한국위기관리논집 제11권 제2호 2015. 2 343~362쪽

Threat of Cyber Terrorism to Modern Society*

- Different Approaches from Different Perspectives -

Kwang Ho Chun**

Faculty of International Studies, Chonbuk National University, 567 Baekje-daero, Deokjin-gu, Jeonju-si, Korea

Abstract

Is cyber terrorism the threat to modern society? Not only has the socio- and geo-political climate changed dramatically in the last decade, but there has also been a technological change with the advent of the 'information revolution'. Governments all over the world are trying to protect critical national infrastructure from a new apolitical threat, yet they are not able to agree upon a common cyber-threat vocabulary. This paper compares two different approaches to combatting the cyber threat and underlines their common understanding yet different articulation of what constitutes cyber terrorism. The central argument of the paper is that cyber terrorism against critical national infrastructure is not presently a great threat but perceptions of it make it a useful tool in securing financial interests and controlling domestic populations.

Key words: cyber terrorism, cyber warfare, cyberspace, technology, internet

Ⅰ. Introduction

This paper will argue that there is a lack of coherence between different definitions in the cyber sphere, especially between cyber terrorism and cyber warfare. Furthermore, the aim of this paper is to assess whether the internet is a useful weapon for cyber terrorists and whether it

---

* This paper was supported by research funds of Chonbuk National University in 2014.

** Tel. +82-63-270-2100. Fax. +82-63-270-2099 E-mail. khchun@jbnu.ac.kr

Submission & Publication Process

Received: Jan. 5, 2015 / Revised: Feb. 3, 2015 / Accepted: Feb. 20, 2015

poses a real threat to modern societies or just a new challenge to protect new vulnerabilities in critical national infrastructure. A study will then be done to discover the criticality of national infrastructure in modern societies and how useful the existent countermeasures are against cyber terrorism. In addition, this paper will compare the UK approach, as a NATO and an EU member, and Switzerland, as a small neutral country in Western Europe. The paper will conclude that there are undoubtedly some serious problems to solve in cyber security and will offer some approaches to coping with this new challenge. It is concluded that the term 'cyber terrorism' is an ideal tool for governments to secure monetary interests and to control domestic populations. Cordesman and Colarik have covered significant parts of this large topic and so their contributions are called upon in making a grounded assessment. Later, the paper will often refer to the Rt Hon Francis Maude(MP, Minister for the Cabinet Office) in regards to the UK's perspective and to Daniel Möckli from the Center for Security Studies(CSS), ETH Zürich in regards to the Swiss approach to the cyber threat.

During the last two decades the infrastructure of modern western economies has changed fundamentally.

Cyber technology can be used to attack the machinery of a state, its financial institutions, national energy supply, transport infrastructure, and public morale(Cordesman & Cordesman, 2002). While some actions may appear aggressive and warlike, the cyber activities of terrorists, spies and organised criminals do not necessarily constitute acts of cyber warfare. Operating behind false IP addresses and the use of foreign servers allows cyber activists almost complete anonymity and a relative impunity. Cyber technology gives a disproportionate power to small and otherwise relatively insignificant actors and furthermore it allows a mixing of military and civilian actors. This operation without boundaries is blurred between physical and virtual, and power can be exerted by states or non-state actors, or even by proxy.

II. Definition of Cyber Terrorism and its Difference with Cyber Warfare

Cyberspace is an apolitical space and might be a security challenge for governments, commercial enterprises and for private individuals as well. International organisations too may become victims of threats in cyberspace, because all branches in modern life rely heavily on digital communications and information transfer infrastructure. These challenges are often called cyber security. In addition, media and politicians often discuss cyber warfare in terms of alarming

anecdotes which often seem closer to the world of science fiction than public policy.

A Chatham House Report used the term 'cyber warfare' in order to focus discussion on activities which are 'warlike' but which may or may not be 'war' per se. 'Warfare' is a more open-ended term, more useful in exploring an environment that is not only virtual but also largely uncharted. The report identifies the essential characteristics of cyber warfare as a strategic phenomenon by describing the actions of cyber attackers and the reactions of defending governments and by analysing the 'ends, ways and means' of cyber warfare. As a result it proposes the following definition:

> Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target(Cornish, *et. al.,* 2010: 7).

The Cyber Warfare definition says nothing about the distinction between the different levels. A Cyber attack could occur on many different levels. The US Commission on Critical Infrastructure Protection mentioned five different levels:

* A cyber-attack on the specific database of an owner/operator
* A cyber-attack for the purpose of gaining access to a network
* A cyber-attack for the purpose of espionage
* A cyber-attack for the purpose of shutting down service
* A cyber-attack for the purpose of introducing harmful instructions(Crdesma & Cordesman, 2002).

The basic cyber-attack tools are common between a nation-state led cyber attack and recreational hacker. Therefore every cyber attack has to be judged independently for a proportionate response. In order to understand whether a hostile action in cyberspace is warlike, it is necessary not just to observe the event but also to understand the actor's intent. The three most probable reasons for cyber attacks are:(Janczewski & Colarik, 2008: 13)

Firstly, fear factor: the most common denominator in the majority of terrorist attacks is a terrorist's wish to create fear in individuals, groups, or societies. Secondly, spectacular factor: spectacular attacks should create direct losses and result in a lot of negative publicity and finally the vulnerability factor: some of the most effective ways to demonstrate an organisation's vulnerability are to deny its service and to deface it through its web page.

Cyber terrorism is an attractive option for modern terrorists, who value its anonymity, its potential to inflict massive damage, its psychological impact, and its media appeal. Before discussing threats from cyber terrorism, it would however be helpful to define this threat. Andrew M. Colarik and Lech J. Janczewski define cyber terrorism in their book as follow:

> Cyber terrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data resulting in violence against non-combatant targets(Janczewski & Colarik, 2008: 13).

Gabriel Weimann(2005: 131-132) described other reasons in his article for cyber terrorism angst. It is the combination of psychological, political and economic forces who promote the fear of cyber terrorism. First, the psychological impact might be even greater than the effect of a conventional bomb because of a lack of understanding. Second, the promotion of fear with the impact of mass media headlines such as the following: 'Cyber-Attacks by Al Qaeda Feared, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say.' published in the Washington Post in June 2003. Mass media does often not distinguish between adventure hackers and cyber terrorists. The third factor is the big business earning money from the fear of other people. Cyber terrorism merges two spheres together: terrorism and technology. Security consultants are highly motivated to increase the belief that every single network in a company is critical to security. Cyber terrorism is therefore an intentionally emotive expression that underlines this belief to increase IT security spending.

This explanation does not distinguish between cyber terrorism and cyber crime. Not every act against somebody to gain money is a cyber-act of terror. Therefore one needs clarity about terrorism and activities concerning technology. Terrorism is defined as follows:

'Violence or the threat of violence, used and directed in pursuit of, or in service of, a political aim(Hoffman, 2006).'

Dorothy Denning, a professor of computer science, tried to be more precise about the definition of cyber terrorism. She used has made her definition in numerous articles, and in her testimony on the subject before the congressional House Armed Services Committee:

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

> Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not(Weimann, 2005: 135).

The lack of a clear and coherent definition of cyber terrorism is obvious. The mass media and journalists are looking more for sensationalism than to define a new term related to terrorism and computer networks. Currently, it is very common to create new words simply by placing the words 'cyber', 'computer' or 'information' before another word. This tendency is neither helpful nor useful in coping with a new challenge or threat in a more connected world. Decisions makers need a common framework to handle this complex topic. International operational definitions of cyber threats like cyber vandalism, cyber crime, cyber espionage, cyber sabotage, cyber terrorism and cyber warfare might be the first step for cooperation on several levels(Vernez, *et. al.,* 2011: 8).

III. The Internet as a Weapon of Terrorism

> The low cost and largely anonymous nature of cyber space makes it an attractive domain for use by those who seek to use cyber space for malicious purposes. These include criminals, terrorists, and states, whether for reasons of espionage, influence or even warfare(UK Cabinet Office, 2009: 12).

The vast majority of cyber attacks are launched by hackers with few if any political goals. The attacks are mostly conducted to cause disruption. The attacks are not able to create public fear or to destroy a property(Weimann, 2005: 131).

> Although there is no conclusive evidence(certainly in the public domain) that groups such as Al-Qaeda have the capabilities or resources yet to launch a major cyber attack, terrorist groups are increasingly web-literate and use the internet and deep web in order to propagate their message and mobilize supporters. The potential applications of communications networks, mobile information systems and intelligent technology in facilitating terrorist attacks were all in

evidence during the Mumbai bombings of November 2008 when terrorists(Lashkar-e-Taiba) used GPS systems and 3G Smartphone's, alongside conventional weapons, to prepare for and carry out attacks on civilian targets(In this case the technology was used in a relatively rudimentary manner, recording and detailing reconnaissance information on the targets, enabling communication between the perpetrators and providing tactical guidance to the gunmen during the attack.)(Cornish, et. al., 2010: 8).

