Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How New EU Cyber Sanctions Compare To US Policy

By **Michelle Linderman, Maarten Stassen, Dj Wolff and Heidi Waem**
(July 30, 2019, 3:29 PM EDT)


Michelle Linderman


Maarten Stassen


Dj Wolff


Heidi Waem

On May 17, 2019, the Council of the European Union adopted new legislation in the form of Council Decision 2019/797[1] and Council Regulation (EU) 2019/796,[2] which allow the council to impose sanctions on people and entities responsible for cyberattacks that constitute a threat to the European Union and its member states.

Cybersecurity is one of the EU's biggest concerns. Network and information systems are crucial for the economy, and securing them is essential in this era of digitalization.

Over the last few years, there has been a significant increase in the number, scale and severity of cyberattacks. Against that background, the EU has promulgated various pieces of law including:

- Directive (EU) 2016/1148 of July 6, 2016 concerning measures for a high common level of security of network and information systems across the EU.[3] This directive set out measures to achieve a high level of security for so-called essential and digital services.

- Regulation (EU) 2019/881 of April 17, 2019, the European Union Agency for Network and Information Security and information and communications technology cybersecurity certification.[4] This regulation, which is also called the Cybersecurity Act, grants ENISA a permanent mandate to carry out various tasks in the field of cybersecurity and establishes a European cybersecurity certification framework.

Where these legislative acts are focused on securing network and information systems, the new EU legislation addresses cybersecurity from another angle by providing a sanctions regime to impose restrictive measures on people and entities responsible for cyberattacks.

What Is the Scope of the Sanctions Regime?

The council regulation applies to cyberattacks that have a significant effect,

including attempted cyberattacks with a potentially significant effect, that constitute an external threat to the EU or its member states.

To assess whether a cyberattack has a significant effect, the following factors will be taken into account:

- The scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical state functions, public order or public safety;
- The number of natural or legal people, entities or bodies affected;
- The number of member states concerned;
- The amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;
- The economic benefit gained by the perpetrator, for himself or for others;
- The amount or nature of data stolen or the scale of data breaches; or
- The nature of commercially sensitive data accessed.

A cyberattack will be considered an external threat when it:

- Originates, or is carried out, from outside the EU;
- Uses infrastructure outside the EU;
- Is carried out by any natural or legal person, entity or body established or operating outside the EU; or
- Is carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the EU.

How Is Cyberattack Defined?

Cyberattacks are defined as actions involving any of the following: (1) access to information systems, (2) information system interference, (3) data interference or (4) data interception, where such actions are unauthorized or are not permitted under the law of the EU or of the member state concerned.

Who Can Be Subject to Sanctions?

Sanctions can be imposed on:

- Natural people who are responsible for cyberattacks or attempted cyberattacks;
- Natural people who provide financial, technical or material support for or are otherwise involved in cyberattacks or attempted cyberattacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission; and

- Natural people associated with the people covered by points (1) and (2).

The council will establish and make available a list of people who fall within the scope of the sanctions regime and on whom sanctions should be imposed. The list is currently still empty.

What Sanctions Can Be Imposed?

The sanctions regime provides for a travel ban and an asset freeze on targeted individuals and entities listed by the council. In addition, EU people and entities are prohibited to make funds or economic resources available, either directly or indirectly, to those entities and people included in the cyber sanctions list.

How Does the EU Cyber Sanction Regime Compare With U.S. Cyber Sanctions?

The United States already has a similar sanctions regime in place. On April 1, 2015, President Barack Obama issued Executive Order 13694, which was later amended by Executive Order 13757 to expand the scope of cyber-enabled activities subject to sanctions.

