POLICY ALERT // MAY 30, 2019

New Cyber Sanctions Align European Union with United States

The EU Council on May 19, 2019, issued restrictive measures to deter and respond to cyber-attacks threatening the EU, its members, third countries, or international organizations. The measures provide the authority to block the assets of individuals and entities involved in cyber-attacks and enable enhanced coordination with the United States, which first authorized sanctions targeting similar activity on April 1, 2015.[1] The EU's new cyber measures mark the continued expansion of its global, conduct-based sanctions programs.

- The EU Cyber Diplomacy Toolbox, which was announced in June 2017, included sanctions among the tools that the EU could deploy to prevent and respond to malicious cyber activities, and the EU took nearly two years to deploy the sanctions authority.[2]
- The threat of malicious Russian cyber activity, along with continued threats and cyber activity from China[3] and North Korea,[4] probably drove the adoption of the authority, judging from press reporting on concerns about Russian interference in upcoming elections[5] and on other Russian cyber activity in the EU.[6]
- In October 2018, the United Kingdom, the Netherlands, the Baltic States, Finland, Denmark, and Romania circulated a paper arguing that cyber sanctions were "a pressing priority,"[7] but the adoption of this cyber sanctions authority failed to gain a consensus then.[8]

Overview of the Authorities Provided in the EU Restrictive Measures

The EU's new sanctions authority defines cyber-attack broadly, making it a robust platform for targeting malicious cyber actors aggressively. The EU did not impose any sanctions on any individuals or entities when it adopted the new authority, however, and the EU has struggled to implement its other targeted sanctions amid legal challenges.

- Cyber-attack is defined as "any action involving access to information systems, interference in information systems, data interference, or data interception."[9]
- The authority is focused on cyber-attacks that threaten the EU or its member states and also allows for the targeting of actors who conduct cyber-attacks with "significant effect" against third countries, international organizations, or

businesses in critical infrastructure sectors.[10]

- The EU has struggled to implement existing targeted sanctions authorities amid legal challenges. Intelligence that supports designations is often classified and the EU has been hesitant to declassify much of this evidence. As a result, lawsuits at the European Court of Justice have proven successful for designated persons who have challenged due to lack of public evidence.[11]

New EU Authority Provides Sound Basis for Transatlantic Cooperation

The new EU measures and the cyber sanctions adopted by the United States in 2015[12] and 2016[13] seek to target similar malicious cyber activity, though the EU authority is slightly narrower than the U.S. authority.

- The U.S.[14] and EU[15] cyber-related sanctions programs are generally aligned on the type of attack that would be in-scope to trigger a targeted response. Both programs, for example, provide designation authorities in response to attacks on critical infrastructure and certain economic activities.
- The inclusion of authorities for restrictive measures in response to attacks on third countries or international organizations could allow for increased transatlantic coordination on targeting.[16]
- The EU authority appears to be drafted more narrowly than the U.S. authority. The U.S. program authorizes sanctions in response to cyber-attacks on U.S. political parties or businesses[17] and the U.S. has targeted malicious actors for attacks on the Democratic National Committee[18] and SONY Pictures.[19] In a divergence from the U.S. authority, the EU authority does not explicitly authorize sanctions in response to cyber-attacks on EU political parties or on EU businesses outside of the critical infrastructure sectors.[20]

Implications of EU Cyber Restrictive Measures for Financial Institutions

Financial institutions may have significant exposure to individuals and entities that are eventually targeted under the new EU authorities, because Russian oligarchs with substantial holdings in the European Union have been involved in Russian efforts to use cyber attacks against Western targets. The cyber sanctions may open the EU's targeting aperture with respect to Russia.

- The EU's targeting authorities with respect to Russian activity were previously linked only to Crimea, Ukraine, and Russia's use of chemical weapons. The EU may be willing to bear more significant costs for deterring or responding

to Russian malign activity in the EU than it has been willing to bear for responding to Russian activity in Ukraine.

- Russian companies and businessmen are entangled in Russia's projection of power abroad, melding Russian business interests with covert action against Western targets. Yevgeny Prigozhin, who is accused of funding the troll farm used to interfere in the 2016 U.S. election, also runs a large catering business.[21]
- Oleg Deripaska, a Russian aluminum magnate, was designated by OFAC for his involvement with an array of Russian "malign activity around the globe."[22] Alexander Torshin, a former deputy governor of the Russian Central Bank, is accused of directing a scheme to infiltrate powerful American political organizations[23] and was also sanctioned by OFAC.[24]

The EU's creation of its cyber sanctions program marks the continued expansion of EU authorities that target individuals and entities based on their conduct.

