INSS Insight No. 1364, August 24, 2020

For the First Time, EU Sanctions in Response to Cyberattacks: Enhanced Deterrence Efforts by Western Countries?

Vered Zlaikha

On July 30, 2020, the European Union decided to impose restrictive measures on nine individuals and entities from China, North Korea, and Russia for their responsibility or involvement in cyberattacks. The sanctions include a travel ban, asset freeze, and prohibition to make funds available to these individuals and entities. On the political level, it seems that Western countries have managed, despite other differences, to demonstrate a coordinated approach in this field and act in cooperation. From the perspective of international cyber policy, this step seems to be in line with previous measures taken by Western countries and by the European Union itself, as well as with the cyber deterrence strategy advanced in recent years by the United States. The European Union may be seeking to send a deterrent message against cyberattacks, in particular during the Covid-19 crisis.

On July 30, 2020, the European Council announced the imposition of sanctions ("restrictive measures") against six individuals and three entities from China, North Korea, and Russia, for their responsibility or involvement in cyberattacks or attempted cyberattacks. According to Josep Borrell, High Representative of the European Union for Foreign Affairs and Security Policy, this step was taken "in order to better prevent, discourage, deter and respond to such malicious behaviour in cyberspace." The new sanctions were imposed in accordance with the cyber sanctions regime that was adopted by the European Union in May 2019 following the framework that has developed since 2017 for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox").

Pursuant to the sanctions regime, targeted restrictive measures can be taken against cyberattacks of significant effect that pose an external threat to the EU or individual member states (or attempted cyberattacks with a potentially significant effect). Similarly, restrictive measures can also be taken in response to cyberattacks of significant effect against third states or international organizations, if deemed necessary to achieve EU common foreign and security policy objectives set out in the Treaty on European Union.

The sanctions taken include a travel ban, asset freeze, and prohibition to make funds available to these individuals and entities on the sanctions list. The targets of the sanctions are alleged to have been involved in various types of cyberattacks, most of

which took place and attracted media and international attention in 2017 and 2018, as follows:

a. A North Korean company for its alleged involvement in a series of cyberattacks, including "Wannacry," which "disrupted information systems around the world by targeting information systems with ransomware and blocking access to data. It affected information systems of companies in the Union, including information systems relating to services necessary for the maintenance of essential services and economic activities within Member States."
b. Two Chinese individuals and a technological development company from China that employed them, for their alleged involvement in an attack on information systems of multinational companies in six continents, including companies located in the European Union, gaining unauthorized access to commercially sensitive data, resulting in significant economic loss ("Operation Cloud Hopper," APT10).
c. Four members of the Russian military intelligence officers for their alleged involvement in an attempt to gain unauthorized access to the Wi-Fi network of the OPCW (Organisation for the Prohibition of Chemical Weapons) in The Hague in April 2018. According to the sanctions list, if successful, the attack would have compromised the security of the network and the OPCW's ongoing investigatory work. In addition, sanctions were imposed on the Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), for its involvement in cyberattacks according to the sanctions list, including the "NotPetya" cyberattack in June 2017, which "rendered data inaccessible in a number of companies worldwide, including in the Union, wider Europe and worldwide, by targeting computers with ransomware and blocking access to data, resulting amongst others in significant economic loss," and for its involvement, according to the list of sanctions, in cyberattacks directed at a Ukrainian power grid in 2015 and 2016.

Most of the main incidents on the sanctions list had already resulted in public denouncements on the part of the Western countries. These included condemnations and/or indictments in some cases, with responsibility assigned to individuals or entities, or even attributed to states. The EU itself has condemned most of these incidents in public announcements, and the new sanctions in this regard appear to be a complementary step.

Soon after the sanctions were announced, the United States, the UK, Australia, and Canada expressed their support and welcomed the European Union's step. The UK announced that the sanctions were in force in the UK as well, and mentioned the coherent

autonomous UK Cyber Sanctions regime, created following Brexit, in order to implement this regime. For their part, Russia and China reportedly criticized the EU decision to impose sanctions instead of conducting a dialogue. Inter alia, the Russian Foreign Ministry stated that this was a "unilateral" measure that is "absolutely illegal in the context of international law," and that "in diplomacy, everything is reciprocal." The Chinese mission to the EU also expressed reservations about the step, and "urged the international community to communicate based on mutual respect and mutual benefit to safeguard cyber security."

An initial examination of the EU step leads to some interesting observations. First, from a broad international dynamics perspective, the imposition of sanctions by the EU at the current time, supported by the US, the UK, and other Western countries, can be seen as reflecting a coordinated approach in international cyber policy from Western countries, despite differences on other matters (including Brexit arrangements, or Covid-19-related issues).

Second, these sanctions seem to be a step that goes along with the US deterrence strategy (which is a part of the National Cyber Strategy), issued by the White House in September 2018. According to this strategy, the United States will work with like-minded states "to ensure adversaries understand the consequences of their malicious cyber behavior" through a variety of deterrent response measures, including "intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors." The EU sanctions seem to go hand in hand with this approach, particularly taking into account that the step was preceded by condemnations and denunciations by Western countries in response to most of the incidents mentioned.

The sanctions should also be understood in the context of the broader picture of condemnations, denouncements, and imposition of responsibility during recent months in response to other cyber incidents, including: condemnation and public statements by international organizations and countries during the Covid-19 crisis in relation to cyber incidents against the healthcare sector (examples reported in the media include an attack on the computer system of a Czech hospital; an attempted attack on the World Health Organization; and commercial espionage against companies developing coronavirus vaccines); the submission of indictments in the US against two Chinese individuals for a cyber commercial espionage campaign of companies and entities in various states; and an arrest warrant issued in Germany against a Russian intelligence operative suspected of involvement in a cyberattack on the Bundestag (German parliament) in 2015, which caused leaks of sensitive correspondence.

Third, in any event, the decision to impose sanctions reflects an enhanced effort by the EU to denounce malicious cyber incidents. The sanctions are intended to send a sharp and clear message that the EU will not tolerate such activities, and that it is determined to protect itself and its member states. The imposition of sanctions at this time may reflect a strategic choice to act fiercely and to strengthen deterrence, perhaps in light of the cyberattacks against the healthcare sector during the Covid-19 crisis (and following the European Council declaration of April 2020 in that regard).

Fourth, the European Union's step reflects a cautious approach with regard to attribution of responsibility toward specific countries, apparently for political reasons. The EU did clarify that "targeted restrictive measures have a deterrent and dissuasive effect and should be distinguished from attribution of responsibility to a third state." The fact that statements and condemnations regarding the main cyber incidents mentioned in the sanctions list were already issued in the past by the EU probably made it easier for the EU to reach a consensus to impose concrete sanctions on those responsible. Moreover, it seems that the decision to impose sanctions regarding a group of different cyber incidents and on a variety of individuals and entities from different countries at the same time, rather than directing them at one entity, may have a softening effect. At the same time, this move can send a deterrent message of the EU willingness to impose sanctions against those involved in cyberattacks, irrespective of the source of the attack.

To sum up, the recent EU cyber sanctions are another step in shaping the cyber rules of the game and deterrence policy. They join the increasing condemnations and denunciations formulated lately by Western countries with regard to different cyber incidents (some of them launched during the pandemic). It remains to be seen how this deterrent effort will develop: what will the immediate effects of this step be like; will additional sanctions be adopted in the near future by the European Union, and for what cyber incidents; how effective would these efforts be in the long term; and would these European sanctions influence other issues on the international cyber agenda.

* Adv. Vered Zlaikha is an expert in cyber law and policy.