2 The inhabitants of cyberspace's hostile side

Most of us think of "hostile" parties as having strong bodies, being armed, faces hidden by masks or helmets and exhibiting menacing behaviour.

Figure 5; Find the hacker – they couldn't be, could they?
CC BY schwgir SA

The reality is that malicious actions in cyberspace involve well educated, smart, creative individuals with a good knowledge of information technology. Any of the above graduating youngsters could be one (or more) of the characters in the list below.

This list is not comprehensive and evolves through human creativity. Gaps in legislation, that develops at a slower rate than new forms of crime, allows hostile elements to act with impunity and immunity.

YOU, accidentally. The author assumes you would not act deliberately against someone else. In fact, you yourself could be the problem when your electronic devices have been compromised and are used to spread malware, spam or messages pretending to be from you but sent by a third party with malicious intent. USB flash memories (also called thumb drives) are notorious offenders.

SOMEONE, deliberately. It does happen, in the form of fraud, sabotage, theft of intellectual property, planting compromising information on someone else's devices, etc. These are legally punishable offences but require the perpetrator to be caught and that the digital forensic evidence complies with legal requirements). It may also involve a non-criminal offence like giving you an infected USB memory as a gift that may not contain malware but has instead copies of copyrighted material.

Individual hackers. They could be anyone, anywhere, with good technical skills who choose to target a specific individual or organization. In 2002, a young Scotsman successfully committed what was described at the time as "the biggest military hack of all times" involving 97 US military and NASA computers. A request to extradite the individual to the USA, where the military hack took place, was denied by his country of origin on humanitarian grounds.

Malware suppliers. The design and distribution of malware has become a business (An article in The Economist referred to this as Crimeware As A Service or CaaS. Custom made malware designed to target a very specific target has been, designed, the best known being the Stuxnet malware used in 2010 to sabotage uranium enrichment facilities in Iran.

Professional hackers. The equivalent of a gun for hire, those who operate unethically specialize in the field of private detectives, industrial espionage and theft of intellectual property. Happily, many such professionals provide a service that tests the effectiveness of protective measures implemented by organizations. Called Ethical Hacking or Penetration Testing, it provides a "second opinion" (for a fee).

Hackers with a cause. Often referred to as "Hacktivists" work as loosely associated groups of individuals who have hacking skills and a particular target in mind (chosen by factors ranging from idealism to protest and revenge).

Cyber criminals. Working alone, in small groups or as part of Organised Crime, their motivation is primarily financial. They are behind the most successful scams that get individuals to give them money because they believe their stories.

Non-state actors. Usually referred to as "terrorists" or equivalent terms, their motivation is the disruption of civil society and governments.

State sponsored. Referred to as "cyber-armies", these are increasingly being mentioned in the Media but rarely, if ever acknowledged by governments. Clearly, the gathering of Intelligence and Counter-intelligence the context of National Security is neither new nor unusual – the tools have changed. There is considerable debate about what might be the appropriate balance between defensive measures and offensive capabilities.

Beyond the above list of players, there are others who provide questionable services such as downloads of music, video, electronic books, etc., that infringe the copyright of their legitimate creator, depictions of extreme violence, child pornography, hate sites and other. I you can think of it, you can find it. The same is true for software that if knowingly faulty or corrupted with malware. Best to be suspicious of "free" versions of software you normally have to pay for.

As there are no editorial controls or quality assurance on the World Wide Web, the contents of the 640 million websites (identified at the end of 2012), these range from trusted, high quality information to incorrect, biased, hateful content designed to mislead or influence.

To gain a quantified understanding of cyberspace, there are several sources of dependable information, such as http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/