Cyberterrorism could get personal, researchers suggest

January 12 2017, by David Bradley

Cyber terrorism is a controversial term. In considering terrorism, the popular image is of hijacked aeroplanes, buildings and lives destroyed by bombs, multiple shootings and other large-scale life-threatening incidents. It would be easy to marginalise cyberterrorism as nothing more important as a bit of hacking, a few leaked emails and passwords, a website blocked. Unfortunately, one must consider the scenario in which a cyberterrorist takes control of important infrastructure, transport systems, power grids, and defence installations. Where a network of terrorists might organise a large-scale terror attack involving conventional weapons, the cyberterrorist might take control of or even destroy infrastructure on which millions of lives depend.

Writing in the *International Journal of Business Continuity and Risk Management*, Nicholas Ayres, Leandros Maglaras, Helge Janicke, Richard Smith and Ying He of the School of Computer Science and Informatics, at De Montfort University, Leicester, UK, explain that in cyberterrorism the computer, the digital world, becomes both weapon and target, and the consequences of malicious use in such a context could have global consequences. They point out that the main focus of defence and intelligence agencies when it comes to the diffuse term cyberterrorism is currently critical national infrastructure. However, a very large proportion of the global population is now online. With simple tools, our personal computers and communications devices could be an easier and more tempting target for the cyberterrorist.

The cyberterrorist might, for instance, permanently disable our

connectivity at the individual level and cause harm perhaps by blocking access to utilities, health, and emergency services. They might physically damage our homes and other property by taking control of the growing number of Internet of things (IoT) devices used to control heating, refrigeration, lighting, security and other domestic systems, and increasingly our vehicles. Moreover, the concept of distributed denial of service attacks (DDOS) carried out by so-called "zombie" computers operating as part of a botnet have already been used widely in hacking well-known corporate databases. It may well be only a matter of time before a botnet is used to take control or manipulate with malicious intent critical systems in the domestic environment as well as in industry, commerce and defence.

"The postmodern cyberterrorist can deploy a digital weapon such as a virus that can be programmed to 'explode' or activate at a specified time or if a specific condition is met," the team suggests. "A whole new arsenal of digital armaments in order to attack a target that is anywhere in the world and equally can be deployed from anywhere," the team adds. Given that the primary motive of the terrorist is to instil fear in people, this might be possible on a global level with the threat and demonstration of a sufficiently destructive computer virus that interferes at a critical level in terms of safety, food and water, health and other critical aspects of our daily lives.

In the digital age we have a whole lot more to fear than fear itself, Franklin D…

More information: Nicholas Ayres et al. The mimetic virus: a vector for cyberterrorism, *International Journal of Business Continuity and Risk Management* (2016). DOI: 10.1504/IJBCRM.2016.081256

Provided by Inderscience Publishers