Diplo Foundation IGCBP09 Research Phase

# A Synopsis of Cyber Warfare & Terrorism

**Prepared by:**

**Mr. Shreedeep Rayamajhi**
I GCBP09 Research D Security

**Submitted to:**

**Emmanuel Edet,**

Diplo Foundation Associate and Tutor

IGCBP09 Research Phase

**(emmanuele@diplomacy.edu)**

# Course Objective

## Aim

To empower the participants to take part in the IG process through competent policy research. The training will focus on developing research skills, defining the role of policy research in the IG process and on practical opportunities for becoming the part of the policy process. It is likely that many of you have never worked on a policy research; even those with experience in academic research might not have faced this specific format. Thus, the research phase aims at providing you with some basic skills to produce a policy research project – which is, to put your knowledge and analysis together in a comprehensive way and present it to relevant institutions, either local and regional or global.

## Format

During the research phase we will introduce the concept of policy research within IG through a short online course, followed by an exercise in form of the online policy research project that you will be working on. The short online course will be conducted within an online classroom – similar to what you have done during the previous few months. It will cover the following areas:

1) Introduction to policy research, including: the difference between policy and politics, what is policy research, who commissions policy research and who conducts it, and policy research in Internet Governance
(This module will give you clear understanding of the role and importance of policy and policy research in Internet Governance)

2) Conducting policy research, including: policy research methodologies, finding and assessing information on the web, and citations and plagiarism
(This module will bring the basics of producing policy research, i.e. how to collect and organise data, how to find reliable sources of information, how to introduce proper referencing, etc.)

3) Structuring information, including organising the information in a wiki format.

(This module will help you understand the format of wiki - the format you will be using when building your research later on – you will note the differences from a traditional paper format of research)

4) Using the wiki platform, including: how to use wiki, goals and examples (This module will instruct you how to use wiki platform, explain what is expected from you as a final wiki deliverable, and introduce some successful examples)

After the short course you will be working in a specific thematic area group to produce an online research portal using the wiki platform. Participants will be divided into groups per topic of interest, with the task of building up a predefined research grid with information and analysis of the situation. The most successful wikis will be promoted through the Diplo web and by Diplo associates at the IGF meeting in Egypt in November 2009.

**Topics**

Six topic areas have been proposed for this year's Research Phase, based on the most recent agenda of IGF and general interests in specific topics by the IG actors. They will be defined more specifically during the course, with appropriate sub-topics to ensure a coherent structure.

- e-Democracy
- Intellectual Property Rights
- Cyber-Security and Safety
- Infrastructure and Critical Resources
- Development Issues
- Regional LAC Group (Spanish)

After the short course, each of you will be assigned to a group which will produce a policy research wiki on one of these topics. Each group will collaboratively build up several general pages of wiki, under the guidance of the tutor. Then, each participant will be assigned a sub-topic of interest to work on individually by drafting several wiki pages, yet with peer-to-peer feedback and under the guidance of the tutor. At the end, the drafted wiki pages will be polished and interlinked to produce a whole wiki.

Due to the dynamic nature of wiki, allowing (and even requiring) it to be constantly updated, those interested to continue will be able to further update their research wiki pages in the future.

**Deliverables**

- Research course assignments
- Group and individual wiki pages
- Presentation of results

**Timeline**

The Research Phase will start with a short course on 1 September 2009.

1 September - 2 October (5 weeks): Online course
5 October - 8 November (5 weeks): Online research work

The wikis should be ready by 10 November. The most successful wiki projects will be presented at the IGF meeting in Sharm el-Sheikh, 15-18 November, though short PowerPoint presentations and a poster session.

# Content

# Abstract

Cyber warfare and terrorism is a fight of power where the big fish eats the small fish. The only way to solve it is by overcoming the barriers of discrimination in binding within the dynamic of standardization.

