International Journal
Sustainable Future for Human Security
J-SustaiN Vol. 2 No. 2 (2014) 29-34
http://www.j-sustain.com

SOCIAL SCIENCES

There is Nowhere to Hide: A Threat from Cyber Terrorism

Agus Trihartono[a*], **Halimin Herjanto**[b]

[a]*Ritsumeikan University, Japan 603-8577 and Jember University, Indonesia 68121.*

[b]*School of Business, Faculty of Business and Law - AUT University, Auckland, 1010, New Zealand.*

Received: May 29, 2013/ Accepted: September 30, 2014

Abstract

The advent of the Internet over 20 years ago has led to human beings around the globe becoming increasingly dependent on it as a means of communication, commerce, news gathering and socializing. This dependency has offered a perfect platform from which to launch cyber terrorism. This paper investigates the wide-reaching consequences of using the Internet in terms of human security. Our study finds that cyber terrorism, like traditional terrorism, has an obvious negative impact which involves economic, legal, physical, psychological, political and social consequences. It is the aim of this paper to show how these consequences pose a significant threat to human security and sustainability.

Keywords: *human security; cyber terrorism; the Internet; consequences of cyber terrorism.*

Abbreviations:

GBP	:	Great Britain Pound
IFPI	:	International Federation of Phonographic Industries
IT	:	Information Technology
NATO	:	North Atlantic Treaty Organization
UNDP	:	United Nations Development Program
US	:	United States
USD	:	United States Dollar
WMD	:	Weapons of Mass Destruction

1. Introduction

More than half a century ago, Maslow, a legendary psychologist, suggested that one of our most fundamental needs is security. To Maslow, security is not only essential to ensure the safety and future sustainability of humankind, but it also serves as a foundation from which to maintain our relationships with others. A high level of security helps people to live in certainty, lower risks, reduces competition, fear and suspicion towards others, and ultimately, improves relationship stability, harmony and wellbeing. In the absence of security, people may experience emotional disorders and high levels of depression which in turn generate trauma and adverse behaviors.

Recognizing the importance of "security", psychologists and other related academicians, including political and international relations scholars, have joined forces to investigate and discuss the concept of human security. Historically, these scholars see such security as closely related to political security.

Political security refers to a state's security, with a particular emphasis on the stability of the state's sovereignty. The concept usually focuses on state actors and their military capacities to protect national security. For example, during the Cold War period, security was closely associated with physical border security. Both Western allies and Warsaw Pact countries built and maintained their "security" through their military power capabilities.

In their Human Development Report 1994, the United Nations Development Program (UNDP) suggested that since the end of the Cold War in the early 1990s, the concept of security has evolved dramatically. According to the report, state security should no longer be the sole focus of governments; instead it is vital that human security needs are met – needs that include economic, food, health, environment, community and political security. Based on this argument, human security concerns are fundamentally linked with issues such as poverty, inequality [1], and conflict and freedom limitations [2].

Since the introduction of the Internet, the stability of human security has been under a new kind of threat [3]. Emails, chat rooms and websites provide a perfect platform for users to destabilize human security. This type of threat is known as a cyber-terrorism [4].

Numerous scholars maintain that cyber terrorism is now the biggest threat to human security [5], with the ability to reduce human security to a level lower than any other type of existing threat is able to achieve [4]. For example, in mid-2011, unknown hackers launched a cyber-attack on the Lockheed Martin Defense Department. Although, the hackers failed to steal very sensitive defense information, this event was enough to create panic among US and Lockheed Martin officials and forced them to urgently upgrade their computer security.

[*] *Corresponding Author*
E-mail: atrihartono@gmail.com

Despite the evidence of the pernicious nature of cyber terrorism, surprisingly, there appear to be few human security scholars and very limited discussion on cyber terrorism. In order to expand our understanding of cyber terrorism and its effects on human security, this study will attempt to fill this gap by investigating the extant literature from other disciplines that discuss this topic and integrating it into the human security discipline perspective. In addition, this paper will also attempt to investigate the different consequences of cyber terrorism and their relationship to human security.