The U.S. cyber sanctions regime provides broad designation criteria. First, the U.S. Office of Foreign Assets Control may designate people determined to be engaging in, directly or indirectly, "cyber-enabled" activities originating from, or directed by people located outside the United States, that are reasonably likely to result in, or have materially contributed to, a significant threat to U.S. national security, foreign policy, economic health or financial stability of the U.S. and that have the purpose or effect of:

- Harming or otherwise significantly compromising the provision of services by a computer or network of computers that support entities in a critical infrastructure sector;

- Significantly compromising the provision of services by an entity in a critical infrastructure sector;

- Causing a significant disruption to the availability of a computer or network of computers;

- Causing a significant misappropriation of funds, economic resources, trade secrets, personal identifiers or financial information for commercial or competitive advantage or financial gain; or

- Tampering with, altering or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.

Second, OFAC also has authority to designate people, subject to certain conditions, determined to be a commercial entity operating outside the United States and using trade secrets misappropriated through cyber-enabled means for commercial or competitive advantage. Finally, OFAC has authority to designate any person (1) assisting, sponsoring, financing or supporting any of the aforementioned activities, (2) owned or controlled by or acting on behalf of any person designated pursuant to the other authorities, or (3) that attempted to engage in the aforementioned activities.

To date, OFAC has designated 66 people — including 21 entities and 45 individuals — pursuant to these cyber-related authorities, including most prominently a number of people for alleged cyber-enabled intervention in the 2016 U.S. presidential election. Importantly, OFAC also has a number of related authorities that it can, and has, used historically to target malicious cyber-related activities, such as

designating a number of Russian people pursuant to the Countering America's Adversaries Through Sanctions Act for intervention in the 2016 election,[5] as well as sanctioning a number of North Korean officials pursuant to the North Korean sanctions program for the cyberattack on Sony Pictures Entertainment Inc.[6]

Impact of the Cyber Sanctions Regimes

The new EU cyber sanctions regime reflects the EU's desire to enhance its reaction to malicious cyberattacks in the wake of serious incidents that have occurred across member states in recent times. There are a number of similarities between the U.S. and EU regimes, and it will be interesting to see first, whether the EU begins to designate people pursuant to its new authority and second, if so, to what extent there will be any similarities in terms of the people targeted by the U.S. and the EU.

One important similarity is that this new EU cyber sanctions regime targets individuals rather than states. This constitutes a shift in the EU's Common Foreign and Security Policy. Generally, EU sanctions regimes are country sanctions regimes targeting states as a whole, e.g., Russia and Iran. However, recently, there has been a shift toward so-called horizontal sanctions regimes which are theme-based regimes. In 2018, the EU adopted a horizontal sanctions regime addressing the use and proliferation of chemical weapons. This is now followed by the cyber sanctions regime.

The use of horizontal sanctions regimes makes sense as country sanctions regimes typically also target specific entities and people within a certain country. They do not target everybody in a certain country. Nevertheless, by their nature, country-based sanctions regimes are perceived as targeting countries and their populations as a whole. The use of theme-based horizontal sanctions will not target entire nations but only specific entities and individuals. This may make it easier for the EU to respond to cyberattacks and blacklist wrongdoers, regardless of whether the attacks are carried out by state or nonstate actors, without naming and shaming the country in question and without creating a perception that the entire country has been targeted.

For compliance purposes, the new sanctions regimes will, however, simply represent another factor to be taken into account when carrying out due diligence on counterparties, customers and so forth. For those impacted by actual or attempted cyberattacks, the legislation may help with blocking assets and/or shutting down bad actors including those seeking to steal commercial or sensitive information for private gain.

It remains to be seen whether the new EU cyber sanctions regime will lead to fewer cyberattacks. It is too early to draw conclusions. It may help deter financially motivated cyber theft; however, we fear that the impact on the number of other types of cyberattacks may be limited as the actors who carry out such attacks are unlikely to see these measures as much of a deterrent.

Michelle Linderman, Maarten Stassen and Dj Wolff are partners and Heidi Waem is counsel at Crowell & Moring LLP.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0797&from=GA

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.ENG&toc=OJ:L:2019:129I:TOC

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[5] https://home.treasury.gov/news/press-releases/sm577

[6] https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx