Sci Eng Ethics (2019) 25:993–1006
DOI 10.1007/s11948-016-9864-0

ORIGINAL PAPER

Cyber Attacks and Terrorism: A Twenty-First Century Conundrum

Marwan Albahar[1]

Received: 15 February 2016 / Accepted: 19 December 2016 / Published online: 5 January 2017

Abstract In the recent years, an alarming rise in the incidence of cyber attacks has made cyber security a major concern for nations across the globe. Given the current volatile socio-political environment and the massive increase in the incidence of terrorism, it is imperative that government agencies rapidly realize the possibility of cyber space exploitation by terrorist organizations and state players to disrupt the normal way of life. The threat level of cyber terrorism has never been as high as it is today, and this has created a lot of insecurity and fear. This study has focused on different aspects of cyber attacks and explored the reasons behind their increasing popularity among the terrorist organizations and state players. This study proposes an empirical model that can be used to estimate the risk levels associated with different types of cyber attacks and thereby provide a road map to conceptualize and formulate highly effective counter measures and cyber security policies.

Keywords Cyber terrorism · Cyber attack · Terrorism · Counter measure · Risk prediction

Introduction

Battlefields of the twenty-first century are no longer limited by geographical boundaries and thanks to the phenomenal development in information and communication technologies, "virtual" threats have suddenly become very real. The World Wide Web that is intricately interwoven over every aspect of human lives today adds to the picture a whole new dimension to the covert military operations that are carried out to protect lives and safeguard national interests. In the

✉ Marwan Albahar
marwanalialbahar@gmail.com

[1] School of Computing, Kuopio Campus, University of Eastern Finland, P.O. Box 1627, 70211 Kuopio, Finland

last decade, almost every organization, both government and private have become dependent on information technology for their day-to-day operations and this has massively increased the threat levels.

In order to fully comprehend the dynamics of modern day cyber attacks it is important to understand the unique dimensions of the cyber space. Since the cyber space environment is not limited by any conventional boundaries or borders, clandestine cyber attacks can be carried from thousands of miles away at unbelievable speeds. Such attacks can easily be carried out by an individual or a group of individuals with computers, sitting safely in their living rooms without the need for a huge physical army on the ground. The damage from such cyber attacks can be as deadly as any conventional warfare, if not more, so the possibility of such assaults has never been as high as today. There are several aspects or factors that have contributed to the massive increase in cyber attack threats across the globe and the most prominent one is the ubiquity of the Internet. As organizations go for new software upgrades and installations new vulnerabilities and weaknesses emerge that can be exploited by cyber terrorists. The tools that are necessary to carry out an effective cyber attack can even be downloaded from the Internet and there is no need for lengthy and expensive acquisitions and training. It is not wrong to comment that today a simple personal computer can actually be used as a more effective weapon than a conventional gun. A terrorist organization with limited manpower and infrastructure can launch cyber attacks from any location and can cause massive loss, be it infrastructure, finance or human life. James Lewis from the Center for Strategic and International Studies appropriately defines the threat of cyber attacks in the twenty-first century as "a massive electronic Achilles' heel" (Lewis 2002). In order to properly understand the dynamics of cyber attacks and cyber terrorism it is important that the reasons behind their popularity among the terrorists are thoroughly comprehended. Cyber attacks can cause extensive damage at tremendous speeds and in little time. In essence, the outreach of such attacks is massive and the level of publicity that an organization mounting such an attack is enormous. Given the extensive dependence on information technology today, legitimate organizations also bend under a constant fear of becoming the target of malicious agents. All of these make the paradigm of cyber attacks extremely attractive for terrorists. The popular culture has also contributed immensely in creating the paranoia surrounding cyber attacks where scenarios such as terrorists taking control of the air space and nuclear installations and wreaking havoc on millions are routinely publicized and narrated. It will also be prudent to ascertain if the threat of cyber attacks is as real and imminent as is projected by the print and electronic media. As Weimann puts it, virtually every major government, defence and private infrastructure in the west are highly networked and depend heavily on computers (Weimann 2005). Even though this makes operations extremely smooth and agile the possibility of cyber attacks also increases many fold. Terrorist organizations can exploit the loopholes in the network and can launch massive attacks on financial and military installations and can hold an entire nation to ransom. While information technology has significantly improved the quality of life, the tradeoff comes in the form of the increasing vulnerability of major installations to such attacks. These observations clearly establish that the perceived levels of

