GIBSON DUNN

June 19, 2019

THE EU INTRODUCES A NEW SANCTIONS FRAMEWORK IN RESPONSE TO CYBER-ATTACK THREATS

To Our Clients and Friends:

In a previous client alert, we highlighted a recent U.S. sanctions regime aimed at deterring threats of election interference[1], which further expanded the U.S. menu of cyber-related sanctions.[2] Across the Atlantic, as a step forward that demonstrates its voiced determination to enhance the EU's cyber defense capabilities[3], on May 17, 2019, the EU established a sanctions framework for targeted restrictive measures to deter and respond to cyber-attacks that constitute an external threat to the EU or its Member States.[4] The new framework is expounded in two documents, Council Decision (CFSP) 2019/797 and Council Regulation 2019/796.

The newly-introduced framework is significant for two reasons. First, the framework enables the EU to implement unilateral cyber sanctions, a move that expands the EU's sanctions toolkit beyond traditional areas of sanctions, such as sanctions imposed due to terrorism and international relations-based grounds.[5] Second, it represents a major, concrete measure that arose out of the EU's continued interest in developing an open and secured cyberspace and amid concerns for malicious use of information and communications technologies by both State and non-State actors. From the alleged plot by Russia to hack the Organization for the Prevention of Chemical Weapons in the Hague in April last year[6] to the cyber-attack on the German Parliament early this year[7], European leaders have been very concerned about future cyber-attacks on EU Member States. In particular, in light of the European Parliament election that took place on May 23-26, 2019, the framework equips the EU with a potent economic instrument to punish cyber-attacks more ably and directly on a unified front.[8]

Modality for Establishing the List of Sanctioned Parties

Under the new framework, persons, entities and bodies subject to sanctions will be listed in the Annex to the Council Decision (CFSP) 2019/797 ("Annex I"). With a view to ensure greater consistency in the listing of sanctioned parties, the European Council has the sole authority to establish and amend Annex I as needed, and is to review Annex I "at regular intervals and at least every 12 months."[9] The Council will review its decision in light of observations or substantial new evidence presented to it.

External Threats with a "Significant Effect"

The framework applies to "*cyber-attacks with significant effect, including attempted cyber-attacks with a potentially significant effect, which constitutes an external threat to the Union or its Member States*."[10] To be external, it suffices, among other ways, that the attack originates from outside the Union, uses infrastructure outside the Union, or is with the support, at the direction of or under the control of a person outside the Union.[11] The kinds of conduct considered as cyber-attacks include

unauthorized access to and interference with IT systems, as well as data interference and interception. The Council's approach to assessing the "*significant effect*" is by and large result-oriented, focusing, inter alia, pursuant to Article 3 of the Council Regulation, on "*(a) the scope, scale, impact or severity of disruption caused . . . (d) the amount of economic loss caused . . . (e) the economic benefit gained by the perpetrator* [*or*]*. . . (f) the amount or nature of data stolen or the scale of data breaches. . . .*"[12]

Expansive Reach of the Framework

Under the framework, sanctioned persons and entities are those who are responsible for the cyber-attack, and those who attempted, or provided "*financial, technical or material support*" to, or otherwise involved in the cyber-attack (e.g. directing, encouraging, planning, and facilitating the attack).[13]

It is also noteworthy that although the framework primarily targets attacks against Member States and the Union itself, sanctions measures under the framework can also be applied to cyber-attacks with a significant effect against "*third States or international organisations*," if sanctions measures are deemed "*necessary to achieve common foreign and security policy (CFSP) objectives.*"[14] As an initiative to deter cyber-attacks in general, the subjects of cyber-attacks covered under this framework are also expansive, ranging from critical infrastructure to the storage of classified information, as well as essential services necessary for the maintenance and operation of essential social and economic activities, and government functions, including elections.[15]

Sanctions Measures under the Framework

The primary restrictive measures under the framework are asset freeze and travel ban. Generally, all funds and economic resources "*belonging to, owned, held or controlled by*" the sanctioned person or entity will be frozen.[16] Furthermore, "*no funds or economic resources shall be made available directly or indirectly to or for the benefit of*" the sanctioned party.[17]

In broad terms, these EU financial sanctions are similar to a sanctions attendant to designation on the U.S. Specially Designated Nationals And Blocked Persons List.

Comparison with the U.S. Sanctions Regime for Cyber Attacks

In the U.S., besides the country-specific programs, the major source of authority for cyber-related sanctions is Executive Order 13694, titled "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" ("E.O. 13694") signed into effect by President Barack Obama on April 1, 2015.[18] The recently promulgated Executive Order 13848 on "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election" ("E.O. 13848") by President Donald Trump adds a further emphasis on threats of election interference via cyber means.[19]

In comparison, the latecomer EU sanctions framework is by and large similar both in terms of the conduct it seeks to deter and parties potentially subject to sanctions. Like the U.S. sanctions program, the EU framework covers a wide range of significant interferences and expressly highlights interference with "public elections or the voting process" as one of the enumerated predicate cyber-

attacks.[20] Much like the U.S. program's focus on "significant" "malicious cyber-enabled activities," the focus of the EU framework on "willfully carried out" cyber-attacks "with significant effect" gives the European Council substantial flexibility and discretion in its determination of what arises to the level of a sanctionable conduct.[21] In terms of parties covered, both E.O. 13694 (and subsequent E.O. 13848) and the EU framework sanction persons and entities who are responsible for the attack as well as those who are agents, or complicit by providing material assistance, in the commission of the cyber-attack.

