# HACKERS OR POTENTIAL TERRORISTS: ANALYSIS OF CYBER MENACE

**Mr. Pawan Khatri & Mr. Arindam Neral**[1]

## ABSTRACT

*Cyber technology is growing at an enormous rate enabling humans to minimize efforts and maximize efficiency. Real and virtual worlds are coming closer to each other and such growth poses a serious threat of cyber terrorism which has surfaced in the last decade. Cyber terrorism means using severe disrupting activities on cyberspace with an intention of causing mass carnage and destruction. In the recent years, cyber attacks in Europe have risen enormously and indicate a need for more efficient legislative initiatives to deal with them. It is often portrayed as a bigger threat to states which are technologically advanced. The prime question is - the threat is real or the fear is being exaggerated. Cyber terrorism in comparison to physical terrorism is cheaper, offers extreme anonymity and maximum destruction with just a few well-aimed keystrokes and cyber attack techniques. Then, why no instance of extreme cyber attack with an aim of mass destruction has been recorded yet. Few people believe that such attacks go unreported and are treated as state secrets to avoid public fear and incompetence remarks for the government. And even if the fear is exaggerated it can't be blindly ignored or denied because as the tech-savvy generation comes of age the threat will increase many folds.*

*In our research paper, we will firstly examine the methods and tools which are used by the hackers in cyber attacks. The authors shall then discuss the legislative measures or steps in the past and which should be taken by European nations to curb cyber crime and cyber terrorism. Finally, the authors shall discuss some of the major cyber attacks which have damaged the real and virtual worlds in the past with special reference to Europe.*

[1] Student of B.A. LL.B (Hons.), Hidayatullah National Law University, Raipur, Chhattisgarh.

## INTRODUCTION

Data security – the protecting of computer frameworks and the integrity, secrecy, and accessibility of the information they contain – has for some time been perceived as a basic arrangement issue. Its significance is developing as the reconciliation of computers into more parts of present day life proceeds. Also, cyberattacks, or breaks of data security, have all the earmarks of being expanding in recurrence, and few will disregard the likelihood that the seriousness of future attacks could be much more prominent than what has been seen to date.

Among non-conventional security issues, cyber security is likely the one that has increased most unmistakable quality as of late. While a quarter century not very many considered cyber security a test, today it is seen as one of the best difficulties to worldwide security. This is expected, among different elements, to society's expanding dependence on the web and on data and correspondence advances, and in addition to the developing complexity of cyber attacks. A large portion of our basic bases (power lattices, the saving money framework, transportation, and so on) depend on to some degree or completely on the web.

In the cyber world, the present condition with respect to the specialized capacity to track and follow cyber attacks is primitive, best case scenario. Refined attacks can be practically difficult to follow to their actual source utilizing current practices. The anonymity delighted in by today's cyberattackers represents a grave danger to the worldwide cyber society and world security. The developing complexity of cyber attacks has pulled in equivalent consideration recent year. The Stuxnet infection, found in 2010, is a decent sample. The infection focused on a particular bit of IT hardware of Iran's atomic offices with the goal of backing off Tehran's atomic system. This was a very many-sided move, professedly created by the US and Israel[2]. What is by all accounts dissolving or blurring ceaselessly is the fringe in the middle of virtual and genuine security.

Cyber security is an intricate reality with numerous measurements. Reacting to the cyber test requires a decent comprehension of this unpredictable issue. Cyber Attacks are distinguished into various classifications such as cyber theft, cyber harassment etc, out of which the paper would break down critical parts of Cyber Terrorism. Terrorist bunches have been dynamic on the web

[2] V. Manzo, 'Stuxnet and the dangers of cyber war', The National Interest, 29 January 2013.

for quite a while, with the point of radicalizing and enrolling new individuals. The web can be utilized for financing purposes, and also to plan attacks, for the occasion using smart administrations, for example, Google Earth. Terrorist gatherings could likewise dispatch full-scale cyber attacks to seek after their political goals. Some security specialists trust that there is a believable danger of cyber attacks from terrorist bunches later on.