threat surrounding cyber attacks are not unfounded and there is a clear necessity for robust policies to ensure that such attacks never happen. This paper attempts to present an insight surrounding the possibility of cyber attacks in the present day and in the future and thoroughly examines the different aspects and dynamics of cyber attacks and cyber terrorism. Section "What is a Cyber Attack: The Inherent Types and Dynamics" of the **paper presents the concept and the architecture of cyber attacks in detail with appropriate evidence to previous research. Section "The Rising Possibility/Popularity of Cyber Attacks" of the paper focuses on the reasons behind the increasing popularity of cyber attacks among modern day terrorist organizations and presents a critical analysis of the vulnerabilities that can be exploited. A wide range of credible journal publications and articles are examined to highlight and establish the fears and the possibilities of cyber attacks and ascertain if there are any solid reasons for concern. Section "Empirical Examination of Terrorism and Cyber Attacks: Insights from Past Research" of the paper draws up information from different empirical studies carried out in the past that explore the conjunction between cyber attacks and terrorism. An empirical model to ascertain the level of risk is also presented based on some recent cyber attacks from across the globe. Section "Conclusion and Future Direction" sums up the paper with a conclusion that is directed towards the future and proposes a strong argument in favor of constant vigil and policy changes to effectively deal with the real threats without falling victims to paranoia and unwarranted fears.

What is a Cyber Attack: The Inherent Types and Dynamics

The concept of a cyber attack is relatively modern and it encompasses a wide range of nefarious activities that can be carried by exploiting the capabilities of sophisticated information and communication technologies available today. A type of attack carried out in the cyber space that has become significantly popular and common in recent times is the Distributed Denial of Service attack. During this type of attack, the server that is the target is swamped with data traffic to such an extent that legitimate access to a particular portal or website becomes impossible. A prominent cyber attack incident took place at the Natanz uranium enrichment plant in Iran that resulted in the massive failure of centrifuges that were used for the enrichment of uranium. The agent that was responsible for this attack is popularly known as the Stuxnet worm which was essentially malware targeting the control system of the Iranian nuclear installation. Many consider this entity as the first cyber weapon and it was clearly able to demonstrate the possibilities and the capabilities of modern day cyber warfare. A Congressional research service report released in 2015 states that the threat levels of terrorism in cyber space have increased significantly in the present day and the possibility of the premeditated use of information and communication technologies to cause harm and achieve political and ideological objectives have become real (Theohary and Rollins 2015). When it comes to attacks in cyber space, criminal entities and terrorist organizations depend on the state-of-the-art information technologies and they represent a wide range of affiliations. Perpetrators of cyber attacks can be terrorist organizations that are

covertly state-sponsored or supported by an organization with specific religious, political or cultural ideologies. Islamic terrorist organizations that have declared a holy war or "Jihad" against the west have routinely used the Internet to spread their ideologies, brainwash their recruits, plan their subversive activities and disrupt normal ways of life (Rollins and Wilson 2007). Even Though there is no formal report from the government on cyber attacks that have crippled a major infrastructure in the United States, the probability of the same is definitely not a myth as it was shown by the Department of Homeland Security in 2009. The department carried out an elaborate experiment where they demonstrated the effectiveness of a sophisticated cyber attack by crippling the control systems of the power grids. The called the experiment the Aurora Project and that eventually caused complete destruction of the grid power equipment (Kerr et al. 2009). Even though this was a controlled experiment carried out by the department of homeland security, it laid bare the possibilities and the vulnerabilities that lie within critical national infrastructures. For this reason a major concern for the United States government today is how to safeguard the national interests from falling victim to debilitating cyber weapons (Rustici 2011). To address this threat the American government defines any form of cyber attacks on its critical infrastructure as serious national security concerns and have even declared cyber space as a war domain (O'Harrow 2013). Government agencies and researchers who are closely following the rising trends and frequency of cyber attacks have constructed a range that defines the severity of such attacks in terms of the damage they cause. While intrusions in the form of spam mails or distributed denial of service attacks are considered low in severity, other state-of-the-art intrusions that are carried out by sophisticated cyber agents to penetrate protected government, defence or financial cyber spaces and disrupt their activity are considered as high in severity (Rid and McBurney 2012). Even though it has been firmly established that the possibilities of debilitating cyber attacks are immense, there has not been such an attack yet that has caused complete breakdown of power grids or collapse of financial markets or led to massive loss of human lives. This has led some observers to express certain levels of cynicism with regards to linking cyber attacks with the conventional definition of terrorism. According to them, cyber attacks can and will only lead to minor disruption and that they are not capable of inflicting damage at the levels of conventional nuclear, biological or chemical weapons. Others contradict and this believe that given the overwhelming reliance of virtually every major infrastructure on the virtual network, cyber attacks can bring about sufficient damage in the form of financial loss, psychological impact and even loss of human lives that would qualify them as major acts of terrorism. In a Congressional Research Service report, Wilson describes two forms of cyber attack that can be ascribed to an act of terrorism, in other words, cyber terrorism. When computer mediated attacks cause a negative psychological impact on the masses like conventional acts of terrorism it is defined as effect-based cyber terrorism. Similarly, when computer or network-based attacks are carried out to achieve a political or ideological objective it is called intent-based cyber terrorism (Wilson 2003). Clarke, a former national security advisor to the U.S. government states that if under any circumstances a terrorist organization decides to launch a cyber attack against the United States it will most

