**Cyber-Terrorism**

In common with other forms of cyber-attacks, cyber-terrorism refers to computer-generated attacks that target other computers in cyberspace by use of internet to carry out acts of terror or create fear and panic within societies. It typically involves attacks on computer systems or networks, aiming to disrupt or damage critical infrastructure, steal sensitive information, or spread propaganda. These attacks vary from Cyber stalking, Hacking, Phishing, Bot Networks, Cyber squatting, Cross site scripting.

Cyber stalking, is one of the most common, is use of the Internet or other electronic means to stalk someone. Since cyber stalking is largely misunderstood, many incorrectly assume that cyber stalking involves an element of sexual obsession which is not as conclusive in that regard. Cyber stalking is a criminal offense motivated by interpersonal hostility and aggressive behaviors stemming from power and control issues rather than material gain or sexual obsession. Cyber stalking, like traditional offline stalking, is fueled by rage, power, control, and anger that may have been precipitated by a victim’s actions or, in some cases, the victim’s inactions.

Hacking is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Once the hacker gains access to the system be it bank account or any other account may steal or transfer money or whatever data they could be interested in. The situation can only be saved by the operator of the system.

Phishing is a social engineering technique that, through the use of various methodologies, aims to influence the target of the attack to reveal personal information, such as an email address, username, password, or financial information. This information is then used by the attacker to the detriment of the victim. A good example is innocently giving confidential bank accounts details to someone masquerading as a bank official only for it to be used to steal your money from your account.

Cyber squatting is the act of registering or using a famous domain name and then selling it for a fortune to profit from a trademark, corporate name, or personal name of an individual. In the context of this cybersquatting definition, domain squatting takes place as either a form of extortion or as an attempt to steal business from a rival. In the era of social media it’s a common occurrence for someone to register an account with a name of an already famous individual who is well known and will receive much more attention.

Bot Networks' is another form where spammer and other perpetrators of cyber crimes remotely take control of computers without the users realizing the fact that their system is being in use by some fake user. A bot is a piece of malware that infects a computer to carry out commands under the remote control of the attacker.

Cross site scripting is a type of computer security threat in which malicious users insert some harmful code into the web pages of trusted web sites viewed by other users to gain access in their devices. This attack occurs when a malicious user uses a web application to execute or send [malicious code](https://www.sciencedirect.com/topics/computer-science/malicious-code) on another user’s computer. This is a type of [attack](https://www.sciencedirect.com/topics/computer-science/cyber-attack) by which vulnerabilities are searched in a web application to introduce a harmful script.

Other forms may include obscene publication, obtaining license of digital signature by providing false information, breach of privacy, offence against public servant, forgery, criminal breach of trust etc.

Cyber terrorism or other forms of cyber attacks unlike other forms of traditional crimes present a lot of complexities that make them challenging to handle and resolve by the authorities due to changing technological complexities they present.

With the rise of work-from home revolution continuing, the risks posed by workers connecting or sharing data over improperly secured devices will continue to be a threat. Sharing of data over the internet exposes the victim especially through links and websites some which may not be easy to be suspicious about if they are sent by people known to you.

In cybercrime investigations, the process is not only impeded by the lack of knowledge regarding cybercrime but also the anonymity of suspects and often victims, lack of investigator understanding of these individuals and their lives and the asynchronous and non-physical nature of the Internet itself. Initial investigations will consist of obtaining accounts from victims and witnesses, ensuring their needs are met, identifying suspects, examining crime scenes, identifying further potential sources of evidence and documenting and submitting all relevant records and intelligence. Usually, the factors which determine the solvability of a case consist primarily of technical and physical evidence and other aspects such as the severity of potential damage or damage done.

Another challenge comes with the fact that the devices used to commit the crime especially computer security systems currently used do not track, trace and generate legally admissible evidence through the systems designed into computers which may impede the investigation. In the case of cyber squatting having just a name and not being able to track the individual involved undermines the investigation.

Police/law enforcement agencies have been found to lack knowledge about crime on the Internet. Some of the crimes committed over the internet are or may not have been legally known or documented as crimes/offence or have not been properly interpreted as crimes. Lack of understanding in law enforcement is considered a highly influential factor in war on cyber crimes.

Many police officers perceive cybercrime as quiet and distinct from traditional crimes, rather than as an extension or adaptation of them. The perceived differences between these crimes, and thus perceived applicability of existing skills and experience, reportedly affect investigator’s sense of preparedness and confidence in responding to cases of cybercrime. Better understanding and appropriate training are considered crucial in the response to cybercrime. Good police training determines their preparedness to deal with cybercrime cases and engage with victims.

Another issue comes in as the crimes committed over the internet may pose a problem to identify the perpetrator location and hence the jurisdiction. International law defines 'jurisdiction' as: "the limits of the legal competence of a State to make, apply, and enforce rules of conduct upon persons. The main issue regarding jurisdiction in the international space of the internet is the dichotomy which exists among three components of jurisdiction in cyber space that are personal jurisdiction, territorial jurisdiction, and universal jurisdiction. Of these, territorial jurisdiction and universal jurisdiction are more attuned to deter cyberterrorism. However, universal jurisdiction is the more suited to deter cyberterrorism due to the nature of the internet and the initial reality of cyberterrorism. This is because it ignores national borders. Although many steps have been taken to combat cyber-terrorism, from legal to technical steps, these attempts have not been sufficient to prevent cyberterrorism. Greater international cooperation is needed and nations must come up with self-regulatory legal mechanisms to combat against the misuse of new technologies; however, such mechanisms need to be supported by international agreements and appropriate national legislation.

Cyber‐terrorism is often a traditional crime just like fraud, identify theft, child pornography only that its executed swiftly and to vast numbers of potential victims, as well as unauthorized access, damage and interference to computer systems. Most detrimental are malicious and exploit codes that interrupt computer operations on a global scale and along with other cyber‐crimes threaten e‐commerce. The cross‐national nature of most computer‐related crimes have rendered many time honored methods of policing both domestically and in cross‐border situations ineffective even in advanced nations, while the digital divide provides safe havens for cyber‐criminals. In response to the threat of cyber‐crime there is an urgent need to reform methods of mutual legal assistance (MLA) and to develop trans‐national policing capability.

References

Rao, S., Verma, A.K. and Bhatia, T. (2021) /chapter/evolving-cyber-threats-combating-techniques-and-open-issues-in-online-social-networks/261732, <https://www.igi-global.com>.

Singh, D. (2023). Emerging Trends in Cyber Crimes. *Sustainable Business and IT*, 39-45.

Tehrani, P. M. (2017). *Cyberterrorism: The legal and enforcement issues*. World Scientific.