## CYBER TERRORISM

Cyber terrorism is the joining of the internet and terrorism. It alludes to unlawful attacks and dangers of attacks against computers, systems and the data put away in that when done to threaten or force a legislature or its kin in encouragement of political or social destinations. Further, to qualify as cyber terrorism, an attack ought to bring about viciousness against persons or property, or if nothing else causes enough damage to produce dread. Attacks that prompt passing or substantial damage, blasts, or extreme monetary misfortune would be cases. Genuine attacks against basic bases could be demonstrations of cyber terrorism, contingent upon their effect. Attacks that disturb insignificant administrations or that are chiefly an exorbitant annoyance would not.

***"Cyber terrorism is an alluring alternative for current terrorists since it offers assortment and enormous number of targets, it is more mysterious than customary terrorist strategies, it is less expensive than customary terrorist techniques, it can possibly influence specifically a bigger number of individuals than conventional terrorist strategies, cyberterrorism can be led remotely, an element that is particularly speaking to terrorists, requires less physical preparing, mental speculation, danger of mortality, and go than ordinary types of terrorism, making it less demanding for terrorist associations to enlist and hold devotees."***[3]

There have been a few hindrances to making an unmistakable and steady meaning of the expression "cyber terrorism." First, as simply noted, a significant part of the discourse of cyberterrorism has been led in the famous media, where writers regularly take a stab at dramatization and sensation instead of for good operational meanings of new terms. Second, it has been particularly regular when managing computers to coin new words essentially by setting the

[3] Gabriel Weimann, Cyber terrorism How Real Is the Threat? (2003), UNITED STATES INSTITUTE OF PEACE.

words cyber, computer, or data before another word. The basis of the thought of cyberterrorism can be followed back to the mid-1990s when the quick development in Internet use and the civil argument on the rising "data society" started a few studies on the potential dangers confronted by the exceptionally organized, cutting edge subordinate United States. As right on time as 1990, the National Academy of Sciences started a report on computer security with the words, "We are in danger. Progressively, America relies on upon computers. . . . Tomorrow's terrorist might have the capacity to accomplish more harm with a console than with a bomb." in the meantime, the prototypical term "electronic Pearl Harbor" was begat, connecting the risk of a computer attack to an American chronicled injury. "It's nothing unexpected," contends Green, "that cyberterrorism now positions close by different weapons of mass demolition in people in general cognizance[4] . . . yet, there's only one issue:

There is no such thing as cyber terrorism – no case of anybody continually having been murdered by a terrorist (or any other individual) utilizing a computer. Nor is there convincing confirmation that al-Qaeda or some other terrorist association has depended on computers for any kind of genuine damaging movement." It appears to be reasonable to say that the present danger postured by cyberterrorism has been misrepresented. No single occurrence of cyberterrorism has yet been recorded: there were politically propelled cyberattacks, as a type of challenge, as a rule including site ruinations (with a political message) or a few sorts of disavowal of administration (DoS) attack[5]. Be that as it may, while the cyberattacks were politically inspired, from the beginning the attacks were unequipped for hurting individuals or property or imparting dread into the objective populace. Its effect was fundamentally intended to bring about a disturbance and did not seriously affect basic administrations or framework. Most by far of cyberattacks are dispatched by programmers with few if any political objectives and no craving to bring about the anarchy and gore of which terrorists dream. All in all, then, why has so much concern been communicated over a generally minor risk? The purposes behind the fame of cyberterrorism anxiety are numerous. Mental, political, and monetary strengths have consolidated to advance the trepidation of cyberterrorism.

[4] System Security Study Committee, Computers at risk (1991), National Academy Press

[5] The downing of a U.S. spy plane in Chinese airspace (April 2001) resulted in an increase in attacks from both Chinese and U.S. hackers (mostly web site defacements).

In the first place, from a psychological view, two of the biggest fears of cutting edge time are joined in the expression "cyber terrorism."[6] The apprehension of arbitrary, rough exploitation segues well with the doubt and by and large dread of computer innovation. An obscure danger is seen as more undermining than a known risk. In spite of the fact that cyber terrorism does not involve an immediate risk of viciousness, its mental effect on edge social orders can be as intense as the impact of terrorist bombs. In addition, the most ruinous strengths conflicting with a comprehension of the real risk of cyberterrorism are an apprehension of the obscure and an absence of data or, more regrettable, an excess of falsehood.

