious online personas." (Id. ¶ 48.) Because the theft was planned and executed from computers in Russia, it is plain that the "entire tort" did not take place in the United States. The DNC has cited no similar case where the noncommercial tort exception was applied when a portion of the conduct of the foreign government occurred outside the United States.

The D.C. Circuit Court of Appeals considered similar facts in Doe v. Ethiopia, 851 F.3d 7. In that case, the plaintiff was a United States citizen who was born in Ethiopia. Id. at 8. The plaintiff sued the Federal Democratic Republic of Ethiopia,

alleging that Ethiopia violated the Wiretap Act and committed the tort of intrusion upon seclusion in violation of Maryland law. Id. at 9. According to the plaintiff, the Ethiopian government developed a computer virus abroad and emailed it to the plaintiff, who was in Maryland when he opened the email. Id. at 10. When the plaintiff opened the email, the virus downloaded onto his computer and enabled the Ethiopian government to spy on him from abroad. Id. at 8. The district court dismissed the plaintiff's claims, and the plaintiff appealed. Id. at 9. The Court of Appeals noted that "at least a portion of Ethiopia's alleged tort occurred abroad." Id. at 10. The court found that the tortious intent of targeting the plaintiff and the tortious acts of computer programming and sending the infected email took place outside the United States. Id. at 10. Therefore, the Court held that the noncommercial tort exception did not apply.

Similarly, in Broidy Capital Management, LLC v. Qatar, the plaintiff alleged that Qatari agents hacked into the plaintiff's data servers from outside the United States. No. 18cv2421, 2018 WL 6074570, at *5 (C.D. Cal. Aug. 8, 2018). The district court held that the plaintiff had not alleged that the "entire tort" took place in the United States because the computers used to access the plaintiff's servers were located in Qatar. Id. at

*5, *7. The court therefore found that the noncommercial tort exception to the FSIA did not apply. Id. at *5-7.

As in Doe and Broidy, the DNC alleges that the hack was executed from computers located outside of the United States. The GRU agents are alleged to have planned and executed the hack on the DNC's computer systems from Russia. Therefore, the "entire tort" did not take place in the United States and the noncommercial tort exception to the FSIA does not apply.

C.

The DNC also argues that the commercial activity exception to the FSIA applies in this case. This exception to the FSIA provides that a foreign state shall not be immune from the jurisdiction of United States courts in any case "in which the action is based upon a commercial activity carried on in the United States by the foreign state." 28 U.S.C. § 1605(a)(2). The Act provides that a commercial activity may be "either a regular course of commercial conduct or a particular commercial transaction or act," the "commercial character of [which] shall be determined by reference to" its "nature," rather than its "purpose." Id. § 1603(d).

A state engages in "commercial activity . . . only where it acts in the manner of a private player within the market" -- that is, "where it exercises only those powers that can also be exercised by private citizens, as distinct from those powers

peculiar to sovereigns." Petersen Energia Inversora S.A.U. v. Argentine Republic & YPF S.A., 895 F.3d 194, 205 (2d Cir. 2018) (quotation marks omitted) (quoting Saudi Arabia v. Nelson, 507 U.S. 349, 360 (1993)). Therefore, the relevant question "is whether the particular actions that the foreign state performs . . . are the type of actions by which a private party engages in trade and traffic or commerce." Weltover, 504 U.S. at 614 ("[T]he issue is whether the particular actions that the foreign state performs (whatever the motive behind them) are the type of actions by which a private party engages in trade and traffic or commerce." (quotation marks omitted)).

Transnational cyberattacks are not the "type of actions by which a private party engages in trade and traffic or commerce." Id. at 614 (emphasis omitted); Broidy Capital, 2018 WL 6074570, at *9 (holding that the commercial activity exception did not apply because "[c]yber-attacks are not the typical acts of market participants"). Put differently, a country's planned military cyber-strike against a foreign nation's political party cannot be considered genuinely "a private party engage[d] in trade and traffic or commerce." See Weltover, 504 U.S. at 614 (quotation marks omitted).

Moreover, the alleged actions by the Russian Federation -- hacking and theft -- are illegal. "The Second Circuit has made very clear that, for purposes of the FSIA, a commercial activity

must be one in which a private person can engage lawfully." In re Terrorist Attacks on Sept. 11, 2001, 349 F. Supp. 2d 765, 793 (S.D.N.Y. 2005)[14] (emphasis added) (quoting Letelier v. Republic of Chile, 748 F.2d 790, 797-98 (2d Cir. 1984)); see also Nelson, 507 U.S. at 360-62 (holding that detaining and torturing a person is not commercial activity since it "is not the sort of action by which private parties can engage in commerce").

Accordingly, the commercial activity exception to the FSIA does not apply and the Court lacks subject matter jurisdiction over the DNC's claims against the Russian Federation.

* * *

Therefore, the DNC's claims against the Russian Federation are barred by the FSIA and no exception applies. Relief from the alleged activities of the Russian Federation should be sought from the political branches of the Government and not from the courts. Because this Court does not have jurisdiction over the claims against the Russian Federation under the FSIA, it is unnecessary to address the Russian Federation's remaining arguments. The DNC's claims against the Russian Federation are **dismissed.**

[14] On reconsideration in part, 392 F. Supp. 2d 539 (S.D.N.Y. 2005), aff'd, 538 F.3d 71 (2d Cir. 2008), aff'd, 714 F.3d 118 (2d Cir. 2013).

V.

The Campaign, WikiLeaks,[15] Kushner, and Papadopoulos move to dismiss the claims against them based on the First Amendment. These arguments are joined by Gates, Trump Jr., and Stone. The Knight First Amendment Institute at Columbia University, the Reporters Committee for Freedom of the Press, and the American Civil Liberties Union have submitted an amicus brief in support of WikiLeaks's motion to dismiss on First Amendment grounds.

The DNC argues that the defendants conspired with the Russian Federation to steal the DNC's emails, trade secrets, and other documents from the DNC's computer system and disseminate those materials to the public.[16] The DNC does not claim that the stolen materials are false or defamatory. Rather, the DNC seeks to hold the defendants liable for the theft and disclosure of

---

[15] Assange is alleged to have operated WikiLeaks during the presidential election. (See SAC ¶¶ 24, 53.) Therefore, the Court's decisions regarding WikiLeaks apply also to Assange.

[16] Stone argues that the DNC does not have standing to assert the claims against him because it alleges no cognizable injury that can be fairly traced to Stone's alleged actions. Stone states that the allegations against him in the Second Amended Complaint concern an alleged conspiracy relating to Podesta's emails, not the DNC's. He argues, therefore, that he was not part of the RICO enterprise or conspiracy to injure the DNC, steal its "trade secrets," or trespass on the DNC's computers. The DNC responds that the allegations raised against Stone show that he was a coconspirator in the overall scheme to steal and disseminate the DNC's information. The DNC plainly does not have standing to assert claims on behalf of Podesta. See Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992). However, as discussed below, the DNC has failed to allege plausibly claims against Stone. To the extent that the DNC's allegations attempt to impute liability to Stone for his alleged actions injuring parties other than the DNC, the Court does not consider those allegations and they would not support the DNC's claims in any event.

the stolen materials under federal, Virginia, and District of Columbia law.[17] The defendants argue that the DNC's claims against them are barred by the First Amendment because the DNC seeks to hold them liable for publication of documents that they did not help to steal.

The defendants do not argue that the laws at issue are unconstitutional on their face. Accordingly, this is an as-applied challenge to those laws.

A.

In New York Times Co. v. United States, the landmark "Pentagon Papers" case, the Supreme Court upheld the press's right to publish information of public concern obtained from documents stolen by a third party. 403 U.S. 713, 714 (1971) (per curiam).[18] The Court held that there is a "heavy presumption" against the constitutional validity of prior restraints on the publication of such information. Id. The Court elaborated further on this doctrine in Smith v. Daily Mail

---

[17] Specifically, claims are alleged against defendants other than the Russian Federation under RICO, 18 U.S.C. § 1962; the Wiretap Act, 18 U.S.C. §§ 2510-22; the Defend Trade Secrets Act, 18 U.S.C. § 1831 et seq.; the Washington, D.C. Uniform Trade Secrets Act, D.C. Code Ann. §§ 36-401 to 46-410; the Virginia Computer Crimes Act, Va. Code Ann. § 18.2-152.5 et seq.; and for conspiracy to commit trespass to chattels under Virginia law.

[18] In his dissenting opinion, Justice Harlan noted "the seemingly uncontested facts that the documents, or the originals of which they are duplicates, were purloined from the Government's possession and that the newspapers received them with knowledge that they had been feloniously acquired." 403 U.S. at 754.

Publishing Co., 443 U.S. 97 (1979). There, the Court held that two newspapers could not be criminally prosecuted for publishing the name of a minor in violation of a West Virginia statute. Id. at 99. The Court stated in Smith that "state officials may not constitutionally punish publication" of "lawfully obtain[ed] truthful information" "absent a need to further a state interest of the highest order." Id. at 103. In Florida Star v. B.J.F., the Court held that the First Amendment barred civil liability asserted against a newspaper that published an article that revealed the name of a rape victim, even though publication violated a state statute against such disclosure. 491 U.S. 524, 536 (1989). In Florida Star, the Supreme Court held that "the article generally, as opposed to the specific identity contained within it, involved a matter of paramount public import" and furthered a stated interest of the highest order; therefore, the newspaper could not be held liable for the publication of the victim's name. Id. at 536-37.