2. Human Security

The word "security" originates from the Roman word "securitas" which refers to the goddess of stability. According to the online Dictionary.com, "security" means freedom from danger, risk, anxiety, doubt, financial cares or from want. Security implies a well-founded confidence, and something that makes us feel safe. Thus, human security can be defined as something that makes people feel safe from dangerous situations or events.

Numerous scholars and decision makers argue that human security is not as simple as the definition above. They believe that human security is integrally connected with various components of human rights – rights that include political, food, health, environmental, personal, political, and energy security[1],[2],[6]. Possessing these rights of security allows individuals a sense of wellbeing and freedom, especially "a freedom from fear and uncertainty". Thus, in this respect, human security serves as an important vehicle to guarantee humanity's future sustainability and development [7].

Historically, the concept of human security can be traced back to Adam and Eve. According to the Christian Bible, when Adam and Eve ate the forbidden apple, they started to feel shame and insecurity. They lost their freedom and developed a fear of God. The concept of human security is much the same today: freedom from anxiety and fear, especially of the unknown, is paramount in people's minds.

Since the Medieval era, the concept of security has focused on state security. This type of security emphasizes the importance of state sovereignty as the key to all other forms of security. In other words, without state sovereignty, no other forms of security are achievable. State security normally promotes strong military personnel and defense capabilities: the stronger the military power the more secure the state will be. During the cold war era, this idea was heavily adapted. Superpower countries such as the United States of America and the Soviet Union raced to develop their military skills and to recruit as many allies as possible. In this period Security was mostly connected with the concept military capability, deterrence, balance of power, military dilemma and so forth. Throughout this time, both the US and its allies, NATO (North Atlantic Treaty Organization), and the Soviet Union and the Warsaw Pact countries maintained their state security by protecting their borders from direct enemy attacks.

After the collapse of the Soviet Union, the Cold War officially ended. Since then, although countries from both sides have not completely loosened their military power; countries begun to concentrate on other types of human security needs, such as food security and energy security. For example, most countries of the world are now putting their energy into producing enough food for survival and protecting the planet from natural disasters. Scientists and decision makers are working together to develop food technology based on genetic modification in order to produce new food supplies. Similarly, they are also attempting to replace fossil fuels with sustainable products such as palm oil.

However, despite these advances in human security, a parallel event in the mid-1990s meant that the security landscape became far more complex. It was at this time that the Internet became available. Internet technology was originally developed in the late 1960s as a military experiment, but on its general release in the 1990s, it changed the communication landscape forever. The Internet enables its users to communicate instantly, economically and easily with anybody in any part of the world. In addition, the Internet allows users to access information with one easy click.

Since its first general introduction, the Internet has made life easier by replacing many traditional methods of doing things, such as banking, schooling, communicating and even conducting surgery. Because of its helpful features, the number of Internet users according to Internet World Statistic has dramatically increased from 361 million users in the year 2000 to more than 2.4 billion users in 2012 [8]. This represents a nearly 570% increase. This finding shows that Internet use has not only spread and become widely accepted, but it also suggests that people around the world have become more dependent on the Internet. Studies have shown that in extreme cases, some users have become addicted to the Internet [9] – particularly through its gaming and social networking platforms.

As the dependency on the Internet increases, users' level of freedom decreases. According to Creekman, this high level of dependency produces new and significant security threats – from simple cyber bullying, to the extreme risks to national infrastructure systems and national home security [10].

3. Cyber Threats

Cyber threats refer to any risks that are produced and facilitated by the Internet. These threats include cyber-attacks, cyber-crime and cyber terrorism [11]. Cyber attacks refer to any types of attack that are facilitated by the Internet; cyber-crime is any crime conducted through the Internet; and cyber terrorism involves cyber activities that terrorize other users. Although many scholars argue that these negative cyber activities are different [11]; [12]; [13], Mavropalias argues differently. He suggests that these activities have very similar characteristics and are only differentiated by the weight of their word meanings. According to Mavropalias, the terms 'cyber terrorism' and 'cyber-crime' both imply 'cyber-attacks' on others. The only difference between the terms is that cyber terrorism is a stronger description [14]. Our study also holds that the three terms describe the same activity and we refer to all three under the one term, 'cyber terrorism'. Cyber terrorism is any type of cyber activity that intimidates and harms both people and the state, creates fear and anxiety, and threatens stability and security.