probably be an intent-based attack directed towards the financial institutions and any damage to infrastructure or loss of people's lives will be secondary events (Rademacher 2005).

In 2007, the cyber attacks that were targeted towards the European Nation of Estonia cannot be written off as a minor incident of cyber nuisance. On the contrary it needs to be visualized as a serious form of violence that can disrupt the normal way of life and jeopardize critical institutional functionality. The Estonian defence ministry actually equates the damage from such an attack with the loss that could occur if all the ports of a country are permanently shut down (Herzog 2011). In essence, an attack such as this could take the form of a serious economic and information blockage leading to the complete breakdown of not just public infrastructure facilities and financial institutions but also defence establishments. A major reason why such an attack could take place was the lack of adequate cyber defence preparedness of the Estonian Government and the involvement of state players. This incident clearly indicates the emerging seriousness of cyber attacks and cyber terrorism in the twenty-first century and the growing necessity for tools to predict such attacks.

Information and communication technologies have surely improved the quality of life significantly but in the present context, the threat of cyber terrorism has been raised many fold as a trade-off to globalization and smooth information exchange (NATO 2010). The attack against Estonia has clearly shown that a powerful army on the ground or a state-of-the-art nuclear defence shield is no guarantee that institutional sovereignties are not under threat in cyber space. In this context it has become critically important for governments across the globe to ensure that robust early warning protocols are in place and a vigilant cyber monitoring policy is in place as people continue to enjoy the fruits of increasing cyber freedom. Researchers such as Denning and Weimann are of the opinion that cyber terrorism is a real threat at the present time. While Denning talks about the disruption of services and critical infrastructure through targeted cyber attacks Weimann focuses on the use of cyber space by terrorist organizations to radicalize people and carry out recruitment drives (Denning 2001; Weimann 2008). There is still no clear picture when it comes to formally defining a cyber terrorist and different nations adopt different strategies to deal with the problem but with regards to cyber attack threat perceptions, every nation across the globe fully realizes it potential for damage.

The Rising Possibility/Popularity of Cyber Attacks

Threats of attacks in cyber space have risen dramatically in the last two decades and during this period the perpetrators have graduated from individual hackers to well-organized terrorist organizations and even legitimate states. This is truly the age of the Internet and social media and societies from across the globe have never been as connected and intertwined as they are today. Even though this has made it incredibly easy for the government to connect with the masses facilitate avenues for collective governance terrorist organizations are also not lagging behind in using the

medium of the internet and social media to radicalize youth and bring more people into their fold (Dhs.gov 2015). The incredible outreach of the internet that transcends all kinds of borders and physical barriers is very appealing to the subversive organizations that intend to disrupt the fabric of society, cause harm to people and forward their ideological objectives. Bieda et al. carried out a study where they observed that social networks platforms are increasingly being used by extremist organizations to radicalize people without the need for any physical contact or coercing (Bieda et al. 2015). This not only allows them to achieve their objectives from a safe distance but also increases their horizon in a worldwide context. ISIS or the Islamic State of Iraq and Syria has become a mammoth terrorist organization in recent years and it has been observed that they have relied heavily on social media for the recruitment and sharing of ideologies. The organization has routinely tried to create fear in civilized societies by circulating video films of executions on platforms such as YouTube. As it would appear, organizations such as ISIS are extremely professional and effective when it comes to their engagement in the cyber space through different social media platforms. This has not just helped them in getting more recruits but has also brought them international attention (Bieda et al. 2015).

