THE CYBER (SANCTIONS) (EU EXIT) REGULATIONS 2020

REPORT UNDER SECTION 2(4) OF THE SANCTIONS AND ANTI-MONEY LAUNDERING ACT 2018

Introduction

1. This is a report under section 2(4) of the Sanctions and Anti-Money Laundering Act 2018 ("**the Act**") in relation to the Cyber (Sanctions) (EU Exit) Regulations 2020. Section 2(4) requires a report to be laid before Parliament which explains why the appropriate Minister making regulations under section 1 considers that the purposes of the regulations meet one or more of the conditions in paragraphs (a) to (i) of section 1(2) of the Act;[i] why the Minister considers that there are good reasons to pursue that purpose; and why the Minister considers that the imposition of sanctions is a reasonable course of action for that purpose.

2. Sanctions will continue to contribute to the UK's efforts to defend the rules-based international order. The UK will continue to strive to be a global leader on sanctions, based on the smart, targeted use of sanctions, as part of wider political and diplomatic strategies. The UK will enhance its leadership role in developing robust evidence to support sanctions regimes and designations – for national and multilateral sanctions. At the international level, the UK will continue to seek multilateral cooperation on sanctions in response to shared threats, given that a collective approach to sanctions achieves the greatest impact.

3. There is an existing EU cyber sanctions regime, which was established in May 2019 to deter and respond to cyber-attacks and attempted cyber-attacks with a significant or potentially significant effect which constitute an external threat to the European Union or its Member States; it also covers similar attacks in respect of third countries or international organisations. It allows the EU to impose targeted sanctions on individuals and entities responsible for such cyber-attacks, those who provide financial, technical, or material support for them or who are involved in other ways, and those associated with them.

4. Bringing this existing EU sanctions framework into UK law following the Transition Period is consistent with UK policy on taking measures to address the threat. The Cyber (Sanctions) (EU Exit) Regulations 2020 **("the Regulations")** are intended to deliver similar policy effects as the existing EU sanctions regime.

Purposes and reasons for pursuing the purposes

5. The purpose of the sanctions regime, as set out in regulation 4 of the Regulations, is to further the prevention of relevant cyber activity.

6. 'Relevant cyber activity' is defined as:

   (a) accessing, or attempting to access, an information system,

   (b) carrying out, or attempting to carry out, information system interference, or

   (c) carrying out, or attempting to carry out, data interference,

except where—

(i) the owner or other right holder of the information system or part of it has consented to such action,

(ii) there is a lawful defence to such action, or

(iii) such action is otherwise permitted under the law of the United Kingdom;

if that activity:

(a) undermines, or is intended to undermine, the integrity, prosperity or security of the United Kingdom or a country other than the United Kingdom,

(b) directly or indirectly causes, or is intended to cause, economic loss to, or prejudice to the commercial interests of, those affected by the activity,

(c) undermines, or is intended to undermine, the independence or effective functioning of—

(i) an international organisation, or

(ii) a non-governmental organisation or forum whose mandate or purposes relate to the governance of international sport or the Internet, or

(d) otherwise affects a significant number of persons in an indiscriminate manner.

7. The Regulations confer a power on the Secretary of State to designate persons for the purposes of immigration or financial sanctions where the Secretary of State has reasonable grounds to suspect that a person is an 'involved person', and considers that their designation is appropriate, having regard to the purpose stated in regulation 4, and the likely significant effects of the designation on that person. In these Regulations an 'involved person' means a person who:

(i) is or has been involved in relevant cyber activity,

(ii) is owned or controlled directly or indirectly (within the meaning of regulation 7) by a person who is or has been so involved,

(iii) is acting on behalf of or at the direction of a person who is or has been so involved, or

(iv) is a member of, or associated with, a person who is or has been so involved.

8. Carrying out this purpose meets one or more of the conditions set out in section 1(2) of the Act. In particular, carrying out this purpose would fall within sub-paragraphs (b), (c), (d) and (i), in that it would be in the interests of UK national security; be in the interests of international peace and security; further foreign policy objectives of the UK government; and promote respect for democracy, the rule of law and good governance.

9. Pursuing this purpose will help address the ongoing and increased threat in cyber space. Cyber attacks know no international boundaries and have grown in terms of intensity, complexity and severity. Malign actors in cyberspace are active and able to execute successfully operations on countries affecting critical national infrastructure, democratic institutions, businesses and the media. These actors are demonstrating an increased risk appetite, be it for economic, strategic, regional or financial gain. Over the last few years there has been a rise in the scale and impact of operations, with co-ordinated campaigns as opposed to single incidents that potentially allowed wide-ranging access to thousands of victims in countries globally and causing significant financial and material damage.