Second, Cyber terrorism blends two circles terrorism and innovation that numerous individuals, including most legislators and senior organization authorities, don't completely comprehend and consequently tend to fear. Additionally, a few gatherings are excited to adventure this lack of awareness: "Various innovation organizations, as yet reeling from the breakdown of the tech bubble, have recast themselves as trendsetters critical to national security and helped their Washington nearness with an end goal to draw in government dollars." Law implementation and security advisors are moreover exceptionally energetic to have everybody trust that the risk to the country's security is serious. As Ohio State University law teacher Peter Swire contended, "Numerous organizations that rode the website blast need to discover huge new wellsprings of wage. One is immediate deals to the government; another is elected orders. On the off chance that we have a major government push for new security spending, that could prop up the listing market." [7]

Third, the mass communications have added their voice to the frightful tune, trumpeting the danger with front-page features, for example, the accompanying, which showed up in The Washington Post in June 2003: "Cyber-Attacks by Al Qaeda Feared, Terrorists at Threshold of Using the Internet as Tool of Bloodshed, Experts Say." The mass media frequently fail to distinguish between hacking and cyberterrorism and exaggerate the threat of the latter by reasoning from false analogies.

[6] A. Embar-Seddon. “Cyber terrorism.” The American Behavioral Scientist 45 (2002), pp. 1033–1043.
[7] Joshua Green, “The Myth of Cyber terrorism” (2002), Washington Monthly

## EVOLUTION OF HACKING

The principal genuine appearance of a computer hacker happens about 100 years after the fact, in the 1960s. A "hack" has dependably been a sort of alternate way or adjustment—an approach to sidestep or revise the standard operation of an article or framework. The term started with model train devotees at MIT who hacked their train sets so as to change how they functioned. The 1970s created another sort of hacker, one concentrated on phone frameworks. Known as "phreakers," these hackers found and abused operational attributes of the recently all-electronic phone exchanging system that empowered them to make long separation calls for nothing out of pocket. The phreaker development is an imperative early case of a mutinous subculture that brings forth powerful hackers and visionaries in the domain of the computer.

Hacking delighted in a brilliant period of sorts in the 1980s. The presentation of turnkey "individual" computers by Radio Shack, IBM, Apple, and others is a defining moment in hacker history. Presently computers were no more constrained to the domains of bad-to-the-bone specialists and business clients; anybody, including existing but then to-be-acknowledged hackers, could procure a computer for their own particular purposes. Modems, gadgets that empowered computers to speak with each other over phone lines, were likewise all the more broadly accessible and fundamentally expanded the hacker's compass. In spite of the fact that hacking extended and delighted in glorification amid its brilliant years, a gap was framing inside the hacking group by the late 1980s. An expanding number of hackers were no more fulfilled by amiable investigation of frameworks simply to figure out how they functioned. The hacker standard of "flexibility of innovation" as portrayed by Levy was changing, and a more youthful era intrigued by individual addition rose.[8]

This new type of "hacker" coordinated its information and steadiness toward unmistakably criminal interests, including the dissemination of pilfered business programming, amusements, and infections and worms that could essentially close down frameworks. The dim side divided significantly further as a few gatherings framed "electronic groups," headed to take advantage of the delicate data housed inside substantial foundations, similar to government and instructive exploration focuses.

[8] Zuley clarke, A brief history of hacking, 2003, Historical Approaches to Digital Media

One of the most current types of hacking includes finding and associating with unsecured Wireless Access Points (WAPs). Additionally called "whacking," the practice has developed with the inexorably across the board utilization of remote systems.[9] Whacking gains by the relative straightforwardness with which numerous remote systems can be gotten to (by and large in light of the fact that their proprietors haven't found a way to secure them). The remote way of these systems makes them simple to discover and hack, and in light of the fact that they so frequently broaden Internet access, remote systems are particularly tempting focuses for an unapproved use.

