International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-5s, January 2019

An International Study on the Risk of Cyber Terrorism

Suhannia Ponnusamy, Geetha A. Rubasundram

Abstract: ***Cyberterrorism has been a risk since the advent of the Internet. Technology has developed at a rapid pace, and likewise, the risk and impact of cyberterrorism. It is pertinent that secure and updated mechanisms are in place to mitigate the risk of cyberterrorism, with international cooperation and collaboration to further enhance investigation and information gathering. This paper discusses mechanisms such as security applications, security policies, comprehending education programs, international co-operation, monitoring and Artificial Intelligence (AI) and monitoring, using and disrupting approach (M.U.D). Implementations of all the mechanisms allows computer network and systems to be less vulnerable and manages the risk of cyberterrorism because each mechanisms possess separate functions for combatting cyberterrorism. As a result, the objectives and hypothesis for this research evidences a positive correlation between the mechanisms recognized and the perceived risk of cyberterrorism. Various initiatives has been introduced by respective bodies from all over the world in order to ensure that the threat of cyberterrorism is controllable. However, the threat of cyberterrorism continuous to increase due to the constant development of Internet-based platforms. Thus, law enforcements, policies, practices and necessary measures should continue developing contemporarily to the development of computer technology.***

Keywords: Cyber terrorism, Artificial Intelligence (AI), Monitoring, Using and Disrupting (M.U.D).

I. INTRODUCTION

Cyber terrorism has become popular in recent years, especially with the rapidly developing technology and the increasing dependence of the human race on the internet and social media. Although cyber terrorism has been acknowledged as a major risk internationally, there does not seem to be an agreed or universal definition of cyber-terrorism (Dogrul, Aslan and Celik, 2011). Many researchers have cited the definition by Denning (2000); whichdescribes cyber terrorism as "the convergence of cyberspace and terrorismwhere unlawful attacks and threats of attack against computers, networks, and the information stored therein are carried out to intimidate or coerce a government or its people in furtherance of political or social objectives, and should result in violence against persons or property, or at least cause enough harm to generate fear". Though this forms a reasonable definition of cyber terrorism at that point in time, it is crucial that international efforts re-assess the scope and the development of mechanisms behind cyber terrorism to ensure that legislations by itself do not create loopholes for cyber terrorists.

Manuscript published on 30 January 2019.
***Correspondence Author(s)**
Suhannia Ponnusamy, Asia Pacific University of Technology and Innovation, Malaysia.
Geetha A. Rubasundram, Asia Pacific University of Technology and Innovation, Malaysia.

The above definition implies that cyber terrorism is only valid if it damages the confidentiality, integrity and availability (CIA) of the computers, networks and information stored; as well as cause violence or some sort of harm. However, in the modern environment, terrorists also use cyberspace and electronic devices to communicate, plan, carry out attacks, obtain funding, arms procurement, intelligence gathering and toattract supporters. In 2000, an individual hacked and took charge of Australia's waste management control system, Maroochy Shire and remotely released millions of gallons of raw sewage (Prasad, 2012). Increasing numbers of terrorist groups such as the Islamic State of Iraq and Syria(ISIS) and Al-Qaeda, have used the Internet as a medium to promote their cause and conduct of terrorist operations (Hoffman and Schweitzer, 2015). The groups had successfully attracted large number of followers, donors and supporters due to its strong propaganda's; especially reaching out to youths craving for adventure and purpose. The groups use many different fronts to hide their true identity and activities, including using the anonymous protection of the Deep and Dark Web, hiding behind religious and other non-profit oriented bodies etc. It is also intertwined with other illegal activities including money laundering, corruption and organized crime. This causes further dilemmas since the crime can be perpetrated from any part of the world, hidden beneath many layers of activities and individuals. . Hence, it is imperative that all manners to perpetrate this crime is monitored and mitigated.