More recently, in Bartnicki v. Vopper, the Court addressed the issue of civil liability for publishing stolen information. 532 U.S. 514, 525 (2001). In that case, an unknown person intercepted and recorded a call between a teachers' union's president and its chief negotiator. Id. at 518. On the call, the president of the union stated, "If they're not gonna move for three percent, we're gonna have to go to their, their homes

. . . . To blow off their front porches . . . ." Id. at 518-19. At the time, the local school board and the teachers' union were in "contentious" negotiations that had received "a lot of media attention." Id. at 518. After the parties reached a settlement, a local radio station host, who had been critical of the union, played the tape on his radio show. Id. at 519. The two people who were involved in the recorded conversation brought suit against the radio show host for violating federal and Pennsylvania wiretapping statutes. Id.

In addressing the case, the Supreme Court noted that the defendant radio show host had violated federal and state statutes by disclosing the illegal recording. Id. at 525. The Supreme Court accepted as true that the defendant played no part in the illegal interception, but that he knew or had reason to know that the recording had been obtained illegally. Id. Despite finding that the defendant violated the statutes and that he knew that the recording had been illegally obtained, the Court held that the defendant could not be held liable for disseminating the recorded information because the publication was protected by the First Amendment. The Court reiterated its admonition from the Daily Mail case that "state action to punish the publication of truthful information seldom can satisfy constitutional standards." Id. at 527 (quoting Daily Mail, 443 U.S. at 102). The Court ruled that there was no liability for

disclosing stolen information where (1) the disclosing party "did not participate" in the theft, even though that party knows or has reason to know of the theft, and (2) the disclosure "concern[s] public issues." Id. at 517-18.

B.

As Bartnicki makes clear, there is a significant legal distinction between stealing documents and disclosing documents that someone else had stolen previously. The parties do not dispute that the stolen DNC documents concern public issues. However, the parties disagree over whether the DNC has alleged plausibly that the defendants, other than the Russian Federation, participated in the theft of the documents.

The DNC has plainly alleged that the Russian Federation hacked the DNC's computers and stole its information. The Second Amended Complaint alleges that Russian GRU agents hacked into the DNC's computer system on April 18, 2016.[19] Then, from April 22 to early June, GRU agents stole emails, alleged trade secrets, and other information from the DNC's computer system. On June 10, 2016, GRU agents unsuccessfully tried to hack the DNC's backup server. And in September 2016, GRU agents hacked

[19] The Russian Federation also hacked into the DNC's computer system in 2015. However, the DNC states that the "[d]efendants are not liable for the information theft that occurred in 2015[] before there was any [alleged] conspiracy." (DNC Opp'n at 101 n.29.) Rather, the DNC argues that the defendants are liable only for the information that was stolen "after the [alleged] conspiracy was formed in March 2016." (DNC Opp'n at 101 n.29.)

into the DNC's cloud-computing service and copied information onto their own cloud-based server. The DNC has also alleged that the Russian Federation disclosed the stolen materials, although it has not alleged that the Russian Federation disclosed the materials stolen in the September 2016 hack. The Second Amended Complaint alleges that GRU agents posted stolen emails and other documents on the internet via Guccifer 2.0.[20]

However, the DNC has not alleged that any defendant other than the Russian Federation participated in the hack of the DNC's computers or theft of the DNC's documents. The DNC argues that the various meetings and conversations between the defendants in this case and with persons connected to the Russian government during the time that Russian GRU agents were stealing the DNC's information show that the defendants conspired with the Russian Federation to steal and disseminate the DNC's materials. (DNC Opp'n at 34, 37.) That argument is entirely divorced from the facts actually alleged in the Second Amended Complaint. While the Court is required to accept the factual allegations in the Second Amended Complaint, it is not

---

[20] The DNC alleges that those documents were posted on www.guccifer2.wordpress.com. WikiLeaks asserts that documents were also published on a website called "DCLeaks." (WikiLeaks's Mem. at 13, Dkt. No. 208.) WikiLeaks says that documents were posted on Guccifer 2.0's and DCLeaks's websites before WikiLeaks is alleged to have published any documents. There is no allegation in the Second Amended Complaint that any documents were posted to DCLeaks.

required to accept conclusory allegations asserted as facts. Iqbal, 556 U.S. at 678.

For example, the DNC argues in its opposition to the current motions that the conspiracy between the Russian Federation and the other defendants to hack the DNC's computers and steal its electronic information began in March 2016. (DNC Opp'n at 101 n.29.) However, the only events alleged to have taken place in March 2016 are that Manafort was hired as the Campaign's convention manager, Papadopoulos was hired as a foreign policy advisor, and Papadopoulos met with Mifsud on March 14 and 24. The entirety of the DNC's allegations regarding the March meetings between Mifsud and Papadopoulos are that "[o]n March 14, 2016, Mifsud met with Papadopoulos in Italy," and "[o]n March 24, 2016, Mifsud met again with Papadopoulos, this time bringing along a Russian national who was introduced as a relative of Putin." (SAC ¶ 94.) Papadopoulos reported back to the Campaign that "his conversation was to arrange a meeting between us and the Russian leadership to discuss U.S.-Russia ties under President Trump." (Id. ¶ 96 (quotation marks omitted).) These vague references to meetings between Papadopoulos, a foreign policy advisor to the Campaign, and Mifsud, a London-based academic not officially affiliated with the Russian Federation, do not raise a plausible inference that the defendants agreed to participate with the

Russian Federation in hacking the DNC's computers and stealing its documents. See Twombly, 550 U.S. at 556-57; In re Interest Rate Swaps Antitrust Litig., 261 F. Supp. 3d 430, 471 (S.D.N.Y. 2017) (holding that the "mere opportunity to conspire at legitimate meetings does not support an inference" of an agreement to enter into an illegal conspiracy (quotation marks omitted)). To the contrary, Mifsud is alleged to have told Papadopoulos about emails harmful to the Hillary Clinton campaign only after the Russian Federation had hacked the DNC and had those emails in its possession. (See SAC ¶ 94(d) (stating that at the April 26 meeting -- eight days after the April 2016 hack began -- "Mifsud told Papadopoulos that the Russians had 'thousands of emails' that could harm Hillary Clinton's presidential campaign").)[21]

The DNC also repeatedly argues in its brief that WikiLeaks participated in the theft of the DNC documents. (See, e.g., DNC Opp'n at 3 ("The Complaint presents clear evidence that all Defendants -- including WikiLeaks -- participated in a criminal conspiracy to steal the DNC's information and use it to support Russia's preferred presidential candidate.").) But in the Second Amended Complaint the DNC alleges that WikiLeaks first requested stolen DNC materials from Guccifer 2.0 only after the

[21] The Second Amended Complaint does not make clear whether the emails that Mifsud was referring to were stolen from the DNC. (SAC ¶ 94(d).)

Russian Federation had already stolen them and after Russian agents began disseminating them through Guccifer 2.0. (SAC ¶¶ 16-17.) The Second Amended Complaint does not allege that WikiLeaks agreed to participate in the theft or that it had any advance knowledge that the Russian Federation was planning to hack the DNC.

The DNC argues in opposition to the current motions that Trump Jr.'s communications with the Agalarovs and the meeting at Trump Tower are evidence that Trump Jr., Manafort, Kushner, and the Agalarovs participated in the theft of the DNC's documents. But those communications and that meeting took place after the Russian Federation had already hacked the DNC's computer systems and, in any event, there is no allegation that the parties to those discussions talked about stealing the DNC's information, or indeed about information that had been obtained from hacking the DNC's computers or any information to be obtained from future hacking. (See id. ¶ 15.)

Similarly, Stone is alleged to have contacted WikiLeaks through Corsi for the first time on July 25, 2016 and spoke to GRU officers in August 2016 -- months after the April 2016 hack. Stone is not alleged to have discussed stealing the DNC's documents in any of these communications, or to have been aware of the hacks until after they took place.

The allegations against Gates are even more threadbare: he is only alleged to have spoken with Kilimnik -- Manafort's aide -- during the campaign and to have helped prepare for the Trump Tower meeting. It is not alleged that he knew about or participated in the hacks on the DNC's computers.

In short, the DNC raises a number of connections and communications between the defendants and with people loosely connected to the Russian Federation, but at no point does the DNC allege any facts in the Second Amended Complaint to show that any of the defendants -- other than the Russian Federation -- participated in the theft of the DNC's information. Nor does the DNC allege that the defendants ever agreed to help the Russian Federation steal the DNC's documents. Indeed, the DNC does not raise a factual allegation that suggests that any of the defendants were even aware that the Russian Federation was planning to hack the DNC's computers until after it had already done so. At most, the DNC has alleged that after the Russian Federation stole the DNC's documents, Mifsud and the Agalarovs told campaign members about the stolen documents (although it is unclear whether the communications were about stolen DNC documents or generally about documents harmful to Hillary Clinton), WikiLeaks requested the stolen documents and published them, and some of the other

defendants welcomed the publication of the documents at times helpful to the Campaign.