Cyber-attacks can be cheaper than conventional terrorism and requirements are often a simple personal computer and an online connection. Sharing information by use of encryption improves the security and decreases the costs, especially over long distances. Cyber terrorism is more anonymous than traditional terrorist methodology. Terrorists can operate from the 'background' without physical barriers, borders or customs agents. The likelihood of being discovered depends heavily on an individual network's security. That might be one reason why small companies have often more problems with their network security than big companies who spend a large amount of money on network infrastructure. Psychological influence and online recruitment with the help of social networks is another advantage of the use of the internet by terrorists. Cyber terrorism offers finally great potential to affect a large number of people and thereby guarantees greater media coverage(Weimann, 2005: 137). The internet itself might not be threatened by cyber terrorists because they use the internet as a tool of communication and as a tool to spread propaganda worldwide.

The success of a cyber attack depends entirely on the method utilized, the desired end state, the target's individual defence or the monitoring capabilities of the target. Unauthorized access continues to be the second-greatest source of financial loss and is therefore an ideal way to secure a stable financial basis for terroristic attacks(Janczewski & Colarik, 2008: 15). According to a report issued in 2002 by IBM Global Security Analysis Lab, 90 percent of hackers are amateurs with limited technical proficiency, 9 percent are more skilled at gaining unauthorized access but do not destroy anything and only 1 percent are highly skilled and intent on copying files or damaging programs and systems(Weimann, 2005: 137).

Media is coverage is supported by a large number of security consultants. Even software companies are highly motivated to sell security software. At this time, all these actors have to their advantage that everybody believe that the threat from the internet to a modern society is severe(Weimann, 2005: 142). According a Chatham House Report the estimated cost for cyber crime is $1 trillion per year globally, but this figure does not reflect the threat of cyber terrorism.

IV. Critical Infrastructure Protection in Modern Society – Is it a Challenge?

The vulnerability of modern societies represents a growing challenge to security policy. Critical Infrastructure Protection(CIP) has gained new urgency since the terrorist attacks of September 11, 2001. The development of effective protection concepts is, however, difficult. Differentiated situation analyses, a better understanding of the vulnerabilities and a political consensus on priority measures are required. Also, internal and inter-state cooperation as well as functioning public-private partnerships are essential. This is largely due to the traumatic terrorist attacks in New York and Washington(2001), Madrid(2004) and London(2005). In all these cases, the perpetrators had targeted elements of the civil infrastructure for the purpose of indiscriminate murder(Möckli, 2007: 1).

After several improvements, the President's National Strategy for Homeland Security(NSHS) provided an overall definition for America's critical infrastructure.

> Our critical infrastructures are particularly important because of the functions or services they provide to our country. Our critical infrastructures are also particularly important because they are complex systems: the effects of a terrorist attack can spread far beyond the direct target, and reverberate long after the immediate damage.
> America's critical infrastructure encompasses a large number of sectors. Our agriculture, food, and water sectors, along with the public health and emergency services sectors, provide the essential goods and services Americans need to survive. Our institutions of government guarantee our national security and freedom, and administer key public functions. Our defence industrial base provides essential capabilities to help safeguard our population from external threats. Our information and telecommunications sector enables economic productivity and growth, and is particularly important because it connects and helps control many other infrastructure sectors. Our energy, transportation, banking and finance, chemical industry, and postal and shipping sectors help sustain our economy and touch the lives of Americans every day(US Office of Homeland Security, 2002: 30).

The UK followed in 2007, after a structural reorganisation headache with a similar definition. The evolutionary journey of the Critical National Infrastructure(CNI) was an effort to enhance the UK's security and resilience.

The national infrastructure comprises the facilities, systems, sites and networks necessary for the delivery of the essential services upon which daily life in the UK depends.

There are nine national infrastructure sectors which provide these essential services:

* Communications
* Emergency Services
* Energy
* Finance
* Food
* Government
* Health
* Transport
* Water

The UK's infrastructure protection effort is organised around these nine sectors. Work may also be driven forward on cross-cutting themes such as 'space' where there may be infrastructure which supports the delivery of essential services across a number of sectors, or 'personnel security' which will be important to improving security across all of the sectors - these are not recognised as national infrastructure sectors in their own right.

1. Critical Infrastructure

Not everything within a national infrastructure sector is 'critical'. In the sectors there are certain 'critical' elements of infrastructure, the loss or compromise of which would have a major, detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life. These 'critical' assets make up the nation's critical national infrastructure(CNI) and are referred to individually as 'infrastructure assets'. Infrastructure assets may be physical(e.g. sites, installations, pieces of equipment) or logical(e.g. information networks, systems)(Centre for the Protection of National Infrastructure, 2014).