It is important to note that the EU framework expressly permits imposition of sanctions on parties whose conduct is against a "*third* [non-Member] *States or international organizations*", insofar the EU satisfies itself that the sanctions are necessary to achieve CFSP objectives, namely the EU's Union-level foreign policy objectives.[22] In comparison, in the U.S. E.O. 13694, the possibility of imposing sanctions for cyber-attacks against a third party seems to be alluded to by the language "threat to the . . . foreign policy . . . of the United States."[23] Given the recentness of the framework, it is unclear as to the extent to which the EU would exercise its right under this provision, and no other countries have yet commented on this. Nonetheless, it is encouraging that both regimes leave open the possibility of sanctions based on cyber-attacks targeting third states.

Conclusion & Implications

The new framework established by the European Council represents a significant effort by the EU to stiffen its response to cyber-attacks. The framework has broadened EU sanctions both in substance and in scope. To the extent that the EU framework is comparable to the current U.S. cyber-related sanctions program, the EU framework reflects greater synchronization between the EU and the U.S. on the sanctions front. For the time being, no name has been added to Annex I yet. However, as the list grows in the future, businesses should closely assess their existing business relationships with other companies and pay greater attention in their onboarding compliance due diligence efforts. On the other hand, as the decision to list and delist a sanctioned party is reserved for the European Council, there is likely to be greater transparency and legal predictability for compliance purposes.

---

[1] See our client alert dated Sep. 25, 2018 entitled *U.S. Authorizes Sanctions for Election Interference*, https://www.gibsondunn.com/us-authorizes-sanctions-for-election-interference/, for an analysis of E.O. 13848.

[2] *See* Judith Lee, Cybersecurity Sanctions: A Powerful New Tool, LAW 360 (Apr. 02, 2015), https://www.gibsondunn.com/wp-content/uploads/documents/publications/Lee-Cybersecurity-Sanctions-A-Powerful-New-Tool-Law360.pdf, for an analysis by our Washington D.C. partner Judith Lee on the Obama-era executive order that forms the bulk of the current U.S. cyber-related sanctions program.

[3] *See* Council Press Release 301/19, Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace (Apr. 12, 2019), https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/.

[4] Council Press Release 367/19, Cyber-attacks: Council is now able to impose sanctions (May 17, 2019), https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

[5] See Erica Moret and Patryk Pawlak, European Union Institute for Security Studies, Brief, *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?*, p. 2 (Jul. 12, 2017), https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime.

[6] Joe Barnes, *UK Plays Pivotal Role In EU's New Cyber-Attack Sections Regime – 'This Is Decisive Action'*, Express (May 17, 2019), https://www.express.co.uk/news/uk/1128512/UK-news-EU-cyber-attack-section-regime-European-Council-latest-update.

[7] Thorsten Severin, Andrea Shalal, *German Government under Cyber Attack, Shores Up Defenses*, Reuters (Mar. 1, 2018), https://www.reuters.com/article/us-germany-cyber/german-government-under-cyber-attack-shores-up-defenses-idUSKCN1GD4C8.

[8] *See* Natalia Drozdiak, *EU Agrees Powers to Sanction, Freeze Assets Over Cyber-Attacks*, Bloomberg (May 17, 2019), https://www.bloomberg.com/news/articles/2019-05-17/eu-agrees-powers-to-sanction-freeze-assets-over-cyber-attacks.

[9] Council Regulation 2019/796 of May 17, 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States, preamble, art. 13, O.J. L 129I , 17.5.2019, p. 1–12, http://data.europa.eu/eli/reg/2019/796/oj (hereinafter "Council Regulation 2019/796").

[10] Council Decision (CFSP) 2019/797 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States, art. 1(1), O.J. L 129I , 17.5.2019, p. 13–19, http://data.europa.eu/eli/dec/2019/797/oj (hereinafter "Council Decision 2019/797").

[11] *Id.* art. 1(2).

[12] *Id.* art. 3. The same language is also reflected in Council Regulation 2019/796, art. 2.

[13] Council Decision 2019/797, *supra* note 10, art. 4.

[14] Council Regulation 2019/796, *supra* note 9, art. 1(6).

[15] Council Decision 2019/797, *supra* note 10, art. 1(4).

[16] *Id.* art. 5(1).

[17] *Id.* art. 5(2).