Though governments have stepped up security measures including online monitoring, there have been many hurdles in their endeavors. Aly et al (2016) acknowledges that cyber terrorism has commonly been misinterpreted with other similar cyber threats due to its limited branch of knowledge and the ridicule of the danger it poses enhances the risk it poses from cyber-attacks. Conflicting or narrow legislations and regulations can disrupt investigations and litigations.Privacy and Data Protection clausesprovide companies such as Whatsapp, Apple and others that use encryption to protect the privacy of their users has caused many disruptions to investigations and the litigation process.Concerns over stringent legislations also can cause unease amongst the public. In 2017, Amber Rudd, the UK Home Secretary expressed her intention to change the law to increase the penalty of 10 years to 15 years imprisonment for persons who repeatedly view terrorist content online, though with sufficient measures to protect members of the public with the defence of reasonable excuse (Casciani, 2017). The news report also quoted a case where the suspect could not be charged with terrorism, purely since it was required that the material be downloaded and saved, and the suspect had only streamed bomb making videos.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Likewise, news reports of increasing users of The Onion Router (TOR) as compared to other browsers due to privacy concerns and anonymity preferences also enhance the risk of cyber terrorism. TOR is also a gateway to the Dark and Deep Web, including aspects of Crimeware-as-a Service (CaaS) and other organized crimes. The increased use of cryptocurrencies also aids the movement and laundering of funds.

Education and exposure are necessary to mitigate this risk. The increasing number of global internet penetration, lack in security awareness among users and the increase in dependency on online communications is reducing the possibilities of combating cyberterrorism (Jalil, 2003).Respective bodies have been constantly striving to ensure that the threat is under control and it does not affect the citizens or the state of country (Prasad, 2012). Government sectors from all over the world have initiated new systems, programs, policies, stringent laws and various other actions in order to combat the threat of cyberterrorism. However, it is a challenging battle as it continuously needs to be updated and monitored, as the threats themselves develop and grow. Governments, companies and individuals need to be vigilant as the threats could impact their businesses, information, privacy and ultimately their security, caused by their vulnerable computer networks and systems as well as employees or vendors under guise.

Therefore, this paper assesses the perception of the knowledgeable members of public about the risk of cyber terrorism in line with the various efforts and mechanisms available to combat this crime. In order to provide a more robust discussion based on the findings of this research, this paper has been organized as follows: Section 2 discusses the relevant literature, Section 3 the research instrument used, followed by Section 4 which discusses the results and finally, Section 5concludes the overall perspective of this paper.

II. LITERATURE REVIEW

A. Perceived Risk Of Cyber Terrorism

Cyber terrorism lies in between a thin line of becoming a virtual bomb yet not as life threatening as an actual bomb (Lawson, 2002). The risk of cyber terrorism may not seem to as serious as it sounds but it is actually a matter of protecting national security. Being more politically motivated, cyber terrorism is keener towards damaging the critical infrastructure of a country which indirectly relates to effecting the general public in terms of disrupting financial and commercial infrastructure, taking charge of controls of dams and even having access to medical records (Alqahtani, n.d.). Due to the political coordination, the people are facing cyber terrorism effects in reality (Janczewski and Colarik, 2008).These disruptions is sufficient to generate enough fear towards the public and it enables cyber terrorists groups to remotely handle the operations of the country. For instance, attacks could cause water disruptions if cyber terrorists have control over dams,causing water shortage and suffering. Although it may not sound as a serious issue and rather far-fetched, but the risk should be constantly monitored (Alqahtani, n.d.).

Although the public is aware of cyber terrorism through reports in the media, they are still not as informed or knowledgeable in the technicalities of the operations and damage, due to the lack of information and awareness. Studies have shown that the perceived risk of cyber terrorism is relatively low during periods of elevated cyber terrorism attacks (Sjoberg, 2004). Citizens maybe unaware of the red flags ofcyber terrorism due to the complexity and fast paced development of the methods used. It is difficult to predict where and when an attack is going to occur. However, it is possible to minimize the risk by examining the areas that may attract cyber terrorism attacks because the goal of this emergence is to gain access without being detected and to cause intense fear and harm to anyone in the affected (Murrill, 2011).

Fear is the main driver of cyber terrorism as it causes behavioral changes which destabilizesa country's political and economic system, by impacting stock markets, consumer habits and long term financial decisions such as the changes in prices of real estate due to the increase in terrorist incidents in a particular area. Thus, political instability is capable of affecting the local economy as well as the global investment economy. Therefore, the stability of a country's economic and political system should be less vulnerable (Dombe and Golandsky, 2016). The critical infrastructure of a country is said to be the backbone for success. The risk of cyber terrorism attacks towards a nation's critical infrastructure is extremely high. Due to its vulnerability and complexity, damages posed towards a nation's infrastructure could destroy the development of the country (Dombe and Golandsky, 2016). Governments are discovering the needs to protect their information system and critical infrastructure systems in regards to the increasing threat of cyber terrorism. However, many restrictions does not allow completely bringing down the internet as there are various legal issues significantly related. The anonymity of attacker makes it even difficult to identify and prosecute the intruder as numerous geographical and legal restrictions are challenged.