## MAJOR CYBER ATTACKS IN THE PAST

Any nation that uses the web as a major aspect of its base should know about the vulnerabilities and results of a cyber attack on their framework. An intelligible methodology must incorporate web safeguards that are set-up in conjunction with specialized guards. At present, lawful definitions for cyber-violations don't exist in all nations. The global group must look at bargains and overhaul them to better characterize help and basic resistance in the case of a cyber attack. There have been numerous episodes of cyber attacks on different countries which make a wide degree break down the apparatuses and examples utilized as a part of the cyber attacks keeping in mind the end goal to enhance the ability to manage them. The real issue which countries face amid such attacks is the new and advanced systems utilized by the assailants. Taking after are the major cyber attacks in the past furthermore the systems and instruments utilized as a part of those attacks:

## I. CYBER ATTACK ON ESTONIA – 2007

The center of the cyber attack was to totally close down the IT structure of Estonia. The cyber assailants utilized botnet attacks to perform a disseminated foreswearing of administration rendering frameworks that utilization the web pointless. Botnets are seized computers that convey mass measures of data which overpower a web server. The expansion in web activity will bring about a server to surpass its data transfer capacity abilities and cause it to close down. The botnets can be introduced well ahead of time of an arranged cyber attack, and they can be put in any computer anyplace on the planet. In the event that the computer client has not introduced proper

[9] Related practices are “war driving,” or actively seeking usable WAPs, and “war chalking,” See http://www.warchalking.org.

defensive programming on their computer they won't realize that they have been commandeered and that they are taking an interest in a cyber attack. The botnet attacks on the Estonian IT structure finished as unexpectedly as they started driving Estonian authorities to presume that the attack was an arranged and facilitated.[10]

The Estonians could react to the cyber attacks in an extremely capable way, as they could facilitate reactions that just brought about generally fleeting blackouts rather than any perpetual harm to their IT foundation. The Estonian government could utilize its Computer Emergency Response Team (CERT) which facilitated IT reactions among government and regular citizen masters. Nonetheless, because of the uncertain way of the web and the utilization of fake web convention (IP) addresses the Estonian's were not able definitively to demonstrate who started the cyber attacks.[11] The cyber attacks themselves were not very sophisticated as the attackers used techniques that had been in existence for several years.

## II. CYBER ATTACK ON GEORGIA – 2008

On July 20, 2008, the site of the Georgian president went under a dissent of administration cyber attack. The attack close the site down for 24 hours and was an antecedent to a bigger cyber attack that would come not exactly a month later. On August 8, 2008, an organized appropriated dissent of administration attack was made against the Georgian government sites while Russian strengths were occupied with a battle with Georgian powers. As the ground attacks expanded so did the cyber attacks. This was the first occasion when that a cyber attack was done in conjunction with the furnished clash. [12]

The cyber war in the middle of Georgia and Russia concentrated on forming general feeling on the web. Georgian and Russian supporters utilized an assortment of cyber systems including disseminated foreswearing of administration attacks and the making of fake sites to control how their rendition of the "reality of the situation" was conveyed to people in general. Georgia's IT foundation was not exceptionally propelled so the disturbance of administration was not as

[10] Joshua Davis, Hackers Take Down the Most Wired Country in Europe, (Wired Magazine: Issue 15.09).
[11] Mike Collier, Estonia: Cyber Superpower (BusinessWeek, December 17, 2007) http://www.businessweek.com/globalbiz/ content/dec2007/gb20071217_535635.htm.
[12] Alexander Melikishvili, Recent Events Suggest Cyber Warfare Can Become New Threat (WMD Insights, December 2008/January 2009 Issue)

confounded as it was in Estonia. Saving money, media, and government sites were blocked disturbing the stream of data all through Georgia and to the outside world.

The sites of the Ministry of Foreign Affairs and the National Bank were vandalized by including photos of the Georgian President and Adolph Hitler. The cyber attacks against Georgia were not the same as the cyber attacks on Estonia, as these attacks included appropriated foreswearing of administrations utilizing botnets, however, they likewise included SQL[13] infusion attacks that are harder to recognize than a botnet attack since they require fewer computers than a botnet attack. The SQL infusion attack demonstrates a more prominent aptitude in the capacity to lead a cyber attack than the cyber attacks on Estonia's IT base. [14] Georgia got a considerable measure of help to counter the cyber attacks and to impart inside and universally. Google gave area space to ensure the sites of the Ministry of Foreign Affairs and Civil.ge, a Georgian Daily online news administration.

A private American network access supplier (the leader of the organization is an ethnic Georgian) helped the Georgian government by facilitating the Georgian President's site. The President of Poland additionally helped the Georgian government by setting official public statements on his site. Estonia even sent two data security authorities from its Computer Emergency Response Team to help Georgia in countering the cyber attacks.