[18] See *supra* note 2 for an analysis of the Executive Order. *See also* Exec. Order No. 13694, 80 Fed. Reg. 18,077 (Apr. 2, 2015), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf, subsequently amended by Executive Order 13757 of December 28, 2016.

[19] *See supra* note 1. *See also* Exec. Order No. 13848, 83 Fed. Reg. 46,843 (Sep. 12, 2018), https://www.federalregister.gov/documents/2018/09/14/2018-20203/imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election.

[20] Council Decision 2019/797, *supra* note 10, art. 1(4)(c).

[21] *See* Judith Lee, *supra* note 2.

[22] CFSP objectives, as the Council Decision notes, can be found in relevant provisions of Article 21 of the Treaty on European Union. A relevant excerpt of article 21 of the Treaty on European Union:

> 2. The Union shall define and pursue common policies and actions, and shall work for a high degree of cooperation in all fields of international relations, in order to:
>
> (a) safeguard its values, fundamental interests, security, independence and integrity;
>
> (b) consolidate and support democracy, the rule of law, human rights and the principles of international law;
>
> (c) preserve peace, prevent conflicts and strengthen international security, in accordance with the purposes and principles of the United Nations Charter, with the principles of the Helsinki Final Act and with the aims of the Charter of Paris, including those relating to external borders;
>
> (d) foster the sustainable economic, social and environmental development of developing countries, with the primary aim of eradicating poverty;
>
> (e) encourage the integration of all countries into the world economy, including through the progressive abolition of restrictions on international trade;
>
> (f) help develop international measures to preserve and improve the quality of the environment and the sustainable management of global natural resources, in order to ensure sustainable development;
>
> (g) assist populations, countries and regions confronting natural or man-made disasters; and
>
> (h) promote an international system based on stronger multilateral cooperation and good global governance.

Consolidated Version Of The Treaty On European Union, art. 21, O.J. C 326, 26.10.2012, p. 13–390, available online at http://data.europa.eu/eli/treaty/teu_2012/oj.

[23] *Compare* Exec. Order No. 13694, *supra* note 18, sec. 1(a)(ii)(A), *with* Council Decision 2019/797, *supra* note 10, art. 1(6).

The following Gibson Dunn lawyers assisted in preparing this client update: Judith Alison Lee, Adam Smith, Patrick Doris, Michael Walther, Nicolas Autet and Richard Roeder.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding the above developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following leaders and members of the firm's International Trade or Privacy, Cybersecurity and Consumer Protection practice groups:

United States:
Judith Alison Lee - Co-Chair, International Trade Practice, Washington, D.C. (+1 202-887-3591, jalee@gibsondunn.com)
Ronald Kirk - Co-Chair, International Trade Practice, Dallas (+1 214-698-3295, rkirk@gibsondunn.com)
Alexander H. Southwell - Co-Chair, Privacy, Cybersecurity & Consumer Protection Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Jose W. Fernandez - New York (+1 212-351-2376, jfernandez@gibsondunn.com)
Marcellus A. McRae - Los Angeles (+1 213-229-7675, mmcrae@gibsondunn.com)
Adam M. Smith - Washington, D.C. (+1 202-887-3547, asmith@gibsondunn.com)
Christopher T. Timura - Washington, D.C. (+1 202-887-3690, ctimura@gibsondunn.com)
Ben K. Belair - Washington, D.C. (+1 202-887-3743, bbelair@gibsondunn.com)
Courtney M. Brown - Washington, D.C. (+1 202-955-8685, cmbrown@gibsondunn.com)
Laura R. Cole - Washington, D.C. (+1 202-887-3787, lcole@gibsondunn.com)
Stephanie L. Connor - Washington, D.C. (+1 202-955-8586, sconnor@gibsondunn.com)
Henry C. Phillips - Washington, D.C. (+1 202-955-8535, hphillips@gibsondunn.com)
R.L. Pratt - Washington, D.C. (+1 202-887-3785, rpratt@gibsondunn.com)
Audi K. Syarief - Washington, D.C. (+1 202-955-8266, asyarief@gibsondunn.com)
Scott R. Toussaint - Washington, D.C. (+1 202-887-3588, stoussaint@gibsondunn.com)

Europe:
Ahmed Baladi - Co-Chair, Privacy, Cybersecurity & Consumer Protection Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
Peter Alexiadis - Brussels (+32 2 554 72 00, palexiadis@gibsondunn.com)
Nicolas Autet - Paris (+33 1 56 43 13 00, nautet@gibsondunn.com)
Attila Borsos - Brussels (+32 2 554 72 10, aborsos@gibsondunn.com)
Patrick Doris - London (+44 (0)207 071 4276, pdoris@gibsondunn.com)
Sacha Harber-Kelly - London (+44 20 7071 4205, sharber-kelly@gibsondunn.com)

Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Steve Melrose - London (+44 (0)20 7071 4219, smelrose@gibsondunn.com)
Benno Schwarz - Munich (+49 89 189 33 110, bschwarz@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Richard W. Roeder - Munich (+49 89 189 33-160, rroeder@gibsondunn.com)