Why sanctions are a reasonable course of action

10. The imposition of prohibitions and requirements of the kind imposed by these Regulationsis a reasonable course of action for the purpose of furthering the prevention of relevant cyber activity.

11. The UK believes sanctions can be an effective and reasonable foreign policy tool if they are one part of a broader foreign policy strategy for a country or thematic issue, and are appropriate to the purposes they are intending to achieve.

12. Sanctions are not punitive, but designed to bring about a change in policy or behaviour of targeted individuals, entities and, where applicable, their governments. They should be complementary to efforts to hold accountable the perpetrators of relevant cyber activities, including, where possible, criminal prosecution.

13. The objectives of the sanctions include to:

- **Change Behaviour** by imposing a meaningful consequence on those who carry out relevant cyber activity, **coercing** decision makers currently considering carrying out relevant cyber activity into concluding that it is too high cost. This will also **signal** at a political level that relevant cyber activity has consequences, thereby having a deterrent effect.

- **Constrain** those who would seek to commit relevant cyber activity by restricting their access to finances and ability to travel, preventing them from carrying out relevant cyber activity as they would wish.

14. There are two principal kinds of prohibition in the Regulations: those relating to financial sanctions, and those relating to immigration sanctions. These restrictions consist of an asset freeze (including a restriction on providing funds and economic resources) and a travel ban. These restrictions can only be imposed upon specified persons who meet the criteria set out in the Regulations. This is in order to ensure that the sanctions are clearly targeted at those who are or have been involved in this activity, those owned or controlled by those involved, or a member of a group that this involved, and therefore fulfil the stated purpose of the sanctions. The Regulations allow for exceptions to the travel ban and also provide for the financial sanctions to be subject to certain exceptions and a licensing framework. The exceptions and licensing provisions support the reasonableness of imposing these sanctions measures on designated persons, as they mitigate any possible negative or counter-productive impacts.

15. These sanctions are not an end in themselves. They are one element of a broader strategy to achieve the UK's international policy goals for cyber space. Other elements include work on strengthening the rules-based international system, increasing the cost of engaging in malign cyber activity, promoting the use of deterrence measures, the provision of assistance to other states to increase their ability to respond to cyber threats, building international alliances, engagement through the UN and other multilateral fora, and bilateral lobbying.

16. The UK will continue to coordinate with international partners to ensure effective international action against relevant cyber activity, and will support partners looking to implement their own cyber sanctions regime.

17. The Regulations also impose supplemental prohibitions and requirements, in particular those relating to the disclosure of confidential information, the reporting of information by relevant firms, and the holding of records. These kinds of prohibitions and requirements ensure that certain information is appropriately held by those involved with the operation of the sanctions regime, and that certain information is provided to authorities, and ensure that certain sensitive information is treated securely. These kinds of prohibitions and requirements enable the government to properly

operate and enforce the sanctions regime, and therefore their imposition is also considered a reasonable course of action for the purposes of the Regulations.

Conclusions

18. The purpose of these Regulations is to further the prevention of relevant cyber activity. For the reasons set out in this report, carrying out this purpose meets one or more of the conditions in section 1(2) of the Act. As set out in this report, there are good reasons for pursuing that purpose, and the imposition of the kinds of prohibitions and requirements imposed by these Regulations for that purpose is a reasonable course of action.

Lord Ahmad of Wimbledon

Minister of State for South Asia and the Commonwealth, Foreign and Commonwealth Office, on behalf of the Secretary of State for Foreign and Commonwealth Affairs

---

[i] Section 1(2) states:

"A purpose is within this subsection if the appropriate Minister making the regulations considers that carrying out that purpose would –

- *a) further the prevention of terrorism, in the United Kingdom or elsewhere,*
- *b) be in the interests of national security,*
- *c) be in the interests of international peace and security,*
- *d) further a foreign policy objective of the government of the United Kingdom,*
- *e) promote the resolution of armed conflicts of the protection of civilians in conflict zones,*
- *f) provide accountability for or be a deterrent to gross violations of human rights, or otherwise promote -*
  - *(i) compliance with international human rights law, or*
  - *(ii) respect for human rights,*
- *g) promote compliance with international humanitarian law,*
- *h) contribute to multilateral efforts to prevent the spread and use of weapons and materials of mass destruction, or*
- *i) promote respect for democracy, the rules of law and good governance."*