According to Grabosky, cyber terrorism can be classified into two major categories: conventional crimes and attacks on computer networks [15]. Conventional crimes refer to crimes that are facilitated through the Internet. These crimes are normally conducted by single individuals or small groups of computer users. They usually target other single individuals or on occasion, particular groups or businesses. According to Furnell and Warrant, this type of crime is primarily motivated by individuals' needs. That is, the need for financial gain, fun and self-esteem [16]. Online crimes that fit this category include child pornography, identity forgery, web stalking, digital piracy and cyber bullying [14].

Attacks on computer networks, on the other hand, are crimes that are deliberately conducted to attack organization's or government's computer networks. Due to its scale, this type of cyber terrorism has more serious consequences than conventional computer crimes. Attacks on computer networks are usually conducted by expert individuals or deviant groups. These types of people are usually no longer driven by individual needs; instead they have political or generally destructive reasons. Such attacks include theft, espionage, political statement, vandalism, information warfare, revenge and attention seeking [15].

Although these two types of crime have different characteristics, they both have a similar negative impact, generating economic, legal, physical, political, psychological, and social consequences.

4. The Consequences of Cyber Terrorism

As pointed out above, heavy dependency on the Internet makes people more vulnerable. In terms of human security, the Internet allows massive opportunities for terrorists to launch attacks at anytime and anywhere without fear of being identified and caught. Six different potential consequences of cyber terrorism are discussed as follows:

4.1. Economic Consequences

Out of all the consequences of cyber terrorism, the economic consequences are regarded as one of the most significant [17]. Tushabe and Baryamureebaargue that financial losses accruing from cyber terrorism are huge and multiply every year – yet only a small number of cases are reported to the authorities. The authors maintain that there are three different economic consequences of cyber terrorism [18]. The first consequence is the direct and indirect loss of revenue. In terms of direct revenue, the 2012 Norton Symantec report suggests that cyber terrorism has been responsible for the loss of USD $66 billion in potential revenue by governments and businesses. Internet fraud and theft are regarded as the major cause of these losses.

There are several reasons for the loss of indirect revenue. Companies attacked by cyber terrorists often receive negative comments from the media because of their poor security; as a result, their share prices may drop between 1 and 10% [19]. A further result is that such companies experience weaker competitiveness and may lose their market share. For example, the 2011 Business Software Alliance report shows that the global software industry has lost USD $59 billion due to software piracy. In addition, Tushabe and Baryamureeba argue that digital piracy and the cost of combatting digital piracy are also responsible for the indirect loss of revenue [17]. The 2012 Norton Symantec report concludes that the total direct or indirect revenue losses have reached USD $110 billion – or a USD $200 average cost per victim.

The second of the economic consequences is wasted resources. This refers mainly to the unnecessary costs incurred in combatting cyber terrorism. For example, Prydepoints out that one British IT company spent almost GBP £4 billion to employ IT experts to combat cyber terrorism [20]. In addition, nearly 50 terawatt hours of electricity are wasted every year to combat spam and pay for repairs on computer systems [17].

The final economic consequence of cyber terrorism is productivity reduction. Cyber terrorism forces individuals, especially employees of attacked firms, to focus their time and effort on fighting cyber terrorism instead of focusing on their main job [17]. In the entertainment industry, according to International Federation of Phonographic Industry digital piracy victimises the artists who may become demotivated and as a result, produce no new songs or movies [21].

Such economic losses indirectly affect the stability of human security. In absence of profitability, businesses as well as governments have less spending power, resulting in redundancy and economy recessions. This negative economic impact clearly generates a high level of uncertainty and anxiety. As a result, people lose their freedom and start to develop fear and deviant behavior.

4.2. Legal Consequences

The speed at which the world has adapted to the Internet, along with the development of advanced Internet technology, has created different types of moral, social and criminal wrong-doing [22]. Roy maintains that the anonymous nature of the Internet allows smart criminals to conduct illegal behaviors with ease [22] and, as Mitrakas points out, there are not always suitable Cyber laws and regulations to control them [23]. As a result, the authorities are one step behind cyber criminals and have not been able to bring them all to justice. For example, due to outdated Cyber law, New Zealand hackers were in the past able to intercept emails and hack others' computer systems without fear. Cyber bullying was also rampant in New Zealand for the same reason. Because of this negative situation, New Zealand authorities started to reformulate and introduced new Cyber law. Since the year 2000, hacking activities as well as cyber bullying has been classified as illegal and the subject of New Zealand cyber-criminal law.