In accordance with this approach, critical infrastructures should be considered as two elements. The obvious physical element and the information technology firms, networks, services and assets which, if disrupted or destroyed, would have a hugh impact on health, safety or the economic well-being of citizens and as well as on the efficient functioning of the Government of a country. This infrastructure can be endangered by physical factors as well as due to deliberate attacks by

actors. The first category of risks covers natural disasters, civilisation disasters(e.g. dam breakage, nuclear power plant meltdown), personnel failure due to strike or epidemic, organizational shortcomings of technical or people, human failures, technical errors as well as supply bottlenecks. The spectrum of potential attackers, the second category, is far and ranges from the bored teenagers to angry or disgruntled employees, spies, organized crime, terrorists and other states.

The attack options, including hacking attacks as well as the physical destruction of civilian or military facilities, are diverse. The early main American CIP effort was however clearly on the still largely unknown risks from cyberspace: the global information infrastructure seems to allow anonymous attacks from anywhere in the world at the same time: hacking tools are readily available. Due to this threat perception a CIP policy emerged under President Bill Clinton, who directed to a large extent on information security. However, since the terrorist attacks of 9/11, a return of the classic concept of threats in the CIP debate can be recognized.

CIP in the United States was a core component of home land security and is today primarily discussed by a view on strategies against Islamic terrorism. Physical aspects of CIP are brought to the foreground, cyber aspects on the other hand, have lost in importance. An alignment for counter-terrorism of CIP is today also the debate in the EU, which has recently started developing a CIP policy coordinating in particular the actions of its Member States.

It would be naïve to overestimate the political influence of the United States, as well as the willingness of allies and trading partners to take steps that could be interpreted as favouring the West. The geopolitical calculus of the western allies could change aggressive acts of China; there is also the problem of the direction precision power in cyberspace.

In 2008, according to the Washington Post, an elite US Army cyber team was ordered to shut down a joint CIA-Saudi 'honeypot' website that was used by terrorists for communication matters. The website was allegedly used as an intelligence-gathering tool, but unexpected consequences ensued when the team shut it down.

> The dismantling of the CIA-Saudi site inadvertently disrupted more than 300 servers in Saudi Arabia, Germany and Texas, a former official said. "In order to take down a web site that is up in Country X, because the cyber-world knows no boundaries, you may end up taking out a server that is located in Country Y(Cornish, *et. al.,* 2010: 22-23).

The destruction that may have been created by this cyber attack resulted from the forced closure of one website: how much more chaos would result from a sophisticated attack on a server farm or a major internet node(Cornish, *et. al.,* 2010: 22-23)?

2. Challenges for an effective CIP policy

The American example and the difficult experiences of other countries point to four, sometimes closely linked, demands for an effective CIP policy. First, a sound estimation of the nature and extent of the relevant risks and threats must be made. Instead of the currently unilateral focus on terrorism, CIP should again follow a wider approach and deal in general with the vulnerability of highly complex systems. The analysis of the situation seems to be a very important factor and should be allocated to the intelligence services. It is all the more important; depending on the risk the responsibilities are different and protection measures. On the one hand, protection against hazards and risks in the 'normal' framework - from hacker attacks to smaller natural disasters - the infrastructure manager is responsible for managing these issues alone. But the State on the other hand, it is expected that protection can be offered at a higher level from dangers, such as terrorist attacks and conventional warfare from other states(Möckli, 2007: 2).

Second, it is necessary to have a larger understanding of the vulnerabilities including the interdependencies within infrastructures. It has been shown that due to highly complex systems the existing methodology is not sufficient to cover the whole span of the problem. Strategically, it is often less important to have the 'technical access' and to measure and quantify risks than to understand their context in the social, political and institutional, cultural or economic environment(Möckli, 2007: 2).

Third, it is necessary to answer the question "what makes an infrastructure critical?" After 9/11, the list of critical infrastructures was greatly expanded by the United States: it is now critical if it could have repercussions on the psyche and on the national morale. This causes almost insurmountable problems for the conception of protection measures. How can you ensure safety, if potentially almost everything is critical and therefore worthy of protection? Threshold values between normal and critical may be too low. The need for a meaningful prioritization is obvious but this is only possible with a comprehensive risk analysis. The hypothetical vulnerabilities of a target are not valuable as an indicator for whether this objective has to be protected or not. Rather, it takes knowledge of concrete threats and the scope and severity of a possible impact for the meaningful consideration of criticality(Möckli, 2007: 3).