The aspect of Digital Divide and Net Neutrality should be overcome in the most proper way of abolishing discrimination giving substance to the right of information to all. According to Symantec, "Symantec blocked an average of more than 245 million attempted malicious code attacks across the globe each month during 2008. Phony emails, fake web sites and online ads trick innocent victims into divulging personal data like social security and credit card numbers. Cyber criminals then sell the information to the highest bidder on the online black market. Symantec (Nasdaq: SYMC) knows that cyber crime is real crime, that's why today, the maker of Norton security software, is bringing to market a completely unique approach to online security with Norton 2010."

Cyber space has become more vulnerable to externalities of fraud, scams, malicious threats, virus, hacking etc where being secured is a question that haunts everyone. So being secured certainly means being updated where one's security certainly lies at the stake of awareness in the every possible way. On contrary Cyber attackers and their technologies are getting sharper and smarter where the hackers and attackers are one step ahead of us keeping the technological boon manipulating the knowledge and availability in and against the innocent people.

***"Cyber space provide a psychology of war mentality where people win by utilizing others weakness and vulnerabilities and to some extent that limits the use of resources and in so many ways makes it efficient***."

Information of vital resources are easily available on internet, apart from that technical content of making bombs and other relevant terms are easily available on websites making it easy for cyber terrorist groups to harbor and train innocent people.

Apart from that Terrorist groups are increasingly attracted to modern communications technology for planning, recruiting, propaganda purposes, enhancing communications, command and control, fund raising and funds transfer, information gathering etc taking terrorism to the next level. This aspect of cyber terrorism materializes the flexibility of web information for expansion of terror around the world, which indeed is a slacking factor.

# A Synopsis of Cyber Warfare & Terrorism

## 1. Introduction

As technology is driving internet, Cyber space is expanding where virtually everything is possible from 3D animation to remote /open networking to e-banking to entertainment. With the advent of better technologies and systems, life has been a comfort to see and communicate in doing activities at both personal and professional level from one part of the world to the other. This open access and flexibility of the Internet has not only slaved people in enjoying the benefits of technologies but on the other hand the same accessibility is also threatening the system with inevitable threats like virus, worms, hacking, identity theft, copy rights issues and everlasting frauds and scams are tolling up. The dynamics of the open cyber space has not only connected the world in terms of speed, and accessibility but on contrary has also facilitated the wrong doers in effectively channelizing their knowledge to achieve their selfish motive by manipulating the global network in desired way.

However, the interconnection of network that started from a room, today hold the power to connect the world where one's existence is broaden within the virtual identity of seeing and feeling oneself in the 3D animation world of second life which is simply mind boggling. Amazing yet exciting, everything is virtually possible in its dimensions which plays with in the matrix of specific codes.

The expansion of cyber space not only gives space to greater efficacy of sharing and better business opportunity but perversely it has lured different externalities which are creating nuisance proving threat to security online. Perhaps, one might feel secure about one's status but in cyber space nothing is impossible. It is just the possibilities that are suppressed by the knowledge and experience of codes and skills where feeling secured is a theoretical definition that bites reality. Today, Cyber space is not just a platform of information access, it has adapted to a proactive version where different micro and macro elements, ranging from commercialization to technology to terrorism harbor their ultimate dimension of opportunities and possibilities.

Like such **Cyber Warfare & Cyber Terrorism** are some of the burning issues which threats the cyberspace and its operations.

## 2. Background

Cyber warfare and terrorism is the modern transcended version of insecurities of abuse and exploitation within the limitation of terrorizing adapting the modern form of technology and advancement. Reality is Cyber Warfare is a form of attack on a system from various ways making it convey a message or any form of message. Cyber Terrorism is a form of fear and dread utilizing the means of Internet to attack or hack computer systems of significance for acquiring top secret data or making it obsolete. Likewise, within the flexibility and accessibility of open network, terrorist groups are increasingly adapting the power of modern communications technology for planning, recruiting, propaganda purposes, enhancing communications, command and control, fund raising and funds transfer, information gathering, and the same. The true threat of cyber terrorism and warfare is not only aspiring in cyber space for its illegal act of taking control but alternatively is exploiting and manipulating people's psychology using the elements of discrimination, racialism, terror etc , which further is dividing people and creating differences. Some of the examples of cyber terrorism and warfare are mentioned below:

