Foreign Secretary welcomes first EU sanctions against malicious cyber actors

Press release

Dominic Raab welcomes decisive action which raises the cost for hostile cyber activity.

The UK has welcomed today's announcement (Thursday 30 July) that the EU has imposed sanctions against nine individuals and organisations from North Korea, China and Russia, in the first set of sanctions under the EU's cyber sanctions regime. The UK was at the forefront of efforts to establish the EU Cyber Sanctions regime and will continue to implement this regime at the end of the Transition Period, through our own autonomous UK Cyber Sanctions regime.

These sanctions – which are now in force in the UK – send a strong signal that malicious cyber activity against our European partners and allies has consequences. The cyber sanctions will impose meaningful costs for the reckless behaviour of state and non-state actors through asset freezes and travel bans within the EU, including the UK.

The UK is committed to working with our international partners to agree responsible behaviours and promote international security and stability in cyberspace. And we've recently laid the statutory instrument for our own UK autonomous cyber sanctions regime, which will allow us to impose travel bans and asset freezes on individuals and organisations.

The UK has previously identified the organisations sanctioned today for their roles in state sponsored cyber attacks which targeted democratic institutions, critical national infrastructure, media outlets and international organisations. These include:

- North Korean organisation Chosun Expo (linked to the Lazarus Group), for

facilitating and supporting the ‘Wannacry’ attack. This ransomware incident impacted 300,000 computers in 150 countries, including 48 NHS trusts.

- Chinese organisation Tianjin Huaying Haitai Science and Technology Development Co. Ltd, for facilitating and supporting ‘Cloud Hopper’ – a sustained cyber campaign focused on large-scale service providers, seeking to gain access to commercial secrets.

- Unit 74455 of the GRU, the Russian military intelligence service, for the ‘NotPetya’ cyber attack in June 2017 and 4 GRU officers who attempted a cyber attack against the Organisation for the Prohibition of Chemical Weapons (OPCW) in 2018.

The Foreign Secretary, Dominic Raab, said:

> Today’s actions will raise the cost on malicious cyber activity by state and non-state actors and will help counter future hostile activity in cyberspace. The UK was at the forefront of efforts to establish the EU Cyber Sanctions regime and we will continue to implement this regime after the end of the Transition Period.

Notes to Editors

- On 16 July, the UK, US and Canada called for an end to irresponsible cyber attacks by the Russian Intelligence Services, who have been collecting information on vaccine development and research into the COVID-19 virus.

- On 22 July, the UK made a statement following the US Department of Justice’s announcement of charges relating to cyber attacks against institutions in 11 countries, including the UK.

Further information

Published 30 July 2020