B. Measures to Mitigate the Risk of Cyber Terrorism

While the Internet is the largest single component of cyberspace, connected in nearly more than 200 countries with more than 1 billion users globally, the probability for cyber terrorism to occur through the Internet rises drastically because the internet is built upon national and international telecommunications infrastructures which includes landlines, wireless and satellite communications (Goodman, 2007). Cyber terrorists target system could include a country's critical infrastructure which compromises of telecommunication system, transport system, power grid system, utility system and other significant systems that are required to run a country (Prasad, 2012). Thus, if these systems are destructed, then a whole nation can be destroyed in terms of economic and social wellbeing.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The complexity of a country's infrastructure increases the risk of cyber terrorism if it is without the presence of any defense mechanism to protect it against cyber terrorist attacks (Prasad, 2012).

Governments should enhance and harmonise the relevant legislations in their countries with international standards and strictly adhere to having a zero tolerance policy towards cyber terrorism, whilst acknowledging the need for privacy and human rights. Educating members of the public about cyber-terrorism is a must, including providing accessible and accurate information on vulnerabilities, threats and incidents as well, as expected behavior and providing access to officials to address concerns or report suspicious behaviours. This is not just contained to members of the public as individuals, but also organisations who play a key role in monitoring their employees, carrying out background checks and other human resource policies apart from improvising their information security measures in a timely manner. Various online materials are also available for further understanding about the threat of cyber terrorism and also on how to protect the computer from being attacked (Sundaram, 2008). Hence, the key to combatting cyber terrorism is education and public-private partnerships.

Security policies and comprehensive planning to act as a defense mechanism against cyber terrorism attack should be established in organisations (Goodman, 2007). The developed security practices should cover all aspects involved in the information system which could be done by adopting the international standard guidelines on information security. By complying with computer security policies, cyber terrorists would find it difficult to penetrate into a computer system and thus lowers the risk of cyber terrorism to incur (Dogrul, Aslan and Celik, 2011). Implementing security applications in computers makes is harder for cyber terrorism attacks to penetrate since it is time consuming for the cyber terrorists to break into these bridge (Goodman, 2007). These security applications should be updatedfrequently, with boards and managements understanding and acknowledging the urgent necessity and rationalizing the cost incurred for the longer term sustainability of the firm. However, sadly, many firms avoid live "fire drills" involving their own computer systems to check on loop holes that may attract cyber terrorist attacks because it is expensive and it has to be done on their own risk.

A crucial characteristic of cyber terrorism that needs to be addressed is its borderless exposure, anonymity and reduced risk, which in turn motivates the terrorist. A terrorist could plan an attack miles away without leaving home and having a lesser chance of being caught. The current limitation of legislations within jurisdictions is a crucial angle that needs to be enhanced. There is an urgent necessity to harmonize legislations internationally, with more countries cooperating through mutual legal assistance and extradition treaties. International cooperation is required to be developed in regards to controlling cyber terrorism because cyber terrorism is a global issue which involves the government of a country and worldwide organisations that adopt network information systems (Sundaram, 2008). Collaborating with other countries could be initiated through economic tools by forming and promoting common standards for international trade that will attract mutual understanding between countries as well as control the risk of cyber terrorism (Tereshchenko, 2013). Governments, especially those known to harbour or provide safe havens for cyber terrorists have to mutually develop strong international cooperation, information exchange and initiate shared trainings to control the risk of cyber terrorism (Sundaram, 2008). This can be further facilitated by a more active participation from global institutions. The Council of Europe (CoE) Convention of Cybercrime initiated the very first international statement on crimes committed through the Internet and other computer networks. The European Union had also taken certain steps against controlling the illegal contents on the Internet by protecting intellectual property and personal data, promoting electronic commerce and tightening the security of transactions (Dogrul, Aslan and Celik, 2011).

The presence of an active defense system such as the transnational surveillance system is an important element of the mitigating system. It could provide key information on the identity of the terrorist, initiate a counter mechanism and other pro-active steps to combat the risk. However, controversially, although this would infringe the privacy rights of the public, this is still being used by many countries, and would require international collaboration to fully function. One such system is the ECHELON used by countries such as Australia, United Kingdom and New Zealand, which has the ability to capture intelligence information across the globe using a surveillance system designed to filter messages and telephone conversations through a computer system which is able to identify keywords and phrases (Che, 2007). Australia's Defence Signals Directorate (DSD) uses this surveillance system to monitor Indochina, Southern China and Indonesia whereas The United Kingdom's Government Communications Headquarters (GCHQ) uses this surveillance to monitor Europe, Russia and Africa. New Zealand's Government Communications Security Bureau (GCSB) uses this system to monitor the Western Pacific region (Che, 2007).