Despite the legal developments in New Zealand, the adoption and application of Cyber law is slow amongst many other countries in the world – particularly developing countries. According to Moore, Palfrey and Gasser developing countries have significant financial limitations, inefficient and corrupt laws and law enforcement, as well as a lack of understanding [24]. As a result, authorities are unable to help innocent victims, thereby creating a high level of uncertainty, distress and distrust of the authorities. This in turn leaves a country vulnerable to political or terrorists groups who aim to destabilize the national political situation. In the long run, the lack of control can lead to civil war and the likelihood of many refugees. In summary then, the lack of legal consequences for cyber terrorism not only threatens individuals' wellbeing but also endangers political stability.

4.3. Physical Consequences

Cyber terrorism also has indirect and direct physical consequences. Indirect physical consequences refer to indirect physical injuries resulting from cyber terrorism. According to Veersamy, one of the main purposes of cyber terrorism is to create a high level of uncertainty, which leads to an equally high level of anxiety, fear and depression [4]. In the long run, Sirois and Burg argue that such high levels of anxiety and depression negatively affects victims' health and wellbeing [25]. For example, the victims of cyber-bullying are often diagnosed with psychological disorders reflected in low self-esteem and a feeling of being unsafe [26]. According to Corcoran, the negative experiences associated with cyber-bulling destroy victims' self-confidence and give them a false perception of who and what they are, leading to self-loathing and the danger of suicide [27].

Direct physical consequences, on the other hand, refer to the direct physical injuries that result from cyber terrorism. For example Mann notes that the victims of cyber-bullying can experience severe headaches and rapid heartbeat [26]. This physical disorder is regarded as a result of shame and embarrassment and to deal with these feelings, adult victims may turn to drugs or alcohol [27].

These two examples above confirm that cyber terrorism, particularly cyber-bullying, destroys people's freedom and psychological wellbeing. As a result, victims may lose all self-esteem and any sense of meaning in life. The consequences of these negative perceptions of self and life can lead to violent acts by victims –directed either at others or directed at themselves.

4.4. Political Consequences

Cavelty discusses the serious political consequences of cyber terrorism [28]. According to Cavelty, political cyber terrorists are in 'the business of espionage' – they seek to steal sensitive and confidential information from states, organizations, businesses or individuals [28]. For example, in early 2013, the Obama administration accused the Chinese Government of breaking into US Government computer systems and illegally downloading sensitive government and trade data. The Chinese Government strongly denied the allegation and instead accused the US Government, in particular the US Foreign Ministry, of spying on and hacking into Chinese military computer systems. These allegations have created a tension between the two superpowers and threaten their bilateral relations [29].

As well as targeting national governments, cyber terrorists are also able to create disaster at the local government level. For example, in late 2011, Russian cyber terrorists attempted to hack the public water control systems of the US state of Illinois. Although the hackers were blocked, there was brief panic at the potential damage that might have occurred and that would have jeopardised the safety of the citizens of the state of Illinois [30].

Based on the observations above, it is reasonable to say that the failure to prevent cyber terrorism can jeopardise national and international political security. In the most extreme cases, this failure could potentially trigger war [31], including war with high technology of strategic weapons known as WMD (weapons of mass destruction).

4.5. Psychological Consequences

The psychological consequences of cyber terrorism are regarded as the most damaging consequences of all [32]. These consequences involve negative emotional experiences, such as anxiety, fear and anger [33], and can result in emotional and behavioral disorders [26], [37].

In addition, Jones also notes that cyber terrorists have used brain washing as a terrorist technique [34]. He discusses the attempt to recruit suicide bombers by using persuasive ideological information transmitted through the Internet. Once recruited, these victims lose their identity and are willing to sacrifice their own lives in the interests of the terrorists. These brainwashed victims are no longer able to differentiate friend from foe and thus pose a major threat to human security.