In order to fully appreciate the seriousness of cyber attacks and cyber terrorism and contribute resources for counter measures, organizations would naturally want to look at conclusive evidence that points towards an impending threat to their interests. However, the proper estimation of cyber threats is still not accurate and it may not always possible to say that an organization is under threat. This is where the relevance and significance of empirical studies become clearly evident. In essence, it will not be wrong to conclude that every organization will have information to guard against any weakness in cyber security that will make them vulnerable to compromise. Management of cyber attacks is a vital necessity in today's context and it is important that there are avenues available to help in the assessment of risks so that organizations can take a more targeted approach in protecting their assets. The following section highlights the importance of empirical studies on cyber attacks and cyber terrorism and presents a model that will help in acquiring an accurate estimate of risk associated with different types of cyber attacks.

Empirical Examination of Terrorism and Cyber Attacks: Insights from Past Research

In order to formulate robust policies against cyber attacks and cyber terrorism it is pertinent that decisions are properly backed-up by exhaustive empirical studies. While hypothetical situations can definitely give a direction towards a particular line of thought, over-reliance on assumptions, especially when empirical studies present highly contradictory evidence, can lead to disastrous consequences. Complete dependence on policies guided by hypothetical scenarios can lead to predicaments where government agencies might have the capability to deal with expected eventualities but may fare very badly when it comes to agile and effective mobilization of resources in the event of an actual disaster (Dynes 2006). Another

brilliant line of thought is to take a more cohesive approach when it comes to the formulation of effective cyber security policies. A cohesive approach would not just take into consideration the findings presented by empirical studies but will also draw on knowledge and information from other critical aspects such as socio-political dynamics, geography and finance, to name a few (Carr and Shepherd 2010; Lewis 2009). Given the current geopolitical situation of the world where terrorism is a burning issue and incidences of cyber terrorism are rising at an alarming rate, it is prudent that an empirical evaluation is carried out to know the actual perceptions of the threat.

The North Atlantic Treaty Organization (NATO) presents a list of recent cyber attacks that have been carried out against government organizations, defence agencies and financial establishments across the globe. This study will take these incidents into consideration and present a model that can be used to obtain a risk score for every type of cyber attack. Every cyber attack presented by NATO will be assigned a "threat" score and a "likelihood of occurrence" score and they will form a matrix to give an accurate assumption of the risk associated with a particular type of cyber attack. The "threat" and the "likelihood of occurrence" scores will be assigned on the basis of a wide range of factors presented in the tables below. To make the model more robust, an effort will be given to integrate the "vulnerability factor" but it needs to be noted that the recent cases of cyber attacks presented by NATO do have relevant data associated with vulnerability. The "threat" scores are calibrated on a 5-point scoreline depending on the seriousness and severity of the attack and similarly the "likelihood of occurrence" scores are calibrated on a 5-point scoreline depending on the technical competence required to carry out the attack. The "threat" and "likelihood of occurrence" scores are presented in tables below.

Empirical Examination of Terrorism and Cyber Attacks: Insights from Past Research

In order to formulate robust policies against cyber attacks and cyber terrorism it is pertinent that decisions are properly backed by exhaustive empirical studies. While hypothetical situations can definitely give a direction towards a particular line of thought, over-reliance on assumptions, especially when empirical studies present highly contradictory evidence, can lead to disastrous consequences. Complete dependence on policies guided by hypothetical scenarios can lead to predicaments where government agencies might have the capability to deal with expected eventualities but may fare very badly when it comes to agile and effective mobilization of resources in the event of an actual disaster (Dynes 2006). Another brilliant line of thought is to take a more cohesive approach when it comes to formulation of effective cyber security policies. A cohesive approach would not just take into consideration the findings presented by empirical studies but will also draw knowledge and information from other critical aspects such as socio-political dynamics, geography and finance, to name a few (Carr and Shepherd 2010; Lewis 2009). Given the current geopolitical situation of the world where terrorism is a

burning issue and incidences of cyber terrorism are rising at an alarming rate, it is prudent that an empirical evaluation is carried out to know the actual perceptions of the threat.

