Attorney General to set out the UK's position on cybersecurity and international law

News story

The Attorney General will tonight set out more detail on the UK's position on applying international law to cyberspace.

The Attorney General the Rt Hon Suella Braverman QC MP will tonight set out more detail on the UK's position on applying international law to cyberspace in a speech at Chatham House. The Attorney will say that the united international response to the illegal invasion of Ukraine has illustrated the need to have a clear framework for cybersecurity that makes clear when State action is unlawful.

The Attorney will stress that cyberspace is not lawless. The Attorney will argue that a cyber-attack should be treated the same as physical attack and that states must lead the debate on what they see as the 'rules of the road'.

The Attorney will set out the UK's view on what constitutes unlawful cyber behaviour. This will enable the UK and others to better 'call out' unlawful behaviour and give clarity on what action can lawfully be taken in response to a cyber-attack.

The Attorney will say that the threat from cyber-attacks is real, and disruptive state cyber behaviour has caused chaos across the world. Recently, before its illegal invasion of Ukraine, Russia targeted destructive malware against hundreds of systems across Ukraine affecting its IT, energy, and financial sectors.

The Attorney General will say:

> The United Kingdom's aim is to ensure that future frontiers evolve in a way that reflects our democratic values and interests and those of our allies.

The law needs to be clear and well understood if it is to be part of a framework for governing international relations and to rein in irresponsible cyber behaviour. Setting out more detail on what constitutes unlawful activity by States will bring greater clarity about when certain types of robust measures are justified in response.

Note to Editors

1. The UK is a leading voice on cyber at an international level. Online safety and cyber security has featured in discussions among counterparts in the 'Quintet' of Attorneys General from the UK, Australia, Canada, New Zealand and the United States.
2. Examples of cyber-attacks where the UK has 'named and shamed' state actors are:
    1. On 10 May 2022 the UK (along with EU, US and other allies) announced that Russia was responsible for a series of cyber-attacks since the renewed invasion of Ukraine.
    2. In July 2021 the UK assessed that Chinese state-backed actors were responsible for gaining access to computer networks around the world via Microsoft Exchange servers. The attacks took place in early 2021 and open-source reporting indicates that at least 30,000 organisations were compromised in the US alone, with many more affected worldwide.
    3. The UK and US revealed in April 2021 that Russia's Foreign Intelligence Service (SVR) was behind a series of cyber intrusions, including the SolarWinds compromise. These incidents were part of a wider pattern of cyber intrusions by the SVR who have previously attempted to gain access to governments across Europe and NATO members.
    4. In October 2020 the UK exposed malicious cyber activity from Russia's GRU military intelligence service against organisations involved in the 2020 Olympic and Paralympic Games before they were postponed.
    5. The 2017 NotPetya cyber-attack, which masqueraded as ransomware, affected Ukraine's financial, energy and government institutions. Statements of attribution and support were issued by the UK along with the US, New Zealand, Canada, Australia, Sweden, Estonia, the Netherlands and Denmark amongst others.
    6. In December 2017 the UK attributed the Wannacry ransomware incident (which included NHS email systems among its targets) to North Korean actors. UK attribution was done in parallel to allies including the US, Australia, Canada, New Zealand, Denmark and Japan.

Published 19 May 2022