## III. TITAN RAIN-USA – 1998

At some point on November first, 2004, programmers sat down at computers in southern China and set off at the end of the day on their every day chase for U.S. privileged insights. Since 2003 the gathering had been leading wide-ranging attacks on U.S. government focuses on taking touchy data, part of a gigantic cyberespionage ring that U.S. examiners have codenamed Titan Rain. On this specific night, the programmers' quarry was military information, and they were furnished with another weapon to connect crosswise over the internet and get it. This was a scanner program that "made preparations," as indicated by a previous government system investigator who has followed Titan Rain, via looking unfathomable military systems for single computers with

[13] Structured Query Language

[14] Secure Works Press Release, Compromised US and Chinese Computers Launch Greatest Number of Cyber Attacks, according to Secure Works' Data (September 22, 2008)

vulnerabilities that the aggressors could misuse later. Similarly as with a large portion of their apparatuses, this was a straightforward system, yet one that had been cunningly adjusted to fit their needs, and afterward utilized with merciless proficiency against an inconceivable cluster of U.S. systems. In the wake of performing the outputs, the source says, it's a virtual conviction that the assailants returned inside a day or two and, as they had on many military systems, broke into the computers to take away however much information as could be expected without being identified. [15]

## THREAT TO SCADA SYSTEMS

Power matrices, dams, and other mechanical offices observed by SCADA (Supervisory Control and Data Acquisition frameworks) are ready for target and better suit their purpose to harm physical base and upset basic modern offices. Truth be told, numerous late Internet reports demonstrate that SCADA frameworks, for example, water supply, wastewater, and comparable frameworks are especially powerless, in light of the fact that they have for some time been "outside" the domain of thought as basic security and real destruction in these frameworks could without much of a stretch result in frenzy and even mass craziness among the populace, a terrorist's fantasy! These frameworks are the genuine dangers, those that are broad, likely topographically scattered, not considered as being basic frameworks and without which regular life as we probably am aware it is adjusted to the point that open trust in their security would be disintegrated, and further the trust in those that are in charge of their assurance would likewise be criticized.

Obviously, we knew about these dangers before "9/11", yet little consideration was paid to the moderation of these shortcomings on the grounds that other – all the more prominent targets were viewed as more vital. National base data was found on al-Qaeda computers. Agents found a house in Pakistan keep running by al-Qaeda that was committed to preparing for cyber warfare and hacking, as indicated by coalition insight authorities. It is anything but difficult to foresee that in the long run since time is running short and assets, al-Qaeda saltines can and will figure out how

[15] NATHAN THORNBURGH, Inside the Chinese Hack Attack, Thursday, Aug. 25, 2005

to break into these frameworks unless we continue in building new security safeguards around these frameworks to evade their further examination of SCADA frameworks.[16]

## MAJOR THREAT TO EUROPE & EU'S APPROACH TOWARDS IT

Europe has been a prime focus of cyber attacks over all classes of cyber attacks. Numerous cyber occurrences have been accounted for as of late, with a pattern indicating an expansion regarding both recurrence and advancement of the risk.[17] As to cyber terrorism, Europe has seen a developing number of solitary wolf terrorists as of late, self-radicalized through the web. Europol likewise gives careful consideration to the danger of cyberattacks by terrorist bunches. It talked about this particular danger without precedent for its 2012 yearly risk evaluation.[18] In 2007, Estonian servers were likewise casualties of cyber attacks, by and large, ascribed to Russia, arousing Europe to the truth of 'cyber warfare'.[19] On the premise of the developing cyber risk, Europe has endeavored to build up a more key approach and to reinforce cyber security capacities at the national, provincial (EU and NATO) and worldwide levels (G8 and UN).

EU residents are additionally worried about their cyber security. As indicated by a 2011 survey, 81 for each penny of EU nationals trust that cyber wrongdoing is an essential test to the EU's inside security, in spite of the fact that not as a matter of course the most squeezing one.[20] Numerous Europeans might want to see an all the more ace dynamic EU in the territory of cyber security. Among all security challenges, this is the one where the most EU subjects (36 for each penny) consider that the EU could accomplish more.[21] They additionally trust that the cyber test all in all is turning out to be more critical. As per a 2013 survey, 76 for every penny of EU subjects trust that they are more presented to cyber culpability now than they were some time

[16] Michael Ratledge, Cyber Terrorism in the 21st Century, September 26, 2002
[17] Robinson 2012, op. cit. See also Europol, Threat assessment: Internet facilitated organized crime (iOCTA) (The Hague: Europol, January 2011).
[18] Europol, TE-SAT 2012 (The Hague: Europol, 2012).
[19] See e.g. S. Herzog, 'Revisiting the Estonian cyber attacks: cyber threats and multinational responses', Journal of Strategic Security, 4:2, 2011, pp. 49-60.
[20] European Commission, 'Internal security', Euro barometer 371, November 2011.
[21] European Commission, 'Internal security', November 2011, op. cit.

recently.[22] There is in this manner well-known backing for an all inclusive reaction to cyber security.