Another approach that requires international cooperation is the M.U.D approach, which stands for Monitoring, Using and Disrupting. The Monitoring and Using steps can be used to analyse the radicalization process of the terrorist organization in order to come up with solutions for de-radicalize the situation. Disrupting steps can be used by infecting the terrorist websites to destroy or change the contents of the website. It is more of a reverse action done in order to lower the risk of cyber terrorism attacks. However issues arise when different governments have conflicting goals where some may still want to monitor blogs, chat groups etc. and the other ready, to disrupt. This method also assists to identify countries that aid and abet terrorists (Dogrul, Aslan, Celik, 2011).

Due to the increased surveillance and legislations in place, many individuals look for options to protect their privacy even though it may not be with criminal intent. Tools such as encryption techniques, the use of browsers and software to protect their anonymity just make it harder for officials to monitor real threats, especially with the increased traffic using these tools.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Likewise, with easy access to information to carry out cyber terrorism as terrorist groups are using the net and social media to expand their network, it is crucial that these surveillances are updated. Businesses and individuals that provide Crimeware-as-a-Service (CaaS) as well further complicate the process to detect. A possible solution would be to use Artificial Intelligence (AI). AI is an innovative and logical approach that simulates human intelligence in machines, using conventional fixed algorithms, enabling it to make decisions and adapting to their environment since it is able to self-tune, self-configure, self-manage, self-diagnose and self-heal. AI methods seems to provide a more promising outcome in lowering the risk of cyber-attacks and increasing the security of cyber-space (Dilek, Cakir and Aydin, 2015). AI features that have been implemented in software's that combat cyber-attacks include Computational Intelligence, Pattern Recognition, Intelligent Agents and Neural Networks and can be applied to detect and prevent intrusions, denial of service, spams, malwares and assist in forensic investigations (Dilek, Cakir and Aydin, 2015).

III. METHOD & MATERIALS

This paper assesses the influence of tools and mechanisms to mitigate cyber terrorism on the perception of risk of cyber terrorism. In order to assess the relationship, a questionnaire based on a five point Likert Scale was sent out to respondents globally, with the pre requisite that they must have working knowledge in cyber terrorism. A total of 550 questionnaires was circulated and 153 responses received. After eliminating incomplete responses, only 100 respondents were included for the data analysis.

IV. RESULTS AND DISCUSSIONS

All 100 respondents affirmed the pre-requisite of having working knowledge of cyber terrorism. 25% of the respondents were below the age of 25, 15% between the ages of 26 and 35, 36% between the ages of 36 and 45, and 22% above the age of 45. The results shows that 29% of respondents has less than 5 years of working experience, 25% of respondents has more than 5 years but less than 10 years of working experience and remaining 46% of respondents has been employed for more than 10 years.

The Pearson Correlation Test as reflected in Table 1 below indicates that the mitigation mechanisms and tools have a positive significant correlation with the perception of risk on cyber terrorism, as the value of Sig (2-tailed) is 0.002 which is below 0.05 and the r value is 0.300 indicating a positive significant correlation.

Table 1: Correlations

Correlations		
	DV-Perception of Risk	IV – Mitigation
DV Pearson Correlation	1	.300**
Sig. (2 tailed)		.002
N	100	100
IV Pearson Correlation	.300**	1
Sig. (2 tailed)	.002	
N	100	100
** Correlation is significant at the 0.01 level (2-tailed)		

Source: SPSS

Overall, seven (7) key results were prominently agreed by the respondents.

A. General

a) 92% agreed that mitigation mechanisms and tools impact the perceived risk of cyber terrorism, since it lowers the vulnerability of systems and networks.

B. Perception of Risk

b) 87% of the respondents agreed that cyber terrorism poses a real threat

c) 88% agreed that cyber terrorism threatens the safety of an individual by inculcating intensive fear due to its effect on cyber-security.

d) 86% agreed that technology and the loopholes it provides caused an increase in cyber terrorism attacks

C. Mitigating Mechanisms and Tools

e) 81% agreed that a secured mechanism was important to combat the increasing frequency of global cyber terrorism attacks.

f) 92% agreed on the prominence of the roles of global institutions, governments and relevant bodies in combatting cyber terrorism.

g) 95% agreed that international cooperation could be used in combatting cyber terrorism.