The North Atlantic Treaty Organization (NATO) presents a list of recent cyber attacks that have been carried out against government organizations, defence agencies and financial establishments across the globe. This study will take these incidents into consideration and present a model that can be used to obtain a risk score for every type of cyber attack. Every cyber attack presented by NATO will be assigned a "threat" score and a "likelihood of occurrence" score and they will form a matrix to give an accurate assumption of the risk associated with a particular type of cyber attack. The "threat" and the "likelihood of occurrence" scores will be assigned on the basis of a wide range of factors presented in the tables below. To make the model more robust, an effort will be given to integrate the "vulnerability factor" but it needs to be noted that the recent cases of cyber attacks presented by NATO does have any relevant data associated with vulnerability. The "threat" scores are calibrated on a 5-point scoreline depending on the seriousness and severity of the attack and similarly the "likelihood of occurrence" scores are calibrated on a 5-point scoreline depending on the technical competence required to carry out the attack. The "threat" and "likelihood of occurrence" scores are presented in tables below.

The Proposed Risk Estimation Model

Table 1 below illustrates the incidences of recent cyber attacks that took place across the globe. The threat and the likelihood of occurrence scores are presented in Tables 2 and 3 below.

As already mentioned, for every instance of cyber attack a threat and a likelihood score will be assigned on the basis of a ten-point scale. As seen in Table 2, the threat score will increase with the severity of the attack and similarly the likelihood of occurrence will be determined on the basis of the technical competence required to carry out the attack. The assignment of the threat and likelihood of occurrence scores is highly subjective and will depend on the perception of the experts assigning the score for an individual organization as per the score cards. To add more credibility to the model, the aspect of vulnerability is also integrated but it needs to be stated that the data obtained for the purpose of this study does not have adequate information on the vulnerability factor. This is not a major issue because vulnerability is once again subjective and will vary from organization to organization. There is however a vulnerability score card that will provide the roadmap to assigning the appropriate vulnerability scores to a particular cyber attack. The vulnerability score card is shown in Table 4.

The risk factor associated with a particular kind of cyber attack is estimated using the simple formula shown below:

$$\text{Risk} = \text{Threat score} \times \text{Likelihood of Occurrence score} \times \text{Vulnerability score}$$

Table 1 Recent cyber attacks from across the globe

Year	Cyber attack
1998	The Morris worm attack against the U.S. nascent cyber infrastructure. Carried out by Robert Tapan Morris who eventually became a professor at MIT
2006	E mail server threat at NASA. The organization was apprehensive that it might jeopardize their space shuttle launch
2007	A distributed denial-of-service (DDoS) attack against Estonian government agencies. Online services were temporarily disrupted but quickly restored
2007	Intrusion of the Pentagon network and disruption of the mail server accounts
2007	Compromise of the China Aerospace Science and Industry Corporation (CASIC) intranet network. Possible involvement of state players
2008	Intrusion of Georgian government agency networks. Possible involvement of organizations backed by a state player
2009	Compromise of the Israel's internet infrastructure. Possible involvement of terrorist organizations to weaken Israeli military offensive in Gaza at that time
2010	Disruption of service of the popular Chinese search engine called Baidu. Involvement of an organization called the Iranian Cyber Army
2010	The Stuxnet malware attack against the control systems installed at Iranian nuclear reactor facilities. Involvement of state players or state-sponsored organizations
2011	Cyber attack against Canadian government and defence agency networks. Possible involvement of non-state players
2012	An organized cyber attack against government and defence agency networks of Russia and Eastern European nations.
2013	Cyber attack against South Korean financial organization networks and national broadcaster called YTN. Possible involvement of a state player
2014	Attack against Sony Pictures servers to disrupt the release of the movie called the "interview". The attack was highly sophisticated in the sense that several datacenters of Sony pictures were completely compromised and all the data was lost. Possible involvement of North Korea behind the attack
2015	Malware attack against the webpage of the Court of Arbitration located in The Hague, The Netherlands. It is speculated that China may be behind the attack because it occurred during the hearing of the South China sea dispute
2015	Defacing of an official Indian password webpage. Possible involvement of a team of cyber attack experts from Pakistan who may or may not be getting state support
2015	Data breach at the South Korean executive office servers leading to compromise of information belonging to the members of South Korean Legislative Assembly members. Possible involvement of North Korean government agents
2015	A group called Anonymous Lebanon carried out a series of attacks against several Lebanon Government Websites and caused their defacement
2015	Serious data breach of U.S. State Dept.'s email systems forcing the government to shut down their systems. Possible involvement of Russian hackers that may or may not be backed by the Russian state