4.6. Social Consequences

Social consequences are the final major outcome of cyber terrorism [35]. With the inadequate Internet protection systems and a lack of information regarding cyber terrorism, Internet users have difficulty protecting themselves from the cyber-attacks and are likely to blame authorities. Over a period of time, victims' frustrations can lead them to distrust authorities and become reluctant to report the cyber-attacks [36]. In the absence of trust, the authorities can lose victims' support, making the battle with cyber terrorism all the more difficult to achieve.

The second social consequence, according to the International Federation of Phonographic Industries (IFPI), is that creativity deteriorates [37]. Our report shows that the failure of authority digital piracy leads to less production by artists. John Kennedy, the Chief Executive Officer and Chairman of the International Federation of Phonographic Industries, in his statement in IFPI points out that digital piracy is killing the music industry because if artists are not paid for the music they create, they will ultimately stop making music[38]. Thus in the long run, this situation will affect overall cultural development.

Conclusion

This investigation shows that despite the relatively recent introduction of the Internet, it now poses a serious threat to human security. Cyber terrorism in all its forms is pernicious and here to stay unless authorities and academics can devote greater attention to means of overcoming it. Failure to handle cyber threats not only affects nations' wealth, sovereignty and international relations, but more importantly it negatively affects people's wellbeing.

References

[1] Steven Lonergan, Kent Gustavson, and Brian Carter. "The index of Human Insecurity." *AVISO Bulletin Issue* 2000; No. 6. http://www.gechs.org/aviso/AvisoEnglish/six/six.shtml. Accessed 24 August 2001.

[2] Hans Van Ginkel, and Edward Newman. In Quest of "Human Security." *Japan Review of International Affairs*2000; 14.1: 79.

[3] Lachow, I., & Richardson, C. Terrorist use of the internet: The real story. Report for National Defence university, institute for national strategy Studies;2007.

[4] Veerasamy, N. Towards a conceptual framework for cyberterrorism. *Council for Scientific and Industrial Research (CSIR)*, Pretoria, South Africa;2009.

[5] Rathmell, A. Cyber terrorism: The shape of future conflict. *The RUSI Journal*1997; 142(5): 40-45.

[6] Sadako Ogata, "Human Security: a Refugee Perspective." Keynote Speech by Mrs.Sadako Ogata, United Nations High Commissioner for Refugees, at the Ministerial Meeting on Human Security Issues of the "Lysoen Process" Group of Governments. Bergen, Norway, 19 May 1999. http://www.unhcr.ch/refworld/unhcr/hcspeech/990519.htm. Accessed 24 August 2001.

[7] Jennifer Leaning, M.D., S.M.H., and Sam Arie. Human Security in Crisis and Transition: A Background Document of Definition and Application. *Working Draft, Prepared for US AID / Tulane CERTI.* September 2000; p.37.

[8] Internet World Users. Internet World Users. Usage and Population Statistics;2013. http://www.internetworldstats.com/stats.htm. Accessed15 March 2013.

[9] Shek, D.T.L., Sun, R. C. F., & Yu, L. Internet Addiction. In D.W. Pfaff. Editors. Biomedical Life Sciences. NeuroScience in the 21st Century; 2013. http://www.springerreference.com/docs/html/chapterdbid/333019.html. Accessed15 March 2013.

[10] Creekman, D.M. A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China.*American University International Law Review*2002; 17(3): 641-681.

[11] Solce, N. The battlefield of cyberspace: The inevitable new military branch-the cyber force. *Law Journal of Science and Technology*2008; 18: 293-324.

[12] Nagpal, R. Cyber terrorism in the context of globalisation. Paper presented at II World Congress on Informatics and Law, Madrid, Spain; 2002.

[13] Clem, A., Galwankar, S., & Buck, G. Health implications of cyber-terrorism. *Prehospital and Dissaster Medicine*2003; 18(3): 272 -275.

[14] Mavropalias. K. Cybercrime & Cyberterrorism: inducing anxiety & fear on individuals. 2011. http://iconof.com/blog/cybercrime-cyberterrorism-inducing-anxiety-fear-on-individuals/. Accessed 16 March 2013.