The above results imply that there have been some changes in perception, knowledge and mitigating mechanisms and tools over the years. Sjoberg (2004) found that 83% of respondents showed no signs of panic following the 9/11 incident and heightened cyber-attacks, and only increasing by 5% in 2003. The study also found that citizens were more likely to become more concerned about the risk of cyber terrorism 9 months after the attacks. In contrast, this research reflects that more than 80% of the respondents are concerned about the risk of cyber terrorism and consistently seem to agree on the various scenarios, mechanisms and tools that have been proposed. Of course, there would be an expected gap in terms of the two results, since one focuses on the general public and this research on individuals with working knowledge in cyber terrorism. However, there has also been increased efforts to educate the public on the risks of cyber terrorisms and the modus operandi to look out for and avoid. Comprehensive education programs are also essential for officials' body in terms of securing a country's critical infrastructure. Since critical infrastructure and computer networks are highly targeted in the United States among all other countries, trainings are provided for technical personnel and managers that are responsible in monitoring and protecting the country's critical infrastructure. The Cyber terrorism Defense Initiative (CDI) includes Comprehensive Cyber terrorism Defense (CCD) and Cyber terrorism First Responder (CFR) program prepares technical personnel to minimize the risk of cyber terrorism attacks and to effectively respond towards any cyber-based terror attacks (Cyber Terrorism Defense Initiative, 2016).

Likewise, Prasad (2012) also supports the need for a coordinated and robust international framework to combat cyber terrorism, and urges the need to for governments and regulators to stop working in silo in order to be able to share intelligence and other forms of cooperation.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Hence, it would also be important to incorporate tools such as AI, M.U.D. and other forms of surveillance to reduce the vulnerability from cyber terrorism (Dogrul, Aslan and Celik, 2011).

V. CONCLUSION

It can be concluded that, the threat of cyber terrorism attacks will constantly increase as people are becoming dependent upon the internet and therefore increasing the possibilities of cyber terrorism attacks. Terrorists such as ISIS are successfully creating a powerful image towards the perception of the public globally. The threat of attacks continuous to grow as the widespread of online users are constantly increasing. The risk of cyber-attacks to incur increases along with the rapid growth of computer technology. Thus, law enforcements, policies, practices and necessary measures should continue to be developing as the computer technology continuous to develop. It is the responsibilities of officials to develop a safe technology which is able to determine suspicious activities by analyzing public and private data (Bogdanoski and Petreski, 2013). Implementations of all these mechanisms allows computer network and systems to be less vulnerable and manages the risk of cyber terrorism because each mechanisms possess separate functions for combatting cyber terrorism. Even though various defence mechanism has already been established, the threat of cyber terrorism continues to increase due to the constant development of Internet-based platforms.