European worries over cybersecurity date far back, yet have been aggravated as of late by two variables specifically. From one viewpoint, the expansion in cyber guiltiness and cyber attacks has underscored Europe's weakness to these sorts of dangers. Then again, the perseverance of the financial emergency and the chase for development has underlined the requirement for cyber 'trust and security', as recognized in the Cyber Agenda for Europe. The EU is not short on "procedures" to manage cyber difficulties. In 2001, the European Commission had effectively distributed a correspondence entitled 'System and Information Security: a proposition for European Policy approach', which recognized key difficulties and figured a few proposals with respect to the issue. As to cyber terrorism, the 2005 counter-radicalization system clarified references to the significance of the web. Cyber security is presently investigated in the six-month to month progress reports of the EU's counter-terrorism organizer.

These advancements in any case, until the end of the most recent decade the EU had drawn closer the issue of cyber security 'in a divided way, where parallel approaches have been propelled with various covering topics'.[23] In 2008, be that as it may, cyber security was distinguished as a key test in the survey of the European Security Strategy (ESS) and, after two years, in the Internal Security Strategy (ISS). A more key methodology was commanded. The ISS made the first commitment by recognizing three clear targets: building limits in law implementation and legal, working with industry, and enhancing abilities for managing cyber attacks. This was supplemented by a Cyber-wrongdoing Action Plan embraced by the European Council in 2010.

In February 2013, the EU received its hotly anticipated Cyber-security Strategy.[24] As it was a joint activity by the Commission and the High Representative, it could connect the diverse aspects of the cyber test into a solitary report, i.e. interior security (counting cybercrime and CIIP), outer security, and remote and resistance strategies.

[22] European Commission, 'Cyber security', Euro barometer 404, November 2013.
[23] A. Klimburg and H. Tirmaa-Klaar, 'Cyber security and cyber power: concepts, conditions and capabilities for cooperation for action within the EU', European Parliament Study, April 2011, p. 29.
[24] European Commission and High Representative, 'Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace', Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013)1, 2013

As per Neelie Kroes, the EU Cyber Agenda official, the EU's cyber security relies on upon its capacity to arrange crosswise over sectoral strategies, not exclusively in part states but rather likewise in participation with key universal partners. A typical European methodology would permit the EU to end up a more vital and trusted accomplice at the universal level, with positive advantages for its security and aggressiveness. The EU has been dynamic in characterizing a 'worldwide coordination system' and a 'mutual structure' to make the web sheltered and stable. [25] Like different difficulties, in cyber security the EU has built up an adaptable multi-layered methodology, drawing in with an assortment of partners at the multilateral, local and two-sided levels.

While this more coordinated methodology speaks to a stage forward in managing a standout amongst the most genuine worldwide difficulties of our time, the EU is falling admirably behind the US in such manner, not minimum since its part states are themselves lingering behind. In 2003, Washington embraced a cyber strategy, while just a couple EU part states have one today. The EU ought to along these lines urge its part states to put more in their cyber security, with a perspective to transforming Europe into a genuine cyber power. Regarding spending plan, the EU is putting critical sums around there, with over €500 million predicted under the exploration and development program 'Skyline 2020'.27 Several activities have additionally been supported under DG Home's ISEC (now IFS Police) monetary instrument.[26] While subsidizing is still extremely minimal, it can be seen as the start of the EU's worldwide part in cyber security.