The DNC has alleged that the Russian Federation hacked into its computer systems and stole its materials. However, the DNC has failed to allege plausibly that any of the other defendants participated in the hack or theft.

C.

The defendants argue that because they are not alleged to have participated in the theft of the DNC's documents, under Bartnicki they cannot be held liable for publishing those documents or encouraging such publication. The DNC argues that Bartnicki is distinguishable and that Bartnicki's holding does not apply to the DNC's claims for trade secret misappropriation.

1.

The DNC's argument for liability is strongest against WikiLeaks because it is the only defendant -- other than the Russian Federation -- that is alleged to have published the stolen information. The DNC alleges that WikiLeaks solicited stolen documents from the GRU and then coordinated with the GRU and the Campaign defendants to publish the stolen documents at times helpful to the Trump Campaign. Like the defendant in Bartnicki, WikiLeaks did not play any role in the theft of the documents and it is undisputed that the stolen materials involve matters of public concern. However, the DNC argues that this

case is distinguishable from Bartnicki because WikiLeaks solicited the documents from the GRU knowing that they were stolen and coordinated with the GRU and the Campaign to disseminate the documents at times favorable to the Trump Campaign. The DNC argues that WikiLeaks should be considered an after-the-fact coconspirator for the theft based on its coordination to obtain and distribute the stolen materials.

As an initial matter, it is constitutionally insignificant that WikiLeaks knew the Russian Federation had stolen the documents when it published them. Indeed, in Bartnicki the Supreme Court noted that the radio host either did know, or at least had reason to know, that the communication at issue was unlawfully intercepted. Bartnicki, 532 U.S. at 517-18; see also Boehner v. McDermott, 484 F.3d 573, 585 (D.C. Cir. 2007) (en banc) (Sentelle, J., dissenting) ("The Supreme Court [has] underlined the lack of constitutional significance of the communicator's knowledge that the interception had been unlawfully conducted.");[22] Jean v. Mass. State Police, 492 F.3d

[22] In Boehner, the Court of Appeals for the District of Columbia Circuit held en banc that former Representative John Boehner could successfully sue Representative Jim McDermott for a violation of 18 U.S.C. § 2511(1)(c) because Representative McDermott disclosed a tape recording of an illegally intercepted conversation in which Representative Boehner participated. However, Part I of the dissenting opinion of Judge Sentelle commanded a majority of the Court. In Part I, Judge Sentelle concluded that Bartnicki applied to Representative McDermott's disclosure of the illegally taped conversation. Judge Sentelle wrote:

24, 31 (1st Cir. 2007) (holding that the First Amendment protected publication in an individual internet post in a case where the publisher "had reason to know that [the recording] had been illegally recorded").

And, contrary to the DNC's argument, it is also irrelevant that WikiLeaks solicited the stolen documents from Russian agents. A person is entitled publish stolen documents that the publisher requested from a source so long as the publisher did not participate in the theft. Jean, 492 F.3d at 31 (holding that the First Amendment protected an individual who posted a

---

> The Supreme Court has decided the first issue of this case, that is, whether the United States (or Florida) can constitutionally bar the publication of information originally obtained by unlawful interception but otherwise lawfully received by the communicator, in the negative. We venture to say that an opposite rule would be fraught with danger. Just as Representative McDermott knew that the information had been unlawfully intercepted, so did the newspapers to whom he passed the information. Representative Boehner has suggested no distinction between the constitutionality of regulating communication of the contents of the tape by McDermott or by The Washington Post or The New York Times or any other media resource. For that matter, every reader of the information in the newspapers also learned that it had been obtained by unlawful intercept.

Boehner, 484 F.3d at 586.

The majority of the en banc Court found that Representative McDermott was not entitled to First Amendment protection solely because Representative McDermott was subject to House of Representatives Ethics Rule 9, which prohibited Committee members from disclosing evidence relating to any investigation by the Committee unless authorized by the Committee. Id. at 580-81. There is no suggestion that there is any similar restriction in this case.

recording on the internet that was illegally recorded and who was in "active collaboration" with the source in disclosing the unlawfully acquired information); see also New York Times, 403 U.S. at 714. Indeed, the DNC acknowledges that this is a common journalistic practice. (DNC Opp'n at 105 (referring to "meeting with information thieves" or "soliciting stolen information" as "common journalistic practices").

The DNC's argument that WikiLeaks can be held liable for the theft as an after-the-fact coconspirator of the stolen documents is also unpersuasive. That argument would eviscerate Bartnicki; such a rule would render any journalist who publishes an article based on stolen information a coconspirator in the theft. Jean, 492 F.3d at 31; Nicholson v. McClatchy Newspapers, 177 Cal. App. 3d 509, 521 (Ct. App. 1986) ("[C]onclusory allegation[s] of a conspiracy cannot serve to transform privileged behavior of the media defendants into tortious misbehavior.").

WikiLeaks and its amici argue that holding WikiLeaks liable in this situation would also threaten freedom of the press. The DNC responds that this case does not threaten freedom of the press because WikiLeaks did not engage in normal journalistic practices by, for example, "asking foreign intelligence services to steal 'new material' from American targets." (DNC Opp'n at 106 (citing SAC ¶ 149).) The DNC's argument misconstrues its

own allegations in the Second Amended Complaint. In the Second Amended Complaint, the DNC states that "WikiLeaks sent GRU operatives using the screenname Guccifer 2.0 a private message, asking the operatives to '[s]end any new material [stolen from the DNC] here for us to review.'" (SAC ¶ 149 (alterations in the original).) This was not a solicitation to steal documents but a request for material that had been stolen.[23] Journalists are allowed to request documents that have been stolen and to publish those documents. See Jean, 492 F.3d at 31; see also New York Times, 403 U.S. at 714; Nicholson, 177 Cal. App. 3d at 521. Therefore, the DNC cannot hold WikiLeaks or Assange liable for publishing the information that Russian agents stole.

2.

The DNC does not allege that the Campaign, the Campaign defendants, the Agalarovs, Stone, or Mifsud ever published any of the stolen documents. And none of the defendants, except the Russian Federation, participated in the theft. Therefore, under Bartnicki the DNC cannot hold these defendants liable for the publication of those documents.

---

[23] The DNC also asserts that WikiLeaks sent Trump Jr. a "password to an anti-Trump political action committee website," so that Trump Jr. could access the site without permission. (SAC ¶ 173.) The DNC argues that this is not a common journalistic practice and therefore WikiLeaks can be held liable. However, it is unclear how that allegation relates to the stolen documents -- the DNC does not allege that it owned the website, or that the website had anything to do with the stolen DNC documents.

The DNC argues that the Campaign, the Campaign defendants, the Agalarovs, Stone, and Mifsud should be liable for the publication of the stolen documents because they encouraged publication and coordinated with WikiLeaks and the GRU to publish the documents at times favorable to the Campaign. Essentially, the DNC seeks to hold these defendants liable for aiding and abetting the publication of the stolen documents.

But even if the documents had been provided directly to the Campaign, the Campaign defendants, the Agalarovs, Stone, and Mifsud, they could have published the documents themselves without liability because they did not participate in the theft and the documents are of public concern. Bartnicki, 532 U.S. at 517. Therefore, the DNC cannot hold these defendants liable for aiding and abetting publication when they would have been entitled to publish the stolen documents themselves without liability.

Accordingly, to the extent that the DNC seeks to hold the Campaign, the Campaign defendants, the Agalarovs, Stone, or Mifsud liable for publishing the stolen documents, those claims are barred by the First Amendment.

3.

The DNC argues that Bartnicki does not apply to the publication of trade secrets and, therefore, the First Amendment

does not protect the defendants from the DNC's claims because its claims are based on the theft of alleged trade secrets.

The DNC alleges that trade secrets were stolen by the Russian Federation in the April and September 2016 hacks of its computer systems. However, only the alleged trade secrets stolen in the April 2016 hack are at issue because the DNC does not allege that the documents stolen in September 2016 were ever given to any of the other defendants by the Russian Federation. The DNC alleges that on July 22, 2016, WikiLeaks published "donor lists" and "fundraising strategies," which the DNC asserts were trade secrets stolen by the Russian Federation. The DNC alleges that the material "would reveal critical insights into the DNC's political, financial, and voter engagement strategies." (SAC ¶ 106.) The DNC does not allege that any other defendant possessed or published any of these documents.

The DNC argues that "the Bartnicki Court specified that its holding did not permit the disclosure of trade secrets." (DNC Opp'n at 104.) But that is not quite right. The Bartnicki Court did not say that its holding "did not permit" the disclosure of trade secrets. Rather, the Court in Bartnicki acknowledged that important privacy interests are served by the federal statute, 18 U.S.C. § 2511(c), that criminalizes the disclosure of illegally intercepted communications and the issue

is whether the interests protected by the statute are sufficient to overcome the First Amendment interest in allowing the publication of truthful information on a matter of public concern. In that context, the Supreme Court stated:

> We need not decide whether that interest is strong enough to justify the application of § 2511(c) to disclosures of trade secrets or domestic gossip or other information of purely private concern. Cf. Time, Inc. v. Hill, 385 U.S. 374, 387-388 (1967) (reserving the question whether truthful publication of private matters unrelated to public affairs can be constitutionally proscribed). In other words, the outcome of these cases does not turn on whether § 2511(1)(c) may be enforced with respect to most violations of the statute without offending the First Amendment. The enforcement of that provision in these cases, however, implicates the core purposes of the First Amendment because it imposes sanctions on the publication of truthful information of public concern.