REFERENCES

1. Alqahtani, A. (n.d.). The Potential Threat of Cyber-terrorism on National Security of Saudi Arabia. 1st ed. [ebook] Department of Politics and International Studies the University of Hull - UK. Available at: http://www.academia.edu/8951385/The_Potential_Threat_of_Cyber-terrorism_on_National_Security [Accessed 19 Sep. 2016].
2. Aly, A., Macdonald, S., Jarvis, L. and Chen, T. (2016). Violent Extremism Online: New Perspectives on Terrorism and the Internet. 1st ed. [ebook] New York: Routledge, pp.18-21. Available at: https://www.book2look.com/embed/9781317431879 [Accessed 5 Sep. 2016].
3. Balkhi, S. (2013). 25 Biggest Cyber Attacks In History. [online] Available at: http://list25.com/25-biggest-cyber-attacks-in-history/ [Accessed 24 Dec. 2016].
4. Bogdanoski, M. and Petreski, D. (2013). CYBER TERRORISM–GLOBAL SECURITY THREAT. 1st ed. [ebook] Research Gate. Available at: http://file:///C:/Users/Win%208.1/Downloads/CYBER%20TERRORISM-%20GLOBAL%20SECURITY%20THREAT%20-%20Mitko%20Bogdanoski.pdf [Accessed 24 Dec. 2016].
5. Casciani, Dominic (2017), Longer Jail Terms for Viewing Terror Content Online. BBC Available at: https://www.bbc.com/news/uk-41479620 [Accessed on 27th Sept 2018)
6. Che, E. (2007). Securing a Network Society Cyber-Terrorism, International Cooperation and Transnational Surveillance. [online] Available at: http://rieas.gr/images/RIEAS113ELIOTCHE.pdf [Accessed 10 Sep. 2016].
7. Cyber terrorism Defense Initiative. (2016). [online] Cyberterrorismcenter.org. Available at: http://www.cyberterrorismcenter.org/ [Accessed 23 Nov. 2016].
8. Dawson, M., Omar, M. and Abramson, J. (2015). Understanding the Methods behind Cyber Terrorism. Research Gate, [online] 3, pp.1539-1549. Available at: http://www.saintleo.edu/media/972036/understanding_the_methods_behind_cyber_terrorism.pdf [Accessed 5 Sep. 2016].
9. Dilek, S., Cakır, H. and Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications, [online] 6(1), pp.21-39. Available at: http://aircconline.com/ijaia/V6N1/6115ijaia02.pdf [Accessed 17 Dec. 2016].
10. Denning, Dorothy E. (2000). Cyberterrorism: Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism
11. Dogrul, M., Aslan, A. and Celik, E. (2011). Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. 3rd ed. [ebook] Istambul: CCD COE Publications. Available at: https://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pdf [Accessed 5 Sep. 2016].
12. Dombe, A. and Golandsky, Y. (2016). A Review and Analysis of the World of Cyber Terrorism. 1st ed. [ebook] Available at: http://www.cyberisk.biz/cyber-terrorism-review-and-analysis/ [Accessed 23 Nov. 2016].
13. Goodman, S. (2007). Science and Technology to Counter Terrorism.Cyberterrorism and Security Measures. [online] Available at: https://www.nap.edu/read/11848/chapter/6 [Accessed 5 Sep. 2016].
14. Hoffman, A. and Schweitzer, Y. (2015). Cyber Jihad in the Service of the Islamic State (ISIS). [online] www.inss.org.il. Available at: http://www.inss.org.il/uploadImages/systemFiles/adkan18_1ENG%20 (5) _Hoffman-Schweitzer.pdf [Accessed 5 Sep. 2016].
15. Hyde, O. (2011). MACHINE L EARNING FOR CYBER S ECURITY AT NETWORK SPEED & SCALE. 1st ed. [ebook] AI-One Inc. Available at: http://www.academia.edu/1026724/Machine_Learning_for_Cyber_Security_at_Network_Speed_and_Scale [Accessed 14 Dec. 2016].
16. Jalil, S. (2003). Countering Cyber Terrorism Effectively: Are We Ready To Rumble? 1st ed. [ebook] SANS Institute. Available at: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154 [Accessed 4 Sep. 2016].
17. Janczewski, L. and Colarik, A. (2008). Cyber Warfare and Cyber Terrorism. 1st ed. [ebook] New York and Hershey: Information Science Reference. Available at: https://books.google.com.my/books?hl=en&lr=&id=XWK9AQAAQBAJ&oi=fnd&pg=PA1&dq=cyber+terrorism+cases&ots=27XIC8yumj&sig=4r2Npu9JU4yVd8U70t8cYkVQa-E&redir_esc=y#v=onepage&q&f=false [Accessed 14 Aug. 2016].
18. Murrill, R. (2011). The Question of Cyber Terrorism. [online] Forensic Focus - Articles. Available at: https://articles.forensicfocus.com/2011/07/23/the-question-of-cyber-terrorism/ [Accessed 5 Sep. 2016].
19. Prasad, K. (2012). Cyber terrorism: Addressing the Challenges for Establishing an International Legal Framework. 1st ed. [ebook] Perth: Edith Cowan University. Available at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act [Accessed 5 Sep. 2016].
20. Santiago, J. (2015). Top countries best prepared against cyber attacks. [online] World Economic Forum. Available at: https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/ [Accessed 24 Dec. 2016].
21. Sjöberg, L. (2004). THE PERCEIVED RISK OF TERRORISM. [online] Available at: http://swoba.hhs.se/hastba/papers/hastba2002_011.pdf [Accessed 19 Dec. 2016].
22. Sundaram, S. (2008). Cyber Terrorism: Problems, Perspectives, and Prescription. [online] Academia.edu. Available at: http://www.academia.edu/812094/Cyber_Terrorism_Problems_Perspectives_and_Prescription [Accessed 5 Sep. 2016].
23. Tereshchenko, N. (2013). US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure. [online] E-International Relations. Available at: http://www.e-ir.info/2013/06/12/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/ [Accessed 9 Sep. 2016].

AUTHORS PROFILE

Suhannia Ponnusamy is working in Asia Pacific University of Technology and Innovation, Malaysia.

Geetha A. Rubasundram is working in Asia Pacific University of Technology and Innovation, Malaysia.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)