Value Determination of Different Model Factors

As observed above, all the three factors constituting the cyber attack risk estimation model is assigned a score. These scores are used in the equation to determine the risk underlying every form of cyber attack. The Threat, Likelihood of Occurrence

Table 2 The threat score card

Threat score	Threat type	Description of the perceived threat
1	Service disruption	Includes malicious intrusion of legitimate computer systems. Service disruption would also include distributed denial of service attacks
2	Subversive cyber activities	Includes more sophisticated intrusion of legitimate computer systems that would involve alteration of files and executables. This would also include defacing of legitimate websites
3	Cyber espionage	Involves well-skilled teams that work towards penetrating sensitive government or organizational servers to steal data
4	An act of sabotage	Compromise of systems that can lead to infrastructural damage causing severe loss of productivity or disruption of essential services
5	Full scale cyber conflicts	This can involve state players and would lead to major loss of human lives

Table 3 Likelihood of occurrence score card

Likelihood of occurrence score	Likelihood of occurrence type	Description of the perceived likelihood of occurrence
1	Lowest chance of occurrence	This type of attack would involve countries and would be highly sophisticated in nature
2	Little chance of occurrence	This type of attack may not involve entire states but individuals who are state-sponsored
3	Moderate chance of occurrence	This kind of attack would be carried by individuals or organizations that may or may not be state supported
4	Good chance of occurrence	This kind of attack would be carried out by skilled individuals or an organization that does not enjoy any support from any country. The attack would also involve software that is freely available on the internet
5	High chance of occurrence	This kind of attack will be carried out by ordinary individuals and would require minimal skill

and Vulnerability scores are determined on the basis of a scale that ranges from 1 to 5. A score of 1 indicates minimum severity and as it increases the degree of severity increases. A threat score of 5 indicates the most severe form of attack that might lead to severe damage to infrastructure or loss of lives. Similarly a likelihood of occurrence score of 5 is indicative of the fact that there is an extremely high chance that the attack is going to happen. A vulnerability score of 5 would mean that perpetrators of cyber attacks can very easily exploit the weakness in the system and could launch an attack.

Even Though the assignment of scores to the different factors is highly subjective and will depend on the perception of the experts assigning them for an individual organization, certain aspects need to be taken into consideration. When assigning a score for the threat factor it is important to consider aspects such as skill level of the attackers, the determination or the motivation to carry out the attack, the options or resources that will be required to carry out the attack and finally the size of the

Table 4 Vulnerability score card

Vulnerability score	Vulnerability type	Description of the vulnerability
1	Lowest vulnerability	This type of vulnerability is practically impossible to discover and the possibility of the attack is virtually theoretical in nature. Would involve state players
2	Low vulnerability	This type of vulnerability is very difficult to discover and the chances of exploiting the vulnerability is also very remote. Would involve either state players or organizations backed by states
3	Moderate vulnerability	This type of vulnerability is easy to detect and organizations have good awareness on the possible chances of the vulnerability being exploited. Would involve organizations that may or may not receive support from states
4	High vulnerability	This type of vulnerability is very easy to exploit and can be carried out by organizations and individuals who does not enjoy any state support. Organizations anticipate exploitation of this kind of vulnerability
5	Highest vulnerability	This type of vulnerability is very easy to exploit and very easily discoverable. Organizations have full knowledge of this kind of vulnerability and information about them may also be available in the public domain. Involves easily downloadable tools that are used to exploit this kind of vulnerability

attacker. If a type of attack would require very high level of IT skills or if an attack is only possible to be carried out by an individual country, the vulnerability or the likelihood of occurrence of such an attack will be low even though the damage will be enormous. On the contrary, a type of attack that would require few IT skills or can be carried out by an individual will minimum resources will have high threat levels, strong likelihood of occurrence and high vulnerability. For example, the Stuxnet computer malware attack that happened in 2010 was highly sophisticated and it targeted the industrial facilities in the Gulf. Iran was worst affected and the most severe form of attack took place at the Bushehr nuclear facility. Given the level of sophistication of the attack and the high level of IT skills that would be necessary, it can be safely assumed that an entire nation could be behind it. When the Stuxnet computer malware is evaluated by the risk estimation model proposed in this paper it is observed that this form of attack has very low likelihood of occurrence, less vulnerability and less threat levels. In essence, there is very little chance that attacks at this level will occur very frequently. Table 5 below illustrates the risk estimation of the Stuxnet computer malware attack.

