Hughes Hubbard & Reed

First Ever EU Economic Sanctions Adopted Following Cyber Attacks

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

September 8, 2020 - Faced with an ever-increasing number of cyber-attacks that undermine the integrity, security and competitiveness of European economic stakeholders, the European Union has in recent years reinforced its capacity to deter and respond to cyber-threats and malicious cyber-activities. On July 30, 2020, the European Union ("EU") used the regulatory arsenal introduced over the past few years for the first time to impose economic sanctions against six (6) individuals and three (3) entities for participating in (i) cyber-attacks against the Organization for the Prohibition of Chemical Weapons, (ii) the "WannaCry" and "NotPetya" attacks, and (iii) the "Cloud Hopper" operation.

The European Regulatory Arsenal

The first EU designations on July 30, 2020, are the culmination of a long process that began on June 19, 2017, with the EU Council's adoption of conclusions on establishing a framework for a joint diplomatic response to malicious cyber activities in the form of a "cyber diplomacy toolkit". The "toolbox" enables the EU to build on existing Common Foreign and Security Policy ("CFSP") tools to protect the integrity and security of the EU and its Member States.[1] Among the existing tools available within this new framework, the EU Council mentions "restrictive measures" or economic sanctions.

This was the backdrop against which the EU Council decided on May 17, 2019, in a CFSP decision and corresponding Regulation, to adopt a framework for imposing targeted restrictive measures against persons or entities (and any associated persons), responsible for cyber-attacks or attempted cyber-attacks, and providing financial, technical or material support for, or being otherwise involved in, such cyber-attacks[2]. These restrictive measures include, in particular, travel bans to and within the EU on sanctioned persons, and assets freeze measures, including a prohibition on making funds or economic resources available.

Use of the Regulatory Arsenal for the First Time: the Council Decision and Corresponding Implementing Regulation

This regulatory framework was used for the first time on July 30, 2020, in a Council Decision and corresponding Implementing Regulation that impose economic sanctions on six (6) individuals and three (3) entities for their role in (i) cyber-attacks against the Organization for the Prohibition of Chemical Weapons, (ii) the "WannaCry" and "NotPetya" attacks, and (iii) the "Cloud Hopper" operation:[3]

- 2 Chinese individuals (*Gao Qiang and Zhang Shilong*) for their participation in "Operation Cloud Hopper", which targeted the information systems of multinationals on six continents, including companies located in the European Union, by retrieving commercially sensitive information resulting in significant economic losses, and a Chinese organization (*Tianjin Huaying Haitai Science and Technology Development Co.*) for providing financial, technical or material support and facilitating "Operation Cloud Hopper";
- 4 Russian individuals (*Alexey Valeryevich Minin, Aleksei Sergeyvich Morenets, Evgenii Mikhaylovich Serebriakov,* and *Oleg Mikhaylovich Sotnikov*) for their participation in an attempted attack on the Organization for the Prohibition of Chemical Weapons in the Netherlands, and a Russian state agency *(Centre for Special Technologies (GTsST) of the Main State Directorate- General Staff of the Armed Forces of the Russian Federation (GU/GRU)*), for its participation in the "NotPetya" or "EternalPetya" attacks, which rendered data belonging to several large companies (such as Merck or Auchan), inaccessible by targeting computers with ransomware and blocking access to data, resulting amongst other consequences in significant economic losses, and a cyber-attack against a Ukrainian power grid, partially paralyzing it during the winter season;
- a North Korean company (*Chosun Expo*) for providing financial, technical or material support and facilitating a series of cyber-attacks with a significant impact, originating from outside the European Union and constituting an external threat to the EU or its Member States, and of cyber-attacks against third-party States, including the cyber-attacks publicly known as "WannaCry", which disrupted information systems in companies in the EU and around the world by targeting information systems with ransomware and blocking access to data.

The sanctions imposed include a ban on entering in and traveling within the EU, and an assets freeze prohibiting EU citizens and entities from making funds available to listed persons and entities.

While the EU restrictive measures are directly applicable (insofar as they are imposed under an EU Regulation), Member States are free to determine the offenses provided for in the event of a violation of the provisions contained in the Regulation (Article 15 of Council Regulation (EU) 2019/796 of May 17, 2019). [4] For example, the French Customs and Criminal Codes provide for criminal penalties in the event of a violation of EU restrictive measures. These sanctions are provided for in Article 459 1 bis and 1 ter of the French Customs Code.

A Swifter and More Aggressive American Response

Also faced with these cyber-threats, the United States seized on this issue at an early stage by adopting Executive Order 13694[5] in 2015, establishing a regulatory framework whereby persons responsible for or complicit in cyber-attacks from abroad against U.S. interests that pose a threat to U.S. national security, foreign policy, the economy and financial stability can be designated on the U.S. assets freeze list (OFAC's List of Specially Designated Nationals and Blocked Persons - SDN List). These sanctions impose a freeze on the assets held by such persons in the United States or that come within the possession or control of any U.S. person and prohibit any U.S. person from entering into or maintaining a business relationship with an SDN.

