

Cyber Terrorism- the Dark Side of the Web World

Cyber coercion is the premeditated ingest of tumultuous activities, or the danger thereof, in cyber space, with the intention to boost social, ideological, religious, semipolitical or similar objectives, or to intimidate some person in progress of such objectives. Computers and the internet are becoming an essential part of our regular life. They are being utilised by individuals and societies to make their chronicle easier. They ingest them for storing information, processing data, sending and receiving messages, communications, controlling machines, typing, editing, designing, drawing, and nearly every aspects of life. The most deadly and destructive consequence of this helplessness is the emergence of the construct of “cyber terrorism”. The tralatitious concepts and methods of coercion impact taken newborn dimensions, which are more destructive and deadly in nature. In the geezerhood of aggregation technology the terrorists impact acquired an expertise to produce the most deadly compounding of weapons and technology, which if not correct safeguarded in due course of time, module verify its own toll. The damage so produced would be nearly permanent and most catastrophic in nature. In short, we are covering the worst modify of coercion popularly known as “Cyber Terrorism”.

The accumulation dealing with cyber coercion is, however, not competent to meet the unsafe intentions of these cyber terrorists and requires a rejuvenation in the light and context of the stylish developments every over the world. Cyber terrorist favour using the cyber move methods because of many advantages for it. These are:-1. It is Cheaper than tralatitious methods. 2. The action is very arduous to be tracked. 3. They crapper conceal their personalities and location. 4. There are no fleshly barriers or check points to cross. 5. They crapper do it remotely from anywhere in the world. 6. They crapper ingest this method to move a bounteous sort of targets. 7. They crapper affect a super sort of people. Forms of cyber terrorism-(I) Privacy violation: The accumulation of concealment is the acceptance of the individual’s correct to be permit alone and to impact his personal expanse inviolate. The correct to concealment as an independent and characteristic construct originated in the field of Tort law, under which a newborn cause of action for damages resulting from unlawful entrance of concealment was recognized. (II) Secret aggregation appropriation and data theft: The aggregation technology crapper be misused for appropriating the valuable Government secrets and data of clannish individuals and the Government and its agencies. (III) Demolition of e-governance base: The aim of e-governance is to make the interaction of the citizens with the government offices hassle free and to deal aggregation in a free and transparent manner. It boost makes the correct to aggregation a meaningful reality. In a democracy, people govern themselves and they cannot govern themselves correct unless they are aware of social, political, scheme and other issues confronting them. This, correct to obtain aggregation is, however, not unconditional but is subject to reasonable restrictions which haw be imposed by the Government in open interest. (IV) Distributed forgoing of services attack: The cyber terrorists haw also ingest the method of distributed forgoing of services (DDOS) to overburden the Government and its agencies electronic bases. This is made possible by prototypal infecting individual open computers by way of virus attacks and then taking control of them. Once control is obtained, they crapper be manipulated from some locality by the terrorists. These pussy computers are then made to send aggregation or demand in such a super sort that the machine of the victim collapses. (V) Network damage and disruptions: The main aim of cyber terrorist activities is to cause networks damage and their disruptions. This state haw entertain the attention of the security agencies for the instance being thus gift the terrorists extra instance and makes their task comparatively easier. This process haw refer a compounding of machine tampering, virus attacks, hacking, etc. The intention of a cyber coercion move could arrange from scheme disruption through the gap of financial networks and systems or utilised in hold of a fleshly move to cause boost confusion and possible delays in proper response. Effects of Cyber Terrorism on scheme & social life-Direct Cost Implications• Loss of income during the disruption • Staff time, network delays, intermittent access for business users • Increased insurance costs due to proceedings • Loss of highbrowed property – research, pricing, etc. • Costs of forensics for recovery and proceedings • Loss of grave communications in instance of emergency. Indirect Cost Implications• Loss of confidence and quality in our financial systems • Tarnished relationships& open image globally • Strained business partner relationships – domestic and internationally • Loss of forthcoming customer revenues for an individual or group of companies • Loss of trust in the government and machine business The following are notable incidents of cyber terrorism: • In 1998, social Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages feature “We are the cyberspace Black Tigers and we’re doing this to disrupt your communications.” Intelligence authorities characterized it as the prototypal known move by terrorists against a country’s machine systems. • During the Kosovo conflict in 1999, NATO computers were blamed with e-mail bombs and impact with denial-of-service attacks by hacktivists complaintive the NATO bombings. In addition, businesses, open organizations, and academic institutes received highly politicized virus-laden e-mails from a arrange of Eastern European countries, according to reports. Web defacements were also common. • Since Dec 1997, the Electronic Disturbance Theater (EDT) has been conducting Web sit-ins against various sites in hold of the Mexican Zapatistas. At a designated time, thousands of protestors point their browsers to a direct place using software that floods the direct with rapid and repeated download requests. EDT’s software has also been utilised by animal rights groups against organizations said to abuse animals. Electrohippies, another group of hacktivists, conducted Web sit-ins against the WTO when they met in metropolis in late 1999. The Interpol, with its 178 member countries, is doing a great employ in conflict against cyber terrorism. They are helping every the member countries and training their personnel. The Council of Europe Convention on Cyber Crime, which is the prototypal planetary accord for conflict against machine crime, is the result of 4 years work by experts from the 45 member and non-member countries including Japan, USA, and Canada. This accord has already implemented after its ratification by Lithuania on 21st of March 2004. The Association of South East Asia Nations (ASEAN) has set plans for sharing aggregation on machine security. They are

feat to create a regional cyber-crime unit by the assemblage 2005. The protection of I.T.A crapper be claimed for: (a) Preventing concealment violations, (b) Preventing aggregation and data theft, (c) Preventing distributed forgoing of services move (DDOS), and (d) Preventing network damage and destruction. Here are some key things to advert to protect from cyber-terrorism: 1. All accounts should impact passwords and the passwords should be unusual, arduous to guess. 2. Change the network configuration when defects embellish know. 3. Check with venders for upgrades and patches. 4. Audit systems and check logs to help in detecting and tracing an intruder. 5. If you are ever unsure most the safety of a site, or obtain suspicious email from an unknown address, don't access it. It could be trouble. The problems associated with the ingest of malware are not peculiar to some particular land as the danger is orbicular in nature. The countries every over the concern are covering this difficulty and are trying their verify best to eliminate this problem. The problem, however, cannot be effectively curbed unless favourite open hold and a vigilant judiciary backwards it. The assembly cannot enact a accumulation against the general open instrument of the commonwealth at large. Thus, prototypal a open hold has to be obtained not only at the domestic verify but at the planetary verify as well. The people every over the concern are not against the enactment of statutes curbing the ingest of malware, but they are conscious most their legitimate rights. Thus, the accumulation to be enacted by the assembly must verify tending of open welfare on a priority basis. This crapper be achieved if a suitable technology is supported by an apt legislation, which crapper exclusively verify tending of the danger created by the computers sending the malware. Thus, the self-help measures constituted by the assembly should not be disproportionate and excessive than the danger received by the malware. Further, patch using such self-help measures the property and rights of the general open should not be affected.