Fourth, CIP requires comprehensive cooperation. A working partnership between Government and industry is indispensable. The globalization process and the liberalisation of many branches of the public sector since the 1980s are responsible for a large part of the critical infrastructure now

being private property. The economy therefore plays an important role in defining and implementing a protection policy. An effective CIP policy needs the coherence between the various governmental offices as well as international cooperation. Acts of terrorism and other crimes as well as natural and other disasters do not stop at national boundaries and therefore they require internationally coordinated countermeasures to ensure the security critical infrastructure(Möckli, 2007: 3).

Ⅴ. Cyber-Terrorism Countermeasures from Different Perspectives

In the international environment, the United States with its military and civilian programs is the most developed country. Thousands of employees with billions of dollars are busy analyzing the dangers of cyber-terrorism and writing policies of how to prepare measures and implement them. Many organisations have developed forms of public private cooperation with various levels of successes. In Europe, Switzerland, Great Britain, Sweden and the Netherlands are relatively active. The EU Commission has started to think about this new threat. NATO has so far only concept papers. Common to all initiatives is the intent to bring together many stakeholders. That may be state institutions and security services on the one hand and infrastructure operators or infrastructure users on the other hand. By their very nature these programs vary. They include consistently:

* Measures for the reliable exchange of information and methods for its analysis
* Development of methods for evaluation and forecast future trends,
* Creation of common situation centres with tasks of observation, assessment, early warning, alert and response measures,
* Development of common education and training facilities,
* Cooperation in research,
* Proposals on dealing with the media, as well as a raising of awareness of the public and leading economic and political leaders,
* Measures to review and adapt legislation and coordinate at the international level(Hutter, 2002: 38). Building company defences will not always be enough to reduce threats. Most of the time, wider cooperation will be required. This cooperation could be divided in two main parts. First, it is important to group organisations which use similar computer systems and therefore have similar threats. An example could be cooperation between Internet Service Providers(ISP). The

handling of distributed denial of service attacks is much simpler if ISPs work together. Such a standard would remove wider system response to this specific threat. Second, it is undeniable to coordinate national and international law. Common sense in what would be strictly forbidden in each and every country would drop the number of hacking attacks. Reaching a global consensus at times may seem to be nearly impossible. However, there are several good examples where world-wide cooperation already works well. Air traffic control is one good example for such a global security arrangement(Janczewski & Colarik, 2008: 418).

1. Cyber crime and the European Union

At the end of last year the European Commission proposed the establishment of a Cyber Centre responsible for coordination of prevention and fight against this new and real nature of the cyber threat. For the EU, it is important to establish this Cyber Centre EU within existing structures. A settlement directly with the European Agency for Network and Information Security(ENISA) seems most efficient(Strasser, 2012). Due to the complexity of technology, many components and actors must work together, and human behaviour has become a crucial factor. Governments are confronted with a greater responsibility for society and therefore governments have to improve and promote electronic communication security in their territory(Janczewski & Colarik, 2008: 427).

All knowledge and all joint efforts at EU level could be bundled. The first step was to establish the EU-US task force, which was agreed during the EU-United States Summit in Lisbon. For a global problem, partnerships must be concluded with third countries, in particular with those countries that already have experience in cyber issues. Thirty percent of global trade is conducted as electronic trade. Ninety-nine percent of the businesses within the European Union are being signed with small and medium-sized enterprises. These are particularly popular victims for hackers due to lower security capabilities. The importance of this threat at European level is therefore very clear(Strasser, 2012). Further first steps concerns Europol and more coordination between EU-Member states. Europol will thus be the Resource Centre for cyber terrorism and cyber crime. To be effective at combating the cross-border threat, Europol will be equipped with new skills. Already in July 2010 the ‘cyber crime task’ was founded, which is to create a central file of criminal groups on the Internet. In addition, ENISA should conduct cyber security exercises in cooperation with states and private companies to raise the cyber-threat topic. The cooperation of EU Member States in the field of cybercrime would need to be increased significantly. Urgent requests for assistance from other EU Member States should be answered quickly to arrest

perpetrators. The now laid down measures in the new directive can only be a first step towards the effective protection against cyber attacks. Prevention and caution is still the best protection against cyber-crime(The European Circle, 2010). 'The issue of cybercrime must urgently be put in the Centre of a European debate, because cyber-crime does not stop at the borders(Strasser, 2012).' Therefore, a consistent approach by all member states on such complex issues is highly desirable to meet the objectives of both effectiveness and proportionality. The EU should avoid a situation where both law enforcement and the internet community would have to suffer from a patchwork of diverse technical and legal environments(Janczewski & Colarik, 2008: 428).

2. Cybercrime Convention

The Council of Europe's Cybercrime Convention is the first international treaty on crimes committed via the Internet and other computer networks. The convention covers infringements of copyright, computer-related fraud, child pornography and violation of network security. The convention contains a series of powers and procedures. It listed four main categories of criminal offenses:

* Offences against the confidentiality, integrity and availability of computer data and systems,
* Computer-related offenses,
* Content-related offenses,
* Offenses related to infringements of copyright and related rights.