Following Russian interference in the U.S. presidential election, this Executive Order was amended by Executive Order 13757 of December 28, 2016, which formed the basis for imposing sanctions on Russian cybercriminals deemed to be responsible for the interference.

Similar sanctions have been imposed in recent years on the basis of Executive Order 13694:

- in September 2017, against one (1) Iranian company and three (3) individuals for causing disruption to the information systems of several American banks in 2011 and 2012, and four (4) other individuals for disrupting the information systems of several companies by working for Mersad, an Iranian security company affiliated with the Islamic Revolutionary Guards;[6]
- in March 2018, against three (3) Russian organizations and thirteen (13) individuals for participating in cybercriminal activities, including interference in the U.S. presidential election;[7]
- in March 2018, against one (1) organization and ten (10) Iranian individuals for stealing online data belonging to American universities and various media;[8]
- in February 2019, against one (1) Iranian company and six (6) individuals involved in cyber-attacks against members of the U.S. government and armed forces;[9]
- in December 2019, against seven (7) Russian organizations and seventeen (17) individuals involved in designing and spreading the "Dridex" virus;[10]
- in June 2020, against six (6) Nigerian cybercriminals for setting up an online fraud scheme enabling them to extort over six (6) million Dollars from U.S. citizens.[11]

Other sanctions were also imposed on the basis of Executive Order 13772 relating to the North Korean sanctions program:

- in September 2018, against one (1) North Korean programmer and one (1) North Korean company (Chosun Expo), for participating in the "WannaCry" attack and the attack against Sony in November 2014;
- in September 2019, against three (3) North Korean organizations (*Lazarus Group, Bluenoroff, Andariel*), benefiting from the support of North Korean intelligence services for targeting U.S. infrastructure.[12]

It is interesting to note that the perpetrators of these attacks were designated by the U.S. authorities two years before being designated by the European Union in July 2020 under the first EU sanctions for malicious cyber activity, which demonstrates very robust activism on the part of U.S. authorities.

Developments and Perspectives

Although new and welcome, these European economic sanctions measures are rather belated and therefore raise the issue of their effectiveness and proportionality in such a context. This is the first time that the European Union has taken a firm stance on malicious cyber activity and therefore seems to be taking the measure of the risk that many European companies face on an almost daily basis. However, the issues here are whether this decision lives up to the multi-dimensional and constantly evolving threat, whether the European Union has not been too slow in reacting to the risk, and finally, whether these sanctions will deter hackers whose presence is undetectable and whose financial assets are difficult to trace.

In any case, these sanctions constitute an exponentially increased use of this legal tool that has long been criticized and disparaged but saw a return to grace in the summer of 2014 when sectoral economic sanctions were imposed against Russian economic interests following the annexation of Crimean territory and Russian forces' involvement in the Donbass insurrection. The last 5 years have seen both Europe and the U.S. impose or strengthen economic sanctions regimes against Iran, Venezuela, Turkey (briefly), and now China as alternatives to military intervention against these same States. At the same time, activism by U.S. regulators, and in particular the Office of Foreign Assets Control, has reinforced the binding effect of these measures on Western companies operating in these countries.

The political situation in Belarus, tensions over the imposition of UN sanctions against Iran (arms embargo), Beijing's interference in Hong Kong, and accusations of espionage by the U.S. administration against Chinese social media are all subject matters presaging significant developments in terms of economic sanctions. The

coming months (and it is against this backdrop that other sanctions news briefs will be published each week), promise to be eventful in terms of developments and lessons to be learned.

_____

[1] https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/ Council of the European Union "Cyber-attacks: EU ready to respond with a range of measures, including sanctions"

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=FR Council Decision (CFSP) 2020/1127 of July 30, 2020, amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States and https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0796&from=FR Council Regulation (EU) 2019/796 of May 17, 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=FR (Council Decision (CFSP) 2020/1127 of July 30, 2020, amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States) and https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020R1125&from=FR (Council Implementing Regulation (EU) 2020/1125 of July 30, 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States)

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0796&from=FR Council Regulation (EU) 2019/796 of May 17, 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[5] https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[6] https://home.treasury.gov/news/press-releases/sm0158.

[7] https://home.treasury.gov/news/press-releases/sm0312.

[8] https://home.treasury.gov/news/press-releases/sm0332.

[9] https://home.treasury.gov/news/press-releases/sm611.

[10] https://home.treasury.gov/news/press-releases/sm845.

[11] https://www.state.gov/u-s-sanctions-nigerian-cyber-actors-for-targeting-u-s-businesses-and-individuals/.

[12] https://home.treasury.gov/news/press-releases/sm774.

Related People

Olivier Dorgans

Paul Charlot

Camille Mayet

Nicolas Burnichon

Related Areas of Focus

Sanctions, Export Controls & Anti-Money Laundering
Data Privacy & Cybersecurity

En français