Figure 1 below illustrates the risk estimation of the recent cyber attacks that have been reported from across the globe.

Each bubble in the figure represents a recent cyber attack and the number next to them represents the risk estimation score calculated using the formula shown above. As it can be seen in the figure above, the distributed denial-of-service (DDoS) attack has the highest risk score of 25 and the Stuxnet malware attack has the lowest risk score of 8. The main reason behind this observation is high likelihood and

Table 5 Risk estimation of Stuxnet computer malware attack

Attack	Threat Score	Likelihood of occurrence score	Vulnerability score
Stuxnet computer malware attack (2010)	4 (high)	1	2

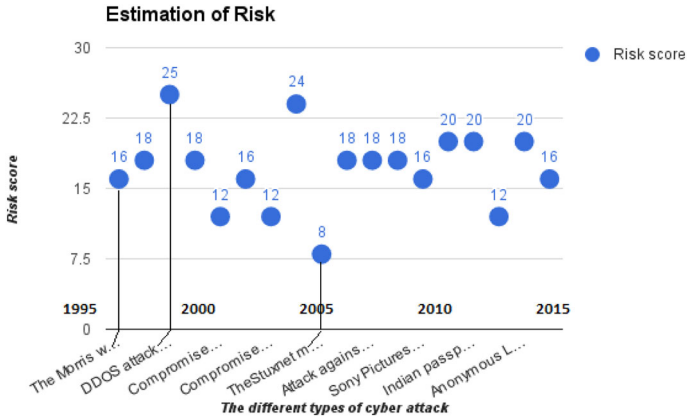

Fig. 1 Risk estimation of recent cyber attacks

vulnerability scores for the DDOS attack and low scores for the Stuxnet attack. The DDOS attack was rated at a high likelihood and vulnerability scores because it can be carried out very easily with minimal IT skills and the vulnerability to carry out this type of attack can be exploited very easily. Similarly, the Stuxnet malware attack is highly sophisticated and requires very high IT skills and that is the reason why this type of attack is relatively uncommon. So the risk of occurrence of incidents such as the DDOS attack is very high and attacks such as the Stuxnet incident is very rare. This is correctly predicted by the proposed risk estimation model. A very worrying aspect of the result seen above is that attacks with reasonably high-risk scores have occurred consistently in recent years. This clearly indicates that terrorist organizations and state players are focusing on cyber offensive like never before and the technology is becoming more readily available to carry out attacks with high levels of threat and impact. Furthermore, not a single incidence of sabotage that has lead to a major disruption of services or cyber war has lead to a loss of human life has occurred until now. With regards to the practical utility or the relevance of the proposed model, it can be stated that the risk estimation scores derived from it are fairly accurate and can serve as a knowledge base for organizations to conceptualize and formulate their cyber defence policies and strategies. The proposed risk estimation model definitely appears to be a robust tool to ascertain if a particular type of cyber attack is likely to happen in the near future but it needs to be noted that the attacks that were evaluated are few. These attacks were reported and properly addressed but there are many that are adopting

innovative paradigms and remain undetected to this date. So there is limited scope to test the efficacy of the model given the variety of attacks that are possible in a real world scenario. The cyber attacks that involve state players are not always widely publicized for investigative reasons and there is limited scope to determine if the proposed model will be able to give a proper risk estimation for the same. Furthermore, it is important that exhaustive information is available on the attackers to determine the most accurate likelihood of occurrence scores and since this is not always available the final risk estimation scores many not be accurate in all instances.