Bartnicki, 532 U.S. at 533-34. So too in this case. It is unnecessary to determine what protection trade secrets should receive in matters of purely private concern. It is sufficient for this case to find that the DNC's privacy interest in the alleged trade secrets is insufficient to overcome the strong public interest in the publication of matters of paramount public concern.

In this case it is plain that the DNC's conclusory allegations that "donor lists" and "fundraising strategies" were among those documents published by WikiLeaks does not provide a

basis to overcome the First Amendment. The DNC's interest in keeping "donor lists" and "fundraising strategies" secret is dwarfed by the newsworthiness of the documents as whole. Id. at 534 ("[P]rivacy concerns give way when balanced against the interest in publishing matters of public importance.").

If WikiLeaks could be held liable for publishing documents concerning the DNC's political financial and voter-engagement strategies simply because the DNC labels them "secret" and trade secrets, then so could any newspaper or other media outlet. But that would impermissibly elevate a purely private privacy interest to override the First Amendment interest in the publication of matters of the highest public concern.[24] The DNC's published internal communications allowed the American electorate to look behind the curtain of one of the two major political parties in the United States during a presidential election. This type of information is plainly of the type entitled to the strongest protection that the First Amendment offers. Buckley v. Valeo, 424 U.S. 1, 14 (1976) ("Discussion of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution. The First Amendment affords

[24] At the argument of the current motions, counsel for the DNC argued that the DNC is a private party with the right to protect its trade secrets. But that misses the point. The DNC cannot prevent the publication of matters of public concern simply by labeling them trade secrets.

the broadest protection to such political expression . . . ."). Indeed, the DNC alleges that the publication of the stolen documents was so significant that it had an impact on the course of a presidential election. The DNC's conclusory allegations that "donor lists" and "fundraising strategies" were among those documents are insufficient to pierce the shield that the First Amendment provides for core political speech. Florida Star, 491 U.S. at 536-37 (holding a newspaper could not be held liable for publishing a victim's name in violation of state law where "the article generally, as opposed to the specific identity contained within it, involved a matter of paramount public import").

Therefore, the DNC cannot hold WikiLeaks liable for the publication of the DNC's alleged trade secrets in this case. And the remaining defendants -- with the exception of the Russian Federation -- did not steal or publish any of the DNC's documents. To the extent that the DNC is seeking to hold those defendants liable for the publication of the DNC's trade secrets, those claims are barred for the same reasons just explained.

* * *

In sum, the DNC does not allege any facts to show plausibly that any of the defendants, other than the Russia Federation, had any role in hacking the DNC's computers or stealing its information -- it attributes that conduct only to the Russian

Federation. And the DNC does not dispute that the documents were of public importance. Therefore, the First Amendment protects the publication of those stolen documents. Accordingly, all of the DNC's claims against the defendants other than the Russian Federation[25] are **dismissed.**[26]

Although all of the DNC's claims are dismissed against all of the defendants because the defendants' actions -- other than those of the Russian Federation -- are protected by the First Amendment and Russia is immunized by the FSIA, there are additional reasons for dismissing specific claims against the defendants. Those reasons are explained below.

VI.

The DNC brings claims against all defendants for violation of RICO, 18 U.S.C. § 1961 et seq. Section 1964(c) of RICO provides that "[a]ny person injured in his business or property by reason of a violation of [18 U.S.C. § 1962] may sue therefor

---

[25] As explained above, the claims against the Russian Federation must be dismissed pursuant to the FSIA.

[26] Although Manafort, Assange, and Mifsud have not appeared in the case and did not move to dismiss the Second Amended Complaint, it is plain that their actions would be protected by the First Amendment. Moreover, the DNC agreed at oral argument that Manafort, Trump Jr., and Assange were properly before the Court on these motions. Therefore, the claims against those defendants and Mifsud are dismissed.

in any appropriate United States district court." 18 U.S.C. § 1964(c).

In order to state a claim under § 1962(c), a plaintiff must allege "(1) conduct (2) of an enterprise (3) though a pattern (4) of racketeering activity." DeFalco v. Bernas, 244 F.3d 286, 306 (2d Cir. 2001) (quoting Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479, 496 (1985)). "Racketeering activity" encompasses, among other things, any act indictable for crimes enumerated under 18 U.S.C. § 1961(1)(B), which include, for purposes relevant to the present case, 18 U.S.C. § 1831 (economic espionage), 18 U.S.C. § 1832 (theft of trade secrets), 18 U.S.C. § 1503 (relating to obstruction of justice), and 18 U.S.C. § 1512 (relating to tampering with a witness, victim, or an informant).

A.

The DNC asserts that there are two enterprises: the Campaign itself (the "Campaign enterprise") and an association-in-fact enterprise (the "AIF enterprise"). Each defendant is alleged to be a part of the Campaign enterprise with the exception of the Campaign itself.[27] The DNC alleges that each

[27] Indeed, "a corporate entity may not be both the RICO person and the RICO enterprise under section 1962(c)." 4 K & D Corp. v. Concierge Auctions, LLC, 2 F. Supp. 3d 525, 535 (S.D.N.Y. 2014) (quoting Riverwoods Chappaqua Corp. v. Marine Midland Bank, N.A., 30 F.3d 339, 344 (2d Cir. 1994)).

defendant and Corsi, who is not a defendant, were a part of the AIF enterprise.

The Campaign enterprise qualifies as an enterprise under RICO. First Capital Asset Mgmt., Inc. v. Satinwood, Inc., 385 F.3d 159, 173 (2d Cir. 2004) ("[A]ny legal entity may qualify as a RICO enterprise."). However, the DNC has failed to allege adequately the existence of an AIF enterprise. An AIF enterprise "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." Boyle v. United States, 556 U.S. 938, 945 (2009) (quoting United States v. Turkette, 452 U.S. at 583 (1981)). This type of RICO enterprise "must have at least three structural features: (1) a purpose, (2) relationships among those associated with the enterprise, and (3) longevity sufficient to permit these associates to pursue the enterprise's purpose." Id. at 946; D. Penguin Bros. v. City Nat. Bank, 587 F. App'x 663, 667-68 (2d Cir. 2014) ("[F]or an association of individuals to constitute an enterprise," the members of the association must "share a common purpose to engage in a particular fraudulent course of conduct and work together to achieve such purposes." (quoting Cruz v. FXDirectDealer, LLC, 720 F.3d 115, 120 (2d Cir. 2013))).

In this case, the DNC has not plausibly alleged a common purpose or sufficient relationships to assert an AIF enterprise.

While the Second Amended Complaint asserts numerous predicate acts to demonstrate the existence of a pattern of racketeering activity, such allegations are not necessarily sufficient to show an association-in-fact RICO enterprise -- the enterprise must have an existence separate and apart from the racketeering activity itself. United States v. Cain, 671 F.3d 271, 289 n.7 (2d Cir. 2012) (A RICO enterprise "is an entity separate and apart from the pattern of activity in which it engages." (quoting Turkette, 452 U.S. at 583)). The DNC's allegations provide no basis to infer either that the alleged AIF members formed an ongoing organization or that the defendants formed a coherent entity that was separate and apart from the predicate acts that allegedly comprise the alleged fraudulent scheme. See D. Penguin Bros., 587 F. App'x at 668; First Asset Capital Mgmt., 385 F.3d at 174.

This is, in part, because the DNC alleges in conclusory fashion that various individuals and entities have committed acts to further the scheme despite not having any apparent connection to most of the other defendants. The DNC asserts only that there were scattered contacts between the alleged AIF members and does not assert any facts suggesting hierarchy or organization. For example, none of the asserted AIF members are alleged to have participated in the theft of the DNC's documents with the Russian Federation or to have even been aware that the

Russian Federation was planning such a theft. The Russian Federation published at least some of the documents via Guccifer 2.0, and there is no allegation that any of the defendants participated in that publication. WikiLeaks contacted the GRU to obtain the stolen documents, but there is no indication that any of the other asserted AIF members were aware of this contact. See D'Addario v. D'Addario, 901 F.3d 80, 101 (2d Cir. 2018) (quoting Boyle, 556 U.S. at 947 n.4), cert. denied, 139 S. Ct. 1331 (2019).

Further, the asserted AIF members are alleged to have been pursuing various goals independent of one another. The Russian Federation stole the documents because it wanted "to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency." (SAC ¶ 81.) WikiLeaks sought to distribute the documents because it had an axe to grind with Hillary Clinton. (Id. ¶ 78.) The Agalarovs sought to use their relationships with the Trump family to "curr[y] favor with Russian officials." (Id. ¶ 80.) And the remaining defendants -- who were part of the Trump Campaign, confidants of Donald Trump's, or, in Corsi's case, an associate of Stone's -- were seeking to get Donald Trump elected president. There is no indication that there was any structure or hierarchy to this group.