[15] Grabosky, P. The global dimension of cybercrime. *Global Crime*2004; 6(1): 146-157.

[16] Furnell, S.M., & Warrant, M. J. Computer hacking and cyber terrorism: The real threats in the new millennium? *Computer & Security*1999; 18: 28-34

[17] Harmantiz, F., & Malek, M. Security risk analysis and evaluation. IEEE Community Society2004; 1897-1901

[18] Tushabe, F., & Baryamureeba, V. Implication of Cyber Crime on social economic development. *Working Paper;*2012. http://cit.mak.ac.ug/staff/tushabe/implicationsCybercrime.pdf. Accessed15 March 2013.

[19] B. Cashell, The Economic Impact of Cyber-Attacks, *CRS Report for Congress*, 2004.

[20] I. Pryde. Counting the cost of unwanted emails.*Security post*2005, issue no. 7,2005.

[21] IFPI. Digital Music Report 2011 Music at touch of a button: International Federation of Phonographic Industries;2011. http://www.ifpi.org/content/library/DMR2011.pdf. Accessed15 March 2013.

[22] Roy, A, K. Role of Cyber law and its usefulness in Indian IT industry. Paper presented in Internal Conference on Advances in Information Technology; 2012.

[23] Mitrakas, Andreas, Information & communications technology law 2006; 15-1:33.

[24] Moore, J., Palfrey, J., & Gasser, U. ICT and entrepreneurship: digital business ecosystems and the law;2003. http://cyber.law.harvard.edu/bold/devel03/modules/episodeII.html. Accessed16 March 2013.

[25] Sirois, B.C., & Burg, M.M. Negative emotion and coronary heart disease: a review. *Behaviour Modification*2003; 27(1): 83-102.

[26] Mann, D. Emotional troubles for cyberbullies and victims. Study shows mental and physical impact of cyberbullying on victims and bullies;2010. http://www.webmd.com/parenting/news/20100706/emotional-troubles-for-cyberbullies-and-victims.Accessed17 March 2013.

[27] Cocoran, K. Inspirations for Youth and Families, LLC – Dr. James HughesStop Cyberbullying and Wired Kids Inc. Teen cyberbullying, a back to school teen behaviour problem;2010. http://teen-drug-rehab.blogspot.co.nz/2010/08/teen-cyberbullying-back-to-school-teen.html. Accessed17 March 2010.

[28] Cavelty, M. D. Cyber terror – looming threat or phantom menace? The framing of the US cyber threat debate. *Journal of Information Technology & Politic* 2007; 4(1), 19-36.

[29] Anonymous. US ready to strike back against China hack attacks;2013. http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10866604. Accessed15 March 2013.

[30] Anonymous. US water system hacked from Russia;2011. http://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=10767234. Accessed16 March 2013.

[31] Gorman, S. Cyber combat: Act of war. Pentagon sets stage for US to respond to computer sabotage with military force; 2011. http://online.wsj.com/article/SB100014240527023045631045763556231357827l8.html. Accessed15 March 2013.

[32] Taliharm, A.M. Cyberterrorism: in theory or in practice? Defence against Terrorism. Review DATR2010; 3(2): 59 -74.

[33] Ganor, B. Terrorism in the Twenty-First Century, Shapira, S., Hammond, J. and Cole, L. Editors.*Essentials of Terror Medicine*, Springer;2009:pp. 13-26.

[34] Jones, C. Book Reviews, Andrew Silke, ed. Terrorists, Victims and Society: Psychological Perspectives on Terrorist and Its Consequences. *Studies in Conflict & Terrorism*2004; 27: 153-158.

[35] Haugen, S. E-government, cyber-crime and cyber-terrorism: a population at risk. *Electronic Government*2005; 2(4), 403-412.

[36] Westby, J. R. Countering terrorism with cyber security. Jurimetric2007; 47: 297 – 313.

[37] IFPI. Digital Music Report. New Business Model for changing Environment: International Federation of Phonographic Industries;2009. http://www.ifpi.org/content/library/DMR2009-real.pdf. Accessed 15 March 2013.

[38] IFPI. Digital Music Report. Music how, when, where you want it;2009. http://www.ifpi.org/content/library/dmr2010.pdf. Accessed15 March 2013.