The Cybercrime Convention mandates laws against cyber-crime and has the authority to provide officials with the necessary procedural authority to investigate and prosecute cyber crime offenses. Every EU-member state should ratify the International Cybercrime Convention as a step towards security integration. However, there are still a lot of doubts about the balance between private data protection and governmental investigation procedures. Moreover, there are some conflicts regarding human rights(Janczewski & Colarik, 2008: 433).

3. The US Approach

The American Government asked for new norms on the internet after Google was forbidden in China. However, the United States did not mention what procedures it will stop and what activities should be allowed on the Internet. Many intrusions into Chinese and American computer systems are reciprocal.

> Simply put, the United States is in a big way doing the very things that Secretary Clinton criticized. The U.S. is not, like the Chinese, stealing intellectual property from U.S. firms or breaking into the accounts of democracy advocates. But it aggressively uses the same or similar computer techniques for ends it deems worthy(Nye, 2010: 14).

One survey of cyber experts found that the United States was the largest source of global intrusions, followed closely by China(Nye, 2010: 14). The U.S. military recognized a growing threat in the mid-1990s to its informational architecture as well as the nation's critical infrastructure from cyber space. The U.S. Department of Defence(DoD) with its installations rely more and more on civilian infrastructure for communications, energy, water, transportation and the full range of logistical support. A threat to any of these critical infrastructures would have a heavy impact of the military deployable capabilities. Therefore, the U.S. military responded to this specific cyber threat on several levels. The U.S. military changed its organisation, doctrine, culture and last, but not least, the career force(Janczewski & Colarik, 2008: 439). Another U.S. approach was to create a Commission on Critical Infrastructure Protection. This commission started work in July 1996 and it truly was a joint government and private sector endeavour. The task of the commission was to establish a national policy and an implementation strategy for protecting critical infrastructure from cyber-attacks(Alexander & Swetnam, 2001). The U.S. differentiates between four major cyber threats to national security. Each cyber threat has its own time horizon and requires its own specific solution. These four categories are as follow:

* Cyber economic espionage
* Cyber crime
* Cyber war
* Cyber terrorism

VI. The UK's Approach and the New Cyber Strategy from Switzerland

1. UK Cyber Security Strategy

> Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty,

fairness, transparency and the rule of law, enhance prosperity, national security and a strong society(Maude, 2011).

To achieve this vision by 2015, the UK set four major objectives. First, the UK should tackle cyber crime and should be one of the most secure places in the world to do business in cyberspace. Second, the UK should be more resilient to cyber attacks and better able to protect its interests in cyberspace. Third, the UK should help shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies. Finally, the UK should have the cross-cutting knowledge, skills and capability it needs to underpin all cyber-security objectives(Maude, 2011). To reach these four objectives the UK Cyber Security Strategy described measures to break down the vision from strategic level to an appropriate operational level. It includes several actions on governmental and private sector and even with other countries or associations like NATO and the EU. The UK takes a risk-based approach to prioritising its response to cyber attacks. The UK Cyber Security Strategy tries to protect the citizens' right to privacy and other fundamental values and freedoms. It will continue to develop norms of acceptable behaviour in an international cyberspace environment. The goals of the UK Cyber Security Strategy are described as follows:

* People know how to get themselves a basic level of protection against threats online. They have access to accurate and up to date information on the online threats that they face, and the techniques and practices they can employ to guard against them.

* Individuals are careful about putting personal or sensitive information on the internet; are wary of email attachments or links from unrecognised senders; and are cautious about downloading files from websites they know little about.

* Everyone, at home and at work, can help identify threats in cyberspace and report them - for example, identifying fraudulent websites.

* Individuals play their part in transacting safely with businesses and Government, protecting passwords, understanding the importance of updating software and operating systems regularly and running anti-malware programs to help prevent their computers being used by others to increase the threat.

* People are clear that, as in the offline world, we are each responsible for our behaviour in cyberspace(including those who harass others, commit crime or 'hack' into systems(Maude, 2011).