- In 2018, the EU established a chemical weapons-related sanctions program and has imposed sanctions on nine individuals and one company under the authority.[25]
- Targeted human rights sanctions are also under current discussion.[26] The approach parallels the development of the Global Magnitsky program that the United States implemented in 2017.
- The EU has had targeted sanctions related to terrorism since December 2001, freezing the funds of Osama bin Laden and individuals and entities associated with him. These have expanded over time with the development of UN sanctions to include sanctions against Al-Qaida and ISIS.[27]

Endnotes

1 Federal Register, Executive Order 13757, December 28, 2016, Accessed online: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf

2 European Council of the European Union, Cyber-attacks: Council is now able to impose sanctions, May 5, 2019. Accessed online: https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

3 Bayer contains cyber attack it says bore Chinese hallmarks, Reuters, April 4, 2019. Accessed online: https://www.reuters.com/article/us-bayer-cyber/bayer-contains-cyber-attack-it-says-bore-chinese-hallmarks-idUSKCN1RG0NN

4 EU leaders to seek cyber sanctions, press Asia for action: draft statements, Reuters, October 17, 2018. Accessed online: https://www.reuters.com/article/us-eu-asia-cyber-sanctions/eu-leaders-to-seek-cyber-sanctions-press-asia-for-action-draft-statements-idUSKCN1MR1Z2

5 https://www.reuters.com/article/us-eu-cyber/days-before-elections-eu-approves-new-cyber-sanctions-regime-idUSKCN1SN1FQ

6 Politico, Europe hopes to fend off election hackers with 'cyber sanctions, February 11, 2019. Accessed online: https://www.politico.eu/article/europe-cyber-sanctions-hoped-to-fend-off-election-hackers/

7 Non-paper published by Politico, "EU Restrictive Measures: DK/EE/FI/LT/LV/NL/RO/UK non-paper," undated, https://g8fip-1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2018/10/POLITICO-non-paper-cyber-sanctions-regime-OCT-10.pdf.

8 Politico, "Russia dodges bullet of EU sanctions on cyber — for now," Oct. 18, 2018, https://www.politico.eu/article/russia-dodges-eu-sanction-on-cyber-for-now/.

9 European Council of the European Union, Cyber-attacks: Council is now able to impose sanctions, May 5, 2019. Accessed online: https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

10 European Council of the European Union, Cyber-attacks: Council is now able to impose sanctions, May 5, 2019. Accessed online: https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

11 Keatinge, Tom and Dall, Emil, Consensus for Action: Towards a More Effective EU Sanctions Policy, November 28, 2018. Accessed online: https://energypolicy.columbia.edu/research/report/consensus-action-towards-more-effective-eu-sanctions-policy

12 Federal Register, Executive Order 13757, December 28, 2016, Accessed online: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf

13 Federal Register, Executive Order 13694, April 1, 2015, Accessed online: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber2_eo.pdf

14 Department of the Treasury Office of Foreign Assets Control, Cyber-Related Sanctions Program, July 2, 2017. Accessed online: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf

15 European Council of the European Union, Cyber-attacks: Council is now able to impose sanctions, May 5, 2019. Accessed online: https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

16 European Council of the European Union, Cyber-attacks: Council is now able to impose sanctions, May 5, 2019. Accessed online: https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

17 Department of the Treasury Office of Foreign Assets Control, Cyber-Related Sanctions Program, July 2, 2017. Accessed online: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf

18 Department of Treasury, Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities, December 19, 2018. Accessed online: https://home.treasury.gov/news/press-releases/sm577

19 Department of Treasury, Treasury Targets North Korea for Multiple Cyber-Attacks, September 6, 2018. Accessed online: https://home.treasury.gov/news/press-releases/sm473

20 European Council of the European Union, Cyber-attacks: Council is now able to impose sanctions, May 5, 2019. Accessed online: https://www.consilium.europa.eu/en/press/

press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

21 Department of Treasury, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks, March 15, 2018. Accessed online: https://home.treasury.gov/news/press-releases/sm0312

22 U.S. Department of Treasury, Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity, April 6, 2018. Accessed online: https://home.treasury.gov/news/press-releases/sm0338

23 Washington Post, Maria Butina, Russian who conspired to infiltrate conservative U.S. political groups, sentenced to 18 months, April 26, 2019. Accessed online: https://www.washingtonpost.com/local/legal-issues/maria-butina-russian-who-conspired-to-infiltrate-the-nra-due-for-sentencing/2019/04/25/3ff24216-66ce-11e9-82ba-fcfeff232e8f_story.html?utm_term=.6538f5cb3f39

24 U.S. Department of Treasury, Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity, April 6, 2018. Accessed online: https://home.treasury.gov/news/press-releases/sm0338

25 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1542&from=EN

26 Politico, In accountability drive, Dutch seek targeted EU human rights sanctions, December 10, 2018. Accessed online: https://www.politico.eu/article/in-accountability-drive-dutch-seek-targeted-eu-human-rights-sanctions/

27 https://www.sanctionsmap.eu/api/v1/pdf/regime?id[]=6&id[]=5&lang=en