Conclusion and Future Direction

This study focused on the dynamics of cyber attacks and cyber terrorism and highlighted the ever-growing possibility of cyber warfare in recent times. With the human race becoming more and more dependent on technology and computers becoming ubiquitous in people's lives, the scope of exploiting the cyber space to compromise the security of an organization or an entire nation is growing rapidly. The empirical findings of this study clearly demonstrate the rising incidences of cyber attacks across the globe but at the same time a majority of the incidences are restricted to malicious intrusions, temporary disruption of services, data breaches and espionage activities. The risk estimation model proposed in this study may not be the most accurate paradigm to determine how likely a particular type of cyber attack is going to happen but it definitely takes into account the maximum number of factors that can be used or exploited to produce a credible score. Furthermore, there is ample scope to sharpen the predictive efficacy of the model by integrating additional factors such as financial implications and technical impact but as of now the proposed risk estimation model stands a good chance of becoming an indispensible tool for organizations to evaluate different types of attack and determine if they are vulnerable to them. As an additional benefit, the model takes into account the vulnerability factor that is not used by any risk estimation procedures available today and given the further scope of improvement, that model stands a good chance of becoming a very credible tool against probable cyber attacks in the future. It is definitely the case that there has never been any single cyber attack that has lead to major breakdown of services or even loss of human life but this definitely does not warrant complacency. A cyber attacks that have occurred recently and are reported in this study would have seemed possible only in fiction just a few decades back but now they are just considered as minor or moderate acts of disruption or espionage. Such is the pace of technological progress and it is a definite possibility that cyber attacks with the highest threat scores will occur in the coming years if appropriate counter measures are not in place. Some would argue that the unwarranted fear surrounding hypothetical cyber attacks have lead to greater militarization and rise in unnecessary insecurity among the masses which is counter productive for development. While this is true to some extent, it also needs to be understood that as technology greatly improves the quality of life and controls more and more aspects of human survival, the trade-off has to be equally impactful.

If technology can take us to the moon, a breakdown or compromise of the same will ensure that we stay there forever and never return. In essence, when gains are huge the losses can be equally big and when seen in this context a more resurgent and robust cyber security policy appears absolutely logical and necessary.

References

Bieda, D., Riddle, E., & Halawi, L. (2015). Cyberspace: A venue for terrorism. *Issues in Information Systems, 16*(3), 33–42.

Carr, J., & Shepherd, L. (2010). *Inside cyber warfare*. Sebastopol, CA: O'Reilly Media Inc.

Denning, D. (2001). Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars the future of terror, crime, and militancy* (1st ed., pp. 239–288). Santa Monica, CA: RAND.

Dhs.gov. (2015). *Cybersecurity|Homeland Security*. Retrieved from http://www.dhs.gov/topic/cybersecurity. Accessed December 24, 2015.

Dynes, R. (2006). *Natural Hazards Observer—November 2006|Natural Hazards Center*. Colorado.edu, Retrieved from http://www.colorado.edu/hazards/o/archives/2006/nov06/nov06c.html Accessed December 25, 2015.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security, 4*(2), 49–60.

Kerr, P., Rollins, J., & Theohary, C. (2009). *The Stuxnet Computer Worm: Harbinger of an emerging warfare capability*. Washington, DC: Department of Homeland Security.

Lewis, J. (2002). *Assessing the risks of cybertwrrorism, cyber war, and other cyber threats*. Washington, DC: Center for Strategic and International Studies.

Lewis, J. (2009). *The "Korean" cyber attacks and their implications for cyber conflict*|Center for Strategic and International Studies, Csis.org. Retrieved from http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict. Accessed December 26, 2015.

NATO. (2010). *Strategic concept for the defence and security of the members of the North Atlantic Treaty Organisation*. Lisbon: NATO.

O'Harrow, R. (2013). *Zero day*. New York: Diversion Books.

Rademacher, K. (2005). *Clarke: ID theft prevention tied to anti-terrorism efforts*. LasVegasSun.com. Retrieved from http://lasvegassun.com/news/2005/apr/13/clarke-id-theft-prevention-tied-to-anti-terrorism. Accessed December 23, 2015.

Rid, T., & McBurney, P. (2012). Cyber-weapons. *The RUSI Journal, 157*(1), 6–13.

Rollins, J., & Wilson, C. (2007). *Terrorist capabilities for cyberattack: Overview and policy*. Washington, DC: Congressional Research Service.

Rustici, R. M. (2011). Cyberweapons: Leveling the international playing field". *Parameters, 41*(3), 32–42.

Theohary, C., & Rollins, J. (2015). *Cyberwarfare and cyberterrorism: In brief*. Washington, DC: Congressional Research Service.

Weimann, G. (2005). Cyberterrorism: The sum of all fears? *Studies in Conflict & Terrorism, 28*(2), 129–149.

Weimann, G. (2008). *Al-Qaida's extensive use of the Internet*, Ctc.usma.edu. Retrieved from https://www.ctc.usma.edu/posts/al-qaida%E2%80%99s-extensive-use-of-the-internet. Accessed December 15, 2015.

Wilson, C. (2003). *Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress*. Washington, DC: Congressional Research Service.