2. National Cyber Defence Strategy of Switzerland

At the moment the Swiss Cyber Strategy is based on several theses and contains five possible areas of action. Basic research studies were done and the cyber project group has worked to finalise the results in a readable and understandable publication. Some theses are formulated to achieve the objectives which are non-negotiable, for example:

* The need for a clear political and legal framework;

* A consensus of all parties involved, that the developed solutions are proportionate and serve the purpose;

* The definition of an real strategic and operational responsibility and management process, which is financially and technically feasible;

* A risk and crisis management, which allows you to focus on the real problems with robust responses and puts the focus first and foremost on the critical infrastructures(including administration and security forces), as well as the economy;

* The creation of professional tools and resources, which layer-friendly can be customized, which are capable of through restraint and that will ensure the continuity of everyday life, also in cyber attacks;

* Provision of sufficient human resources, which have the need cyber skills(Vernez, *et. al.,* 2011: 12).

To live with these theses will not be easy due to the complexity of the matter, the diversity of actors and the rapid development of the threat. It is crucial to know for what we do, why it needs a cyber defence strategy and ultimately what justify its use. The contemporary vision is defined as follows:

> We want to protect the vital functions, based on the stability, security and prosperity of Switzerland; we want tackle cyber threats by using an oriented, dynamic dispositive of prevention, anticipation, deterrence, protection and intervention(Vernez, *et. al.,* 2011: 12).

3. Possible Elements of a National Cyber Defence Strategy

Already today, many actors at different levels are active, to protect Switzerland against cyber attacks. In addition, Switzerland tries to close recognized gaps and to establish primarily a supplementary strategy to consolidate the chain of existing procedures and resources. The aim is to cover the needs of everyday life and to cover the threats to security policy. This work must be carried out in close cooperation with selected foreign partners and international

organizations(UN, EU, NATO and OSCE). Today's perspective already shows the following elements of the future strategy:

* To create favourable conditions for the strategic crisis management. It takes a network of leaders from all sectors concerned, which permanently enables the exchange of information and the coordination of measures favourable conditions for the strategic crisis management.

* It will be necessary to bundle the resources of the national and technical defence. Switzerland should create a platform(in the form of a network), to provide access to information, solutions, analysis and protection measures. This platform has to run nonstop and should deliver a national 'cyber operational picture'. In addition, the platform should be able to analyse any form software, networks, and systems. Finally, the platform will be the national technical certificate authority.

* To strengthen the knowledge and ensuring a sufficient number of cyber skilled personal. Switzerland is already playing an important international role in research and in the development of information and communications technologies. The granting of a new generation of specialized professionals is a core activity(qualitative as well as quantitatively). This improvement has to ensure that our society can successfully master the growing importance of technology. Security is sovereign task bearing no 'outsourcing'.

* To reduce the human vulnerabilities. Every person and the society as a whole have to reduce their risks. Therefore, education at different levels is fundamental to reach this goal. Switzerland has to improve and develop its governmental and private sector institution of education.

* To strengthen the dispositive with customized legal standards. Besides adjusting existing legal bases, it will be necessary to develop new legal bases.

* To consider the international dimension. By definition in a global and international topic, creating a code of common behaviour at various levels of threat will be very important. Bilateral and multilateral coordination might be the key factor for success. The existing network has still space for improvements(Vernez, *et. al.,* 2011: 13-14)

To sum up, the strategy will let no freedom in action when it comes to the definition of the tasks, the definition of the responsibilities and the roles of the state and the private sector to protect the society against the cyber threats. However, Switzerland is forced to bundle its approach against cyber threats and has to establish one cyber defence centre. This might be an advantage for a small nation like Switzerland. Coordination and sharing information should be easier than in a medium sized state. Another advantage should be the fast adaptation of new circumstances for smaller states. A big disadvantage will still be the poor level of integration at international levels. Bilateral and multilateral agreements might be not the best solution to cope

with future threats. The UK and Switzerland have a lot of common standards and procedures in their cyber defence strategies. Both countries know the three levels of responsibility(individual, private sector and government). Both countries see the need to improve the educational level about cyber knowledge and both countries try to establish a common behaviour in cyber space. The schedule for a global player like the UK is without a doubt far more ambitious than the schedule in Switzerland. The UK will spend £650 million over the next four years and underlines its priorities with this measure(Maude, 2011).

VII. Conclusion

The importance of cyber space as an environment to conduct various operations against states or non-state actors is increasing. 'Cyberwar' tends to be a catchword for politicians and especially for the media. The lack of a coherent definition of cyber terrorism is still there. States were not able to define well different levels of cyber activities. Although there are existing definitions for different activities, it will take a long time for a global common understanding of this relatively new threat from cyberspace. Cyber terrorists already have a lot of cyber tools available and, in addition, terrorists may be well motivated with the possibility of creating significant media impact.

