Key players in cyber-espionage world

Britain: Government Communications HQ

United States: National Security Agency

Malware programmes such as ***Warriorpride*** and ***Regin*** are used by Five Eyes – U.S., UK, Canada, Australia and New Zealand – to collect intelligence from email, video, voice and keystroke data

Islamic State: Uses ***Telegram*** messaging app which has end-to-end encryption, channels and self-destruct feature. IS ***Nashir*** channel has 11,700 followers in four languages

North Korea: Around 1,800 army hackers within ***Bureau 121*** assembled to attack financial institutions and media companies in South Korea, Japan, and U.S. Believed to have mounted Sony Pictures hack in 2014

Iran: ***Tarh Andishan*** – consists of at least 20 hackers in Iran with associates in Canada, Netherlands and UK. Group targets critical infrastructure in Europe, North America and Middle East

Syria: ***Syrian Electronic Army*** targets media outlets and journalists. In 2013 SEA hacked Associated Press Twitter account. Fake tweet that White House had been bombed resulted in markets falling by $136bn

China: ***Hidden Lynx*** "hackers for hire" group specialises in attacks on financial and defence sectors. Shanghai-based ***PLA Unit 61398*** targets U.S. intellectual property, business emails, and contacts. ***Putter Panda (Unit 61486)*** has mounted cyber attacks on Canadian, U.S. and EU aerospace companies. In July 2015 ***Deep Panda*** stole personal data of 21.5 million U.S. Federal employees

Russia: State-sponsored ***Energetic Bear*** targets U.S. and European critical infrastructure by sabotaging ICS (Industrial Control Systems). ***BlackEnergy*** malware toolkit captures screenshots, records audio, and harvests passwords and banking credentials from infected computers

Anonymous: Linked to hacks on governments in Canada, U.S. and Israel. Has "declared war" against IS after Paris attacks

Sources: Symantec, Crowdstrike, F-Secure

Pictures: Getty Images