Moreover, the alleged common goal of the AIF enterprise -- to get Donald Trump elected -- is not an unlawful or fraudulent goal. Purchase Real Estate Grp. v. Jones, No. 05cv10859, 2010 WL 3377504, at *6 (S.D.N.Y. Aug. 24, 2010) (stating that members of an AIF enterprise must "share a common purpose to engage in a particular fraudulent course of conduct and work together to achieve such purposes" (quotation marks omitted)). The DNC cannot circumvent the separate enterprise requirement by alleging that illegal means were used to obtain a lawful objective -- that argument seeks to create an AIF enterprise based on individual, uncoordinated racketeering acts alone. See D. Penguin Bros., 587 F. App'x at 668 (holding that an AIF enterprise must exist separate and apart from the pattern of racketeering activity in which it engages).

A plaintiff may not simply "string[] together . . . various defendants and label[] them an enterprise." Town of Mamakating, N.Y. v. Lamm, No. 15cv2865, 2015 WL 5311265, at *9 (S.D.N.Y. Sept. 11, 2015), aff'd, 651 F. App'x 51 (2d Cir. 2016). That is what the DNC attempts to do here. Therefore, the DNC has failed to allege the existence of an AIF enterprise. See Heffernan v. HSBC Bank USA, No. 99cv7981, 2001 WL 803719, at *5 (E.D.N.Y. Mar. 29, 2001) ("An association-in-fact enterprise is not created every time a combination of individuals or entities acts in concert to commit racketeering acts.").

B.

Kushner, WikiLeaks, the Campaign, the Agalarovs, Papadopoulos, and Stone argue that the DNC's RICO claim also fails because the DNC has not alleged that they conducted the affairs of either alleged enterprise.

Under 18 U.S.C. § 1962(c), the plaintiff must show that each defendant "conduct[ed] or participate[d], directly or indirectly, in the conduct of [the] enterprise's affairs." Reves v. Ernst & Young, 507 U.S. 170, 177, 179 (1993) ("[T]he word 'participate' makes clear that RICO liability is not limited to those with primary responsibility for the enterprise's affairs[,] . . . but some part in directing that enterprise's affairs is required."). This element of a § 1962(c) RICO claim is often referred to as the "operation or management" requirement. See id. at 185.

"In this Circuit, the 'operation and management' test is an extremely rigorous test," and "[i]t is not enough to merely take directions and perform 'tasks that are necessary and helpful' to the enterprise. . . . Nor is it enough to simply provide 'goods and services that ultimately benefit the enterprise.'" United States Fire Ins. Co. v. United Limousine Serv., Inc., 303 F. Supp. 2d 432, 451-52 (S.D.N.Y. 2004); see also Elsevier Inc. v. W.H.P.R., Inc., 692 F. Supp. 2d 297, 307-08 (S.D.N.Y. 2010) (dismissing RICO claims against several individual defendants

because "it is not enough to allege that a defendant provided services that were helpful to an enterprise, without alleging facts that, if proved, would demonstrate some degree of control over the enterprise"). This standard is not met where a defendant merely attends to its own business; "liability depends on showing that the defendants conducted or participated in the conduct of the enterprise's affairs, not just their own affairs." Reves, 507 U.S. at 185 (quotation marks omitted).

1.

The DNC has not alleged that any of the defendants operated or managed the alleged AIF enterprise. Rather, each defendant is alleged only to have provided some service or benefit to the AIF enterprise's asserted goal: securing Donald Trump's election. The Russian Federation is alleged to have stolen the documents without telling any of the other alleged AIF members; the Agalarov's are alleged only to have coordinated a meeting with Trump Jr. to discuss "dirt" about Hillary Clinton; Mifsud is alleged to have told Papadopoulos about emails that could be harmful to Hillary Clinton's presidential campaign; WikiLeaks and Assange are alleged only to have distributed the documents and coordinated with the Campaign and GRU regarding release times; Corsi and Stone are alleged to have coordinated with WikiLeaks and/or the GRU about documents that appear to have been stolen primarily or totally from sources other than the

DNC; and Manafort, Gates, and Kushner are alleged to have been carrying on the affairs of the Campaign. Each of these alleged AIF members were working on separate tracks without any allegation that someone was managing or operating the overall group. See Elsevier Inc. v. W.H.P.R., Inc., 692 F. Supp. 2d at 307-08.

2.

Similarly, a majority of the defendants are not alleged to have managed or operated the Campaign enterprise.

Indeed, all of the defendants who were not members of the Campaign -- the Russian Federation, Mifsud, WikiLeaks, Assange, and Stone -- are alleged only to have provided some service to the Campaign: the Russian Federation stole the documents; Mifsud told Papadopoulos about emails "that could harm Hillary Clinton's presidential campaign"; the Agalarovs told Trump Jr. about "documents and information that would incriminate Hillary [Clinton]"; WikiLeaks published the documents; and Stone spoke to WikiLeaks through Corsi and to the Russian Federation about publishing some documents. Each of these acts amounts to an alleged service to the Campaign but do not show that any of those defendants were managing or operating the Campaign. And there is also no allegation that Papadopoulos was managing or operating the Campaign -- he was a foreign policy advisor who provided a service to the Campaign by speaking to Mifsud.

However, the DNC has alleged that Manafort, Gates, and Kushner held managerial positions in the Trump Campaign, which is enough to state a claim that they were operating or managing the Campaign enterprise.

C.

The Agalarovs, Kushner, Papadopoulos, Stone, WikiLeaks, and the Campaign also argue that the DNC has failed to allege a "pattern" of racketeering activity.

To allege a RICO violation, the plaintiff must plead at least two predicate acts, show that the predicate acts are related, and that they amount to, or pose a threat of, continuing criminal activity. See H.J. Inc. v. Nw. Bell Tel. Co., 492 U.S. 229, 239 (1989). Predicate acts are "related" for RICO purposes when they "have the same or similar purposes, results, participants, victims, or methods of commission, or otherwise are interrelated by distinguishing characteristics and are not isolated events." Id. at 240 (quotation marks omitted). The DNC asserts that the defendants violated four statutes that provide the basis for predicate RICO acts: 18 U.S.C. § 1831(a)(5) (economic espionage); 18 U.S.C. § 1832(a)(5) (theft of trade secrets); 18 U.S.C. § 1503 (relating to obstruction of justice); and 18 U.S.C. § 1512 (relating to tampering with a witness, victim, or an informant).

1.

Sections 1831 and 1832 are asserted as predicate acts against each of the defendants and Corsi. Those sections are part of the Economic Espionage Act. The two statutes "guard against the same types of threats to trade secrets, albeit from actors with different motivations": section 1831 prohibits stealing or misusing trade secrets for the benefit of any foreign government; section 1832 prohibits stealing or misusing trade secrets for the benefit of anyone other than the owner. United States v. Aleynikov, 737 F. Supp. 2d 173, 180 (S.D.N.Y. 2010). The statutes' conspiracy provisions reflect these different objectives. Both provisions create liability for someone who "conspires with one or more other persons to" commit a substantive violation of the respective statutes, and commits any act to effect the object of the conspiracy. 18 U.S.C. §§ 1831(a)(5), 1832(a)(5).

Sections 1831 and 1832 were added to the list of RICO predicates on May 11, 2016. See Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat 376 (May 11, 2016) (codified at 18 U.S.C. § 1836 et seq.). Therefore, alleged violations of sections 1831 and 1832 can serve as predicate acts only for offenses occurring after May 11, 2016. See Attia v. Google LLC, No. 17cv6037, 2018 WL 2971049, at *8 (N.D. Cal. June 13, 2018) ("Plaintiffs are required to allege that they suffered injury

proximately caused by trade secret theft by each Defendant after May 11, 2016."); Micron Tech., Inc. v. United Microelectronics Corp., No. 17cv06932, 2019 WL 1959487, at *12 (N.D. Cal. May 2, 2019) (same); Magnesita Refractories Co. v. Tianjin New Century Refractories Co., No. 17cv1587, 2019 WL 1003623, at *11 (M.D. Pa. Feb. 28, 2019) (same). Accordingly, certain acts alleged in the Second Amended Complaint cannot serve as predicate acts to sustain the DNC's RICO and RICO conspiracy claims, namely the Russian Federation's hack of the DNC's computers in 2015 and April 2016.