## INTERNATIONAL LAW & CYBER TERRORISM

Treaties and Conventions with regard to terrorism[27] characterize particular offenses, require states gatherings to criminalize the offenses in national law, order the gatherings take purview over the offenses and set up law authorization help commitments associated with the offenses. Through this methodology, states blended substantive, jurisdictional, and procedural parts of their national criminal laws and set up procedures for reinforced law authorization collaboration on the characterized violations. The formation of numerous arrangements tending to different offenses

[25] European Commission, 'Achievements and next steps: towards global cyber-security', 2011, op. cit
[26] European Commission, 'Table on the Implementation of the "Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace"', Working document, 28 February 2014
[27] See Foot note. 26

streams from states' responses to various terrorist assaults and inability to embrace an exhaustive settlement on terrorism. Counter terrorism arrangements are imperative for various reasons.

In the first place, demonstrations of cyber terrorism may fall inside the extent of a few assertions, making those instruments important for distinguishing universal law appropriate to cyber terrorism. How well or inadequately the counter-terrorism arrangements spread potential demonstrations of cyber terrorism may uncover crevices here of global law. Second, the criminal law approach utilized as a part of the counter-terrorism settlements brings up issues about whether the advancement of universal law on cyber terrorism ought to accentuate this technique. The reliance of administrative and monetary exercises on cyber innovations makes cyber terrorism against divisions and ranges tended to in these settlements conceivable. Universal law is not without bargain law governments could apply in reacting to certain demonstrations of cyber terrorism. The topic of a few settlements incorporates parts frequently specified in dialogs of cyber terrorism, for example, transportation administrations, government offices, atomic plants, and base giving open administrations. Be that as it may, states did not embrace these concurrences with cyber terrorism at the top of the priority list—truth be told, just three bargains recorded in Table 1 were finished up after the Internet turned into a worldwide correspondences stage in the mid-1990s. For instance, the International Convention for the Suppression of Terrorist Bombings (2005) has the broadest extent of the counter-terrorism settlements since its offenses cover various areas as opposed to only one range.[28]

## LEADING TREATIES ON TERRORISM

1963 - Convention on Offenses and Certain Other Acts Committed on Board Aircraft

1970 - Convention for the Suppression of Unlawful Seizure of Aircraft

1971 - Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation

1973 - Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents

[28] David P. Fidler, Study Group on Cyber security, Terrorism, and International Law, INTERNATIONAL LAW ASSOCIATION

1979 - International Convention against the Taking of Hostages

1988 - Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation

1988 - Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf

1988 - Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation

1997 - International Convention for the Suppression of Terrorist Bombings 1999 International Convention for the Suppression of the Financing of Terrorism

2005 - International Convention for the Suppression of Acts of Nuclear Terrorism[29]

## CONCLUSION

"In any event until further notice, captured vehicles, truck bombs, and natural weapons appear to represent a more prominent danger than cyber terrorism. Pakistan, the focal point of Al Qaeda's innovative work for fashioning electronic reports, message encoding and unraveling, encryption strategies, and techniques for breaking encryption. Future terrorists may without a doubt see the more prominent potential for cyber terrorism than do the terrorists of today. Moreover, the up and coming era of terrorists are presently experiencing childhood in a cyber world, one in which hacking devices are certain to wind up all the more capable, easier to utilize, and simpler to get to.

Cyber terrorism may likewise turn out to be more alluring as the genuine and virtual universes turn out to be all the more firmly coupled. For example, a terrorist gathering may at the same time blast a bomb at a train station and dispatch a cyberattack on the interchanges foundation, along these lines amplifying the effect of the occasion. Unless these frameworks are deliberately secured, leading an online operation that physically hurts somebody might be as simple tomorrow as infiltrating a site is today. Incomprehensibly, achievement in "the war on fear" is prone to make terrorists swing progressively to eccentric weapons, for example, cyber terrorism. The test is to

[29] David P. Fidler, Study Group on Cyber security, Terrorism, and International Law, INTERNATIONAL LAW ASSOCIATION

survey what should be done to address this vague, however, potential danger of cyberterrorism—yet do as such without blowing up its genuine essentialness and controlling the trepidation it motivates.

Taking everything into account, the majority of the proof to date demonstrates that terrorist gatherings are making far-reaching utilization of the Internet, however so far they have not depended on cyberterrorism. The risk of cyberterrorism might be overstated and controlled, yet it can be neither denied nor overlooked: Vernon, in Black Ice: The Invisible Threat of Cyber-Terror, cautions that "the terrorist associations are moving toward cyberterrorism," and, "I ask you to contemplate the future before the calamity happens."