Governments and the private sector have realised over the last 15 years how vulnerable modern societies are. They have developed a lot of protection measures against this threat. The private sector has acted to improve business and the government has realised the interdependence between the private sector, national critical infrastructure and national security. The trend towards cohesion is positive. The area for future growth is international effective collaboration in cyber affairs. There is still no common global standard to share information and experience in this security field. The ratification of an international cyber convention is still a long way away. It is clear that despite disparities in state size, the end goals of cyber security policies of those compared states remain very similar. However, it is differences in the proposed methodologies that remain obstructive. The U.S. and the UK both give cyber threats a high priority for their national security and are therefore the leading nations in this affair.

Cyber terrorism is one level in several cyber activities and is generally an attack with a high impact on the society. The probability currently of significant attacks is relatively low. States realised the new threat at the right time and the counter measures seem to be being established pre-emptively. Security will never be integral and societies have to manage the risk which is left.

There is no doubt that governments may use this specific risks to secure financial interests and enlarge domestic control, however, tackling a growing threat of cyber terrorism must continue to be the objective.

References

Alexander, Yonah and Michael S. Swetnam. 2001. *Cyber Terrorism and Information Warfare: Threats and Responses.* Ardsley: Transnational Publishers.

Centre for the Protection of National Infrastructure. *The National Infrastructure.* http://www.cpni.gov.uk/about/cni/(accessed 4th May 2014).

Cordesman, A. H. and J. G. Cordesman. 2002. *Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland.* Washington: Praeger Publishers.

Cornish, Paul., David Livingstone., Dave Clemente., and Claire Yorke. 2010. On Cyber Warfare. *Chatham House.* November: 7-23.

Hoffman, Bruce. 2006. *Inside Terrorism.* New York: Columbia University Press.

Hutter, Reinhard. 2002. *Cyber-Terror: Risiken im Informationszeitalter.* Aus Politik und Zeitgeschichte(B 10-11 2002): 38. http://www.bpb.de/publikationen/NVN0CA,0,0,CyberTerror%3A_Risiken_im_Informationszeitalter.html#art0(accessed 2nd May, 2014).

Janczewski, Lech J. and Andrew M. Colarik. 2008. *Cyber Warfare and Cyber Terrorism.* P.A.: Information Science Reference.

Maude, Francis, MP, Minister for the Cabinet Office and Paymaster General. 2011. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf(accessed 5th May, 2014).

Möckli, Daniel. 2007. *Kritische Infrastrukturen: Verwundbarkeiten und Schutz.* CSS Analysen zur Sicherheitspolitik. http://www.css.ethz.ch/publications/DetailansichtPubDB?rec_id=607(accessed 20th May, 2014).

Nye, Joseph S. 2010. *Cyber Power.* Belfer Center for Science and International Affairs.

Strasser, Ernst. 2012. *Sicherheit im Internet: Ist die EU gerüstet, um Cyber-Kriminalität und Terrorismus zu verhindern?* EU-Infothek. http://www.eu-infothek.com/article/sicherheit-im-internet-ist-die-eu-geruestet-um-cyber-kriminalitaet-und-terrorismus-zu-verhindern(accessed 25th January, 2014).

The European Circle. 2014. *Die Zeiten des Cyberterrorismus Sind Endgültig Angebrochen. EU W appnet Sich Gegen Cyberangriffe.* http://www.european-circle.de/zukunftwissen/meldung/datum/2010/11/25/eu-wappnet-sich-gegen-cyberangriffe.html(accessed 3rd May, 2014).

U.K. Cabinet Office. 2009. *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space.* The Stationary Office.

U.S. Office of Homeland Security. 2002. *The National Strategy for Homeland Security.* Office of Homeland Security.

Vernez, Gérald, Roman Hüssy, and Riccardo Sibilia. 2011. *Cyber Defense der Schweiz.* Military Power Revue(Nr. 1/2011, Beilage der ASMZ 6/11 und RMS 3/11): 8-14.

Weimann, Gabriel. 2005. Cyberterrorism: the Sum of All Fears? *Studies in Conflict & Terrorism.* 28(2): 131-142.

Kwang Ho Chun: Professor and the Dean of the Faculty of International Studies, Chonbuk National University. He was previously an Associate Professor and Course Leader in Asia Pacific Studies, University of Central Lancashire, an Assistant Professor at the Defence Studies Department King's College London and the Defence Academy of the United Kingdom. He also taught as an Assistant Professor at Unité de science politique et des relations internationales, Université Catholique de Louvain, Belgium. He completed his BA and MA at Kyung Hee University, Seoul, Korea before completing his MA in European Studies, and PhD in International Relations at Katholieke Universiteit Leuven, Belgium. His research interests are grand strategy, asymmetric warfare and irregular warfare and published more than 10 books and monographs with more than 60 journal articles(khchun@jbnu.ac.kr).