KINGDOM OF BELGIUM
Federal Public Service
Foreign Affairs,
Foreign Trade and
Development Cooperation

China: Declaration by the Minister for Foreign Affairs on behalf of the Belgian Government urging Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors

July 18, 2022

Belgium exposes malicious cyber activities that significantly affected our sovereignty, democracy, security and society at large by targeting the FPS Interior and the Belgian Defence.

Belgium assesses these malicious cyber activities to have been undertaken by Chinese Advanced Persistent Threats (APT).

We have detected malicious cyber activities that targeted the FPS Interior. These activities can be linked to the hacker groups known as Advanced Persistent Threat 27, Advanced Persistent Threat 30, Advanced Persistent Threat 31.

We have detected malicious cyber activities that targeted the Belgian Defence. These activities can be linked to the hacker groups known as UNSC 2814/GALLIUM/SOFTCELL.

Belgium strongly denounces these malicious cyber activities, which are undertaken in contradiction with the norms of responsible state behaviour as endorsed by all UN member states. We continue to urge the Chinese authorities to adhere to these norms and not allow its territory to be used for malicious cyber activities, and take all appropriate measures and reasonably available and feasible steps to detect, investigate and address the situation.

Belgium reaffirms its strong commitment to responsible state behaviour to ensure a global, open, free, stable and secure cyberspace. To this end, we will continue to work on the establishment of a Programme of Action under UN auspices to advance and effectively support states to adhere to responsible state behaviour in cyberspace.

We reiterate our determination to continue to counter malicious behaviour in cyberspace. With our European partners we will continue to enhance our cooperation, including with international partners and other public and private stakeholders, through increased exchange of information and continued diplomatic engagement, by strengthening cyber resilience and

incident handling cooperation, as well as through joint efforts to improve the overall security of software and their supply chains.