The DNC alleges that the Russian Federation extracted documents from the DNC's email server between May 25 and June 1, 2016 and in September 2016. The DNC argues that these thefts and the subsequent publication of the documents can serve as predicate RICO acts. However, the documents alleged to have been stolen between May 25 and June 1 were from the DNC's email server and are not alleged to have contained any trade secrets. (See SAC ¶¶ 123-31.) Moreover, the Russian Federation is the only defendant who is alleged to have participated in any of the thefts of the DNC's information, and the Russian Federation and WikiLeaks are the only defendants who are alleged to have possessed or published the stolen information. Indeed, the Agalarovs, Mifsud, Stone, the Campaign, and the Campaign defendants are not alleged to have stolen, possessed, or

published any of the DNC's stolen information. The DNC does not provide any plausible factual allegations that any of these defendants knew that there were trade secrets among the stolen documents. Mifsud is alleged to have told Papadopoulos about emails that could be damaging to Hillary Clinton; the Agalarovs are alleged to have told Trump Jr., Manafort, and Kushner about "derogatory information on candidate Clinton from Russian sources," (SAC ¶ 219); WikiLeaks is alleged to have provided Trump Jr. with the password to an anti-Trump website which is not alleged to be owned by the DNC; Stone is alleged to have communicated with the GRU and with WikiLeaks through Corsi. But at no point does the DNC allege that the Agalarovs, Mifsud, the Campaign, Corsi, Stone, or the Campaign defendants ever stole, possessed, discussed, or were even made aware of any stolen trade secrets.

Accordingly, the acts alleged in the Second Amended Complaint to be violations of sections 1831 and 1832 cannot serve as predicate acts for the Agalarovs, Mifsud, Stone, the Campaign, or the Campaign defendants.

2.

The DNC also argues that it has alleged predicate acts for: obstruction of justice under 18 U.S.C. § 1503 against Papadopoulos, Stone, and Manafort; witness tampering under 18 U.S.C. § 1512 against Stone; destroying evidence under 18 U.S.C.

§ 1512(c)(1) against Corsi and Papadopoulos; and obstructing an official proceeding under 18 U.S.C. § 1512(c)(2) against Papadopoulos, Kushner, Stone, Trump Jr., and Manafort. The DNC also asserts that Corsi and Stone conspired to destroy evidence, obstruct an official proceeding, and tamper with a witness in violation of 18 U.S.C. § 1512(k). Each of these acts are alleged to have taken place in 2017 or 2018 after the alleged goal of the conspiracy had already been attained: Donald Trump becoming president.[28] The Second Amended Complaint alleges that "[f]rom the date the [AIF] Enterprise was formed until the present, the members of the [AIF] Enterprise have worked together to further their mutual goal of using illegal means to secure Trump's grip on the Presidency, in part by damaging the DNC." (Id. ¶ 272.) The DNC argues that the alleged acts of obstruction were done to conceal the defendants' allegedly unlawful acts of theft and publication of the DNC's documents.

"[A]cts of concealment done in furtherance of the main criminal objectives of the conspiracy" are considered part of the conspiracy. Grunewald v. United States, 353 U.S. 391, 405 (1957). However, "acts of concealment done after the[] central objectives [of the conspiracy] have been attained, for the

[28] The Trump Campaign is "an American not-for-profit corporation formed and registered in Virginia on June 17, 2015 to support Trump's candidacy for President of the United States." (SAC ¶ 55.)

purpose of covering up after the crime," are not considered part of the conspiracy. Id. Here, the alleged acts of concealment were all done allegedly to cover the defendants' tracks after the goal of the alleged conspiracy had been attained. Therefore, they cannot be found to be predicate acts for the purposes of the DNC's RICO claim. Browning v. Flexsteel Indus., Inc., 955 F. Supp. 2d 900, 919 (N.D. Ind. 2013) ("Labeling a[] crime and its cover-up as a 'pattern of racketeering activity' is problematic even where the underlying crime is itself a RICO predicate act, because a scheme to conceal underlying criminal activity does not extend the length of a RICO scheme."); see also Midwest Grinding Co., Inc. v. Spitz, 976 F.2d 1016, 1024 (7th Cir. 1992) ("A conspiracy ends when the design to commit substantive misconduct ends, it does not continue beyond that point 'merely because the conspirators take steps to bury their traces, in order to avoid detection and punishment after the central criminal purpose has been accomplished.'" (quoting Grunewald, 353 U.S. at 405)).[29]

---

[29] "It may be that in some cases, the acts of concealment are integral to the underlying criminal scheme itself and therefore cause the alleged harm just as much as the non-predicate acts." Browning, 955 F. Supp. 2d at 919. For example, where predicate acts of money laundering are instrumental in covering up an embezzlement scheme, see City of New York v. Venkataram, 396 F. App'x 722, 725 (2d Cir. 2010), or when mail fraud is necessary to induce the sale or lease of environmentally contaminated property, see Fresh Meadow Food Servs., LLC v. RB 175 Corp., 282 F. App'x 94, 99 (2d Cir. 2008), the acts of concealment can be predicate acts for purposes of RICO. This is not such a case. In this case, the harm suffered by the DNC -- theft and publication of its internal documents and communications -- had already taken place before the alleged acts of concealment. The DNC does not allege that

Accordingly, none of the plaintiff's allegations under 18 U.S.C. §§ 1503 and 1512 can serve as predicate acts for the DNC's RICO claim.

D.

The Agalarovs, the Campaign, Kushner, Stone, Papadopoulos, and WikiLeaks also argue that the DNC's allegations do not satisfy RICO's continuity requirement for the alleged pattern of racketeering activity.

"To establish a RICO pattern[,] it must also be shown that the predicates themselves amount to, or that they otherwise constitute a threat of, continuing racketeering activity" -- commonly called the continuity requirement. H.J. Inc., 492 U.S. at 240. "'Continuity' is both a closed- and open-ended concept, referring either to a closed period of repeated conduct, or to past conduct that by its nature projects into the future with a threat of repetition." Id. at 241. Predicates have closed-ended continuity if they "extend[ed] over a substantial period

---

the defendants' alleged acts of concealment were done in order to allow the defendants to continue stealing documents or to continue publishing documents to further the election of Donald Trump. Indeed, the DNC does not allege that any documents were published after the 2016 presidential election concluded. The DNC's argument that the defendants' alleged acts of concealment were done so that they could continue to steal documents and publish them in the run up to the 2020 presidential election is entirely conclusory and speculative. The alleged conspiracy was to hack, steal, and publish documents in support of Donald Trump's 2016 presidential run -- that alleged conspiracy terminated when Donald Trump was elected president. Therefore, the alleged acts of concealment under §§ 1503 and 1512 were not a part of the alleged conspiracy and cannot be considered predicate acts.

of time" in the past, id. at 242; by contrast, predicates have open-ended continuity if they "by [their] nature project[] into the future with a threat of repetition," Reich v. Lopez, 858 F.3d 55, 60 (2d Cir.), cert. denied, 138 S. Ct. 282 (2017). The DNC argues that it has alleged both.

1.

For closed-ended continuity, a plaintiff must allege "a series of related predicates extending over a substantial period of time." H.J. Inc., 492 U.S. at 242. In the Second Circuit, two years is generally required. Reich, 858 F.3d at 60 ("[T]his Circuit generally requires that the crimes extend over at least two years."). The DNC asserts that the conspiracy began in March 2016. It ended, at the latest, on election day in November 2016. Nine months is not a sufficient amount of time for closed-ended continuity. Id. at 60 ("Predicate acts separated by only a few months will not do . . . ."); Spool v. World Child Int'l Adoption Agency, 520 F.3d 178, 184 (2d Cir. 2008) ("[W]e have never held a period of less than two years to constitute a substantial period of time." (quotation marks omitted)). Therefore, the DNC has not established closed-ended continuity.[30]

---

[30] The DNC does not credibly allege closed-ended continuity. In its opposition to the current motions, the DNC argues that "Trump, Jr., Manafort, Kushner, and Stone all committed a variety of predicate crimes for well over a year." (DNC Opp'n at 67.) This refers to alleged acts of obstruction which, as explained above, were not predicate acts in furtherance of the RICO

2.

Open-ended continuity -- "criminal activity 'that by its nature projects into the future with a threat of repetition'" -- can be established in several ways:

> Some crimes may by their very nature include a future threat, such as in a protection racket. When the business of an enterprise is primarily unlawful, the continuity of the enterprise itself projects criminal activity into the future. And similarly, criminal activity is continuous when the predicate acts were the regular way of operating that business, even if the business itself is primarily lawful.

Reich, 858 F.3d at 60 (citations and quotation marks omitted).

In this case, the alleged unlawful activity, the hack and theft the DNC's documents, do not include a future threat of repetition -- those alleged crimes were terminal in nature. Moreover, the alleged theft and publication was not the defendants' "regular way of operating [their] business." Cofacredit, S.A. v. Windsor Plumbing Supply Co., 187 F.3d 229, 243 (2d Cir. 1999). And the DNC cannot plausibly allege that the defendants' business was primarily unlawful: the asserted goal of the enterprises was to get Donald Trump elected, which is not unlawful. See Reich, 858 F.3d at 60 ("Even if [the defendant] pays bribes, it is primarily in the energy business;

---

conspiracy and, in any event, the alleged time period is far less than the Court of Appeals for the Second Circuit requires for closed-ended continuity.

it is not a narcotics ring or an organized crime family."); see also Cofacredit, 187 F.3d at 243 ("[W]here the enterprise primarily conducts a legitimate business, there must be some evidence from which it may be inferred that the predicate acts were the regular way of operating that business, or that the nature of the predicate acts themselves implies a threat of continued criminal activity.").

Therefore, the DNC's allegations do not satisfy RICO's continuity requirement for the alleged pattern of racketeering activity.

* * *

For all of the foregoing reasons, the plaintiff has failed to allege a violation of RICO. Therefore, the DNC's RICO claim is **dismissed against all defendants.**

VII.

The DNC also asserts that each defendant entered into a RICO conspiracy. However, a RICO "conspiracy claim must be dismissed where the substantive RICO claim is deficient." Nat'l Grp. for Commc'ns and Computs. Ltd. v. Lucent Techs. Inc., 420 F. Supp. 2d 253, 272 (S.D.N.Y. 2006). Therefore, the DNC'S RICO conspiracy claim is **dismissed against all defendants.**

VIII.

The DNC asserts that WikiLeaks, the Campaign, the Campaign defendants, and Stone violated the Wiretap Act. The Campaign,

Papadopoulos, WikiLeaks, Kushner, and Stone argue that the DNC has failed to allege a violation of that Act.

The Wiretap Act imposes liability on any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" (the "interception provision"); "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication" (the "disclosure provision"); or "intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication" (the "use provision"). 18 U.S.C. § 2511(1)(a), (c), (d). "'[I]ntercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Id. § 2510(4). The term "intercept" is construed narrowly "to require that the interception of an electronic communication be contemporaneous with the transmission of that communication."

Tantaros v. Fox News Network, No. 17cv2958, 2018 WL 2731268, at *7 (S.D.N.Y. May 18, 2018).[31]

The DNC argues that WikiLeaks violated the Act's disclosure and use provisions and that the Campaign, the Campaign defendants, and Stone violated the Act's use provision. The DNC's argument is not persuasive.

There is no allegation that any of the documents provided to WikiLeaks contained communications that were intercepted contemporaneously with transmission. The documents that the Russian Federation disclosed to WikiLeaks are described as reports and documents rather than items that would suggest electronic communications that were recorded simultaneously with their transmission. (SAC ¶ 148.) In any event, there is no allegation that WikiLeaks was aware that any documents it published were intercepted contemporaneously with transmission.[32]

---

[31] "Every circuit court to have considered the matter has held that an 'intercept' under the Act must occur contemporaneously with transmission." Luis v. Zang, 833 F.3d 619, 627 (6th Cir. 2016) (quotation marks omitted).

[32] At oral argument, counsel for the DNC argued that there is no requirement under the Wiretap Act "that the parties have reason to know that the communication was simultaneously intercepted." (Tr. at 66.) Counsel argued that, instead, "having a reason to know" "only requires the plaintiff allege an awareness that neither party to the intercepted communication had consented to its interception." (Tr. at 65 (citing Fernicola v. Specific Real Prop. in Possession, Custody, Control of Healthcare Underwriters Mutual Insurance Co., No. 00cv5173, 2001 WL 1658257 (S.D.N.Y. Dec. 26, 2001)).) The case cited by the plaintiff in support of its argument, Fernicola, did not address the issue of whether a person was required to know that the communication was intercepted contemporaneously with transmission. Id. at *7. The claim under the statute was dismissed because the defendant lacked knowledge that the information was intercepted in violation of the statute. Id. The text of the statute and the caselaw interpreting it do not support the DNC's argument. See 18 U.S.C. § 2511(1)(d) (requiring that defendants

There would not be anything on the face of emails or reports to indicate that they were intercepted contemporaneously rather than stolen from an archive.

As for the defendants who are not alleged to have possessed or published any of the stolen documents, the only possible route to liability is through a strained reading of the statute's "use" provision based on those defendants' coordination with WikiLeaks and the GRU to publish the documents. But even that tenuous argument is insufficient because there is no allegation that any of those defendants "kn[ew] or ha[d] reason to know that the information was obtained through . . . interception." 18 U.S.C. § 2511(1)(d); Zaratzian v. Abadir, No. 10cv9049, 2014 WL 4467919, at *10 (S.D.N.Y. Sept. 2, 2014), aff'd, 694 F. App'x 822 (2d Cir. 2017).

Therefore, the DNC has failed to allege a violation of the Wiretap Act against any of the defendants with the exception of the Russian Federation. However, the DNC does not assert a claim for violation of the Wiretap Act against the Russian

---

"kn[ew] or ha[d] reason to know that the information was obtained through . . . interception."); McCann v. Iroquois Mem'l Hosp., 622 F.3d 745, 753 (7th Cir. 2010) ("To be liable under § 2511(1)(c) or § 2511(1)(d), a defendant must know or have reason to know 'sufficient facts concerning the circumstances of the interception such that the defendant[ ] could, with presumed knowledge of the law, determine that the interception was prohibited in light of [the Wiretap Act].'" (quotation marks omitted)); Zaratzian v. Abadir, No. 10cv9049, 2014 WL 4467919, at *10 (S.D.N.Y. Sept. 2, 2014) (same), aff'd, 694 F. App'x 822 (2d Cir. 2017).

Federation and, in any event, the Russian Federation could not be held liable because of the FSIA. Therefore, all of the DNC's Wiretap Act claims are **dismissed.**

IX.

The DNC claims that WikiLeaks and the Russian Federation violated the federal Defend Trade Secrets Act ("DTSA") and that all of the defendants violated the D.C. Uniform Trade Secrets Act ("DCUTSA").

The DTSA and DCUTSA require essentially the same allegations. See 18 U.S.C. § 1839; D.C. Code Ann. § 36-401; see also Jazz Pharm., Inc. v. Synchrony Grp., LLC, 343 F. Supp. 3d 434, 445 (E.D. Pa. 2018) (finding that the DTSA and Pennsylvania Uniform Trade Secret Act, which is the same as the DCUTSA, share a common definition of a "trade secret"). To state a claim for trade secret misappropriation, "a plaintiff must plausibly allege that (1) it possessed a trade secret, and (2) the defendant misappropriated the trade secret." Medidata Sols., Inc., v. Veeva Sys. Inc., No. 17cv589, 2018 WL 6173349, at *3 (S.D.N.Y. Nov. 26, 2018); D.C. Code Ann. § 36-401. A plaintiff claiming misappropriation of trade secrets may show that the defendant gained access to the trade secrets through improper means or "that the defendant improperly used or disclosed trade secrets." DSMC, Inc. v. Convera Corp., 479 F. Supp. 2d 68, 79 (D.D.C. 2007) (emphasis added); 18 U.S.C. § 1839. Trade secrets

are any form of financial or business information, "including patterns, plans . . . methods, techniques, processes, [and] procedures . . . [that] (A) the owner thereof has taken reasonable measures to keep . . . secret; and (B) . . . derives independent economic value, actual or potential, from not being generally known." 18 U.S.C. § 1839(3)(A)-(B); D.C. Code Ann. § 36-401(3). "[T]o survive a motion to dismiss, a party alleging that it owns a trade secret must put forth specific allegations as to the information owned and its value." Elsevier Inc. v. Doctor Evidence, LLC, No. 17cv5540, 2018 WL 557906, at *4 (S.D.N.Y. Jan. 23, 2018). While the party must allege more than "conclusory statements that simply restate the elements of a trade secret," id., the allegations need only specify "the general contours of the alleged trade secrets," Dardashtian v. Gitman, No. 17cv4327, 2017 WL 6398718, at *5 (S.D.N.Y. Nov. 28, 2017).

The DNC argues that WikiLeaks acquired the DNC's trade secrets knowing that they had been stolen. Specifically, the DNC alleges that on July 22, 2016, WikiLeaks published "donor lists" and "fundraising strategies." (SAC ¶ 156.)[33] These

[33] The Second Amended Complaint makes more detailed allegations about the Russian Federation's theft of materials in the September 2016 hack, (SAC ¶¶ 180, 182-86), but there are no allegations that these materials were provided to WikiLeaks or published. The SAC asserts: "The GRU could have derived significant economic value from the theft of the DNC's data by, among other possibilities, selling the data to the highest bidder." (Id. ¶ 193.) There is no allegation that the Russian Federation did in fact sell the DNC's

conclusory allegations are insufficient to state that the stolen documents were trade secrets. See Iqbal, 556 U.S. at 678. The DNC has not identified anything about the process of developing donor lists or fundraising strategies or shown how their particular value derives from their secrecy. See Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz, 82 F. Supp. 3d 344, 361 (D.D.C. 2015). Therefore, the DNC has failed to state a claim for trade secret misappropriation against WikiLeaks under either the DTSA or the DCUTSA.

The DNC does not allege that any defendant other than the Russian Federation and WikiLeaks possessed or published its alleged trade secrets. However, the DNC argues that the remaining defendants are still liable under the DCUTSA because they "used" the documents after they had been published by WikiLeaks and the Russian Federation. This argument is untenable -- a "trade secret that becomes public knowledge is no longer a trade secret." BondPro Corp. v. Siemens Power Generation, 463 F.3d 702, 706 (7th Cir. 2006). That the defendants might have used documents that had already been published by the Russian Federation and WikiLeaks is not an unlawful or improper use of the documents.

---

data, and any claims against the Russian Federation under the federal and state statutes proscribing trade secret theft are barred by the FSIA.

Therefore, in addition to the fact that the trade secret claims are barred by the First Amendment, the DNC has failed to state a claim for trade secret misappropriation. The DNC's trade secret claims are **dismissed**.

X.

The DNC asserts its claim for conspiracy to commit trespass to chattels under Virginia common law against all of the defendants.

There are three elements to civil conspiracy under Virginia common law: "(1) that two or more persons engaged in concerted action; (2) to accomplish some criminal or unlawful purpose, or some lawful purpose by some criminal and unlawful means; and (3) that actual damages resulted from something done by one or more of the conspirators in furtherance of the object of the conspiracy." Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 452 (E.D. Va. 1998). Furthermore, to commit a trespass to chattels, one must "intentionally use[] or intermeddle[] with personal property in rightful possession of another without authorization" in a way that "impare[s] . . . the condition, quality, or value" of the chattel. Id. (quotation marks omitted).

Hacking a computer network may qualify as trespass to chattels. Id. A "computer network" may qualify as a chattel because "computers . . . are tangible personal property." Id.

The unauthorized "transmission of electrical signals through a computer network [may be] sufficiently 'physical'" to qualify as intermeddling. Id.

The DNC has alleged that the Russian Federation hacked its computer system and caused property damage. However, as explained above, the DNC has not alleged plausibly that any of the other defendants participated in the theft or agreed to help steal the DNC's materials. Therefore, the DNC has not pleaded the existence of a conspiracy to hack the DNC's computers. The DNC has alleged, at most, that WikiLeaks received the results of the hacking and published those materials and that various of the other defendants welcomed those disclosures. That is not a conspiracy to commit trespass to chattels.

Accordingly, the DNC has failed to state a claim for conspiracy to commit trespass to chattels under Virginia common law against all of the defendants. The DNC's claims for conspiracy to commit trespass to chattels is **dismissed.**

XI.

The DNC asserts violation of the Virginia Computer Crimes Act against all of the defendants.

"The elements of a violation of the [Virginia Computer Crimes Act] are that the defendant (1) uses a computer or computer network; (2) without authority; and (3) either obtains property or services by false pretenses, embezzles or commits

larceny, or converts the property of another." Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 934 (E.D. Va. 2010) (citing Va. Code Ann. § 18.2-152.3).

The defendants, other than the Russian Federation, argue that they did not participate in the hacks on the DNC's computer systems and that, therefore, they cannot be liable under the Virginia Computer Crimes Act. The DNC argues that these defendants are liable for aiding and abetting the Russian Federation in hacking the DNC computer systems. Several of the defendants argue that the Virginia Computer Crimes Act does not provide for aiding and abetting liability and that Virginia courts do not allow claims for aiding and abetting statutory offenses unless the statute specifically allows it.

It is unnecessary to determine whether Virginia allows aiding and abetting liability for the Virginia Computer Crimes Act because, as explained above, the DNC has failed to allege facts showing that any defendant aided or abetted the hack into the DNC computer systems by the Russian Federation. Accordingly, the DNC's claims against all defendants (other than the Russian Federation) under the Virginia Computer Crimes act are **dismissed.** As explained above, the Court lacks subject matter jurisdiction under the FSIA over all claims asserted in this case against the Russian Federation.

XII.

The Campaign has also moved for sanctions against the DNC and the DNC's counsel under Federal Rule of Civil Procedure 11.

Rule 11 of the Federal Rules of Civil Procedure provides, in pertinent part, that, by presenting a "pleading, written motion, or other paper" to the Court, an attorney "certifies that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances":

> (1) it is not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation;
>
> (2) the claims, defenses, and other legal contentions are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law;
>
> (3) the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery . . . .

Fed. R. Civ. P. 11(b). "If . . . the [C]ourt determines that Rule 11(b) has been violated, the [C]ourt may impose an appropriate sanction . . . ." Fed. R. Civ. P. 11(c) (emphasis added). "[S]anctions under Rule 11 are discretionary, not mandatory." Ipcon Collections LLC v. Costco Wholesale Corp., 698 F.3d 58, 63 (2d Cir. 2012). The Court of Appeals for the

Second Circuit has made clear that Rule 11 sanctions should be granted with caution, applied only when "a particular allegation is utterly lacking in support." In re Highgate Equities, Ltd., 279 F.3d 148, 154 (2d Cir. 2002) (quoting O'Brien v. Alexander, 101 F.3d 1479, 1489 (S.D.N.Y. 1996)); see also Kiobel v. Millson, 592 F.3d 78, 81 (2d Cir. 2010); Storey v. Cello Holdings, L.L.C., 347 F.3d 370, 387 (2d Cir. 2003) (Sotomayor, J.) ("When reviewing Rule 11 sanctions, however, we nevertheless need to ensure that any [sanctions] decision is made with restraint." (quotation marks and citation omitted, alteration in original)). When deciding whether to grant Rule 11 sanctions, the Court applies an objective standard of reasonableness, W.K. Webster & Co. v. Am. President Lines, Ltd., 32 F.3d 665, 670 (2d Cir. 1994), and looks to, among other factors, whether the party acted in bad faith; whether that party relied on a direct falsehood; and whether the claim was "utterly lacking in support." New V & J Produce Corp. v. NYCCaterers Inc., No. 13cv4861, 2014 WL 5026157, at *7 (S.D.N.Y. Sept. 29, 2014). All doubts must be resolved in favor of the signer of the pleading. Rodick v. City of Schenectady, 1 F.3d 1341, 1350 (2d Cir. 1993).

The Campaign asserts that the DNC violated its Rule 11 obligations by maintaining this lawsuit after Special Counsel Robert Mueller III's Report was released. The Campaign asserts that the Special Counsel's "investigation definitively refuted

the notion that the Campaign conspired or in any way coordinated with Russia," (Campaign Rule 11 Mem. at 1), and argues that the DNC's claims were rendered frivolous by the Report.

The DNC responds that the Mueller Report simply found insufficient evidence at this time to support further criminal charges concerning the Russian Federation's hacking of the DNC's computers. But, the DNC argues, the standard for pursuing criminal charges is higher than the standard of proof required in a civil case, and the DNC should be permitted to pursue discovery to establish its claims.

The Second Amended Complaint was not "so objectively unreasonable as to warrant the imposition of sanctions," even though the Court has concluded that all of the claims must be dismissed for the reasons explained above. Gameologist Grp., LLC v. Sci. Games Int'l, Inc., No. 09cv6261, 2012 WL 1446922, at *4 (S.D.N.Y. Apr. 26, 2012). Nor was it so objectively unreasonable for the DNC to pursue its lawsuit after the Mueller Report was issued that sanctions should be imposed.

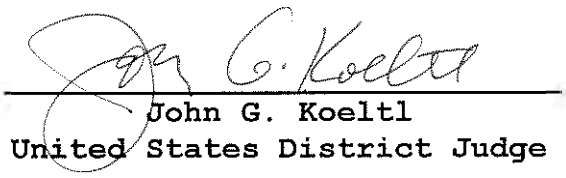
Courts should be cautious in granting Rule 11 sanctions, and the Court here exercises its discretion to decline to award sanctions. See Bowman Imp./Exp., Ltd. v. F.J. Elsner & Co. N. Am., No. 02cv3436, 2003 WL 21543522, at *2 (S.D.N.Y. July 9, 2003). The Campaign's motion for sanctions is **denied**.

CONCLUSION

The Court has considered all of the arguments raised by the parties. To the extent not specifically addressed, the arguments are either moot or without merit. For the reasons explained above, the DNC's Second Amended Complaint is **dismissed with prejudice** and the Campaign's motion for sanctions under Rule 11 is **denied.**[34] The Clerk is directed to enter judgment dismissing the Second Amended Complaint with prejudice. The Clerk is also directed to close this case and to close all pending motions.

SO ORDERED.

Dated: New York, New York
July 30, 2019



John G. Koeltl
United States District Judge

[34] At the hearing on September 13, 2018, the Court allowed the DNC the opportunity to amend the complaint and noted that the Court "assume[s] that the plaintiffs will give . . . their best complaint; that they're going to [say] everything that they possibly can . . . in support of that complaint so that if I were to eventually grant the motion to dismiss after that process, the plaintiffs would not be coming to me and saying, I have something else that we really wanted to say and we didn't say." (Tr. at 6, Dkt. No. 184.) The DNC then filed an amended complaint and several of the defendants moved to dismiss. (Dkt. Nos. 182, 194-96, 200, 203, 205-06, 211.) After the defendants moved to dismiss, the DNC filed a Second Amended Complaint -- its third complaint in this case. (Dkt. No. 217.) Yet, in footnote 41, at page 136 of its brief in opposition to the present motions, the DNC states that "any claims that the Court dismisses should not be dismissed with prejudice." The DNC has now had three chances to plead a viable complaint and it is not clear how the DNC could plead around the fundamental defects in the current complaint. If the DNC seeks to file a fourth complaint in this action, it can move for reconsideration and/or move to file another amended complaint and attach a copy of its proposed complaint and explain why that complaint would not be futile. But, there is no basis at this time based on the papers submitted to stay the judgment dismissing the Second Amended Complaint with prejudice, nor is there any reason to believe that the fundamental defects in the Second Amended Complaint can be cured.