### Estonia Cyber Attack 2007/2008

Cyber attacks on Estonia (also known as the Estonian Cyber war) refers to a series of cyber attacks that began April 27, 2007 and swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters, amid the country's row with Russia about the relocation of the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn. Most of the attacks that had any influence on the general public were distributed denial of service type attacks ranging from single individuals using various low-tech methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements including that of the Estonian Reform Party website also occurred. Some observers reckoned that the onslaught on Estonia was of a sophistication not seen before. The case is studied intensively by many countries and military planners as, at the time it occurred, it may have been the second-largest instance of state-sponsored cyber warfare, following Titan Rain. Estonian Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyber attacks. On September 6, 2007 Estonia's defense minister admitted he had no evidence linking cyber attacks to Russian authorities. "Of course, at the moment, I cannot state for certain that the cyber attacks were managed by the Kremlin, or other Russian government agencies," Jaak Aaviksoo

said in interview on Estonian's Kanal 2 TV channel. Aaviksoo compared the cyber attacks with the blockade of Estonia's Embassy in Moscow. "Again, it is not possible to say without doubt that orders (for the blockade) came from the Kremlin, or that, indeed, a wish was expressed for such a thing there," said Aaviksoo. Russia called accusations of its involvement "unfounded," and neither NATO nor European Commission experts were able to find any proof of official Russian government participation. As of January 2008, one ethnic-Russian Estonian national has been charged and convicted.

During a panel discussion on cyber warfare, Sergei Markov of the Russian State Duma has stated his unnamed aide was responsible in orchestrating the cyber attacks. Markov alleged the aide acted on his own while residing in an unrecognized republic of former Soviet Union, possibly Transnistria. On March 10, 2009 Konstantin Goloskokov, a "commissar" of Kremlin-backed youth group Nashi has claimed responsibility for the attack.

(Source: http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia)

**Twitter Attack 2009**

As Twitter struggled to return to normal Wednesday evening, a trickle of details suggested that the outage that left 30 million users unable to use the micro-blogging service for several hours - at least in part - may have been the result of a spam campaign that targeted a single user who vocally supports the Republic of Georgia.

According to Bill Woodcock, research director at the non-profit Packet Clearing House, the torrent of traffic that brought the site to its knees wasn't the result of a traditional DDoS, or distributed denial of service attack, but rather people who clicked on a link in spam messages that referenced a well-known blogger called Cyxymu.

(Source: http://www.theregister.co.uk/2009/08/07/twitter_attack_theory/)

**South Korean Attacks**

South Korea is experiencing a third wave of suspected cyber-attacks - co-ordinate attempts to paralyze a number of major websites. One of the country's biggest banks, a leading national newspaper and the South Korean spy agency appear to have been targeted. Some reports suggest the attacks might be the work of North Korea. South Korea and the US reported similar attacks earlier in the week, with the White House

and the Pentagon targeted. The South Korean government, and the country's internet service providers, are still trying to fight off what appears to be a deliberate attempt to shut down major websites that began earlier this week. In what is known as a "denial of service" attack, thousands of virus-infected computers are hijacked and simultaneously directed to a particular site, overwhelming it with the sheer volume of traffic.

(Source: http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm)

## 3. Cyber Warfare

Technically speaking, Cyber Warfare refers to any considerable act using computers and engaging in warfare activities by any means in targeting or causing any harm to the websites or groups in cyberspace with a selfish motive is called **Cyber Warfare**. This includes vandalizing websites, circulating false information, misguiding and rejection of service attacks, creating false accusation and propagandas, and gathering classified data in the cyber space.

Cyber warfare is overcoming the expectation of researchers and security analysts in every possible way posing a high level threat to any country. With high strategic target results and precision, its use should not be underestimated as it is highly flexible and hard to detect. The low cost allows training or hiring a team capable of doing more damage than battle fields. Moreover, the digitizations of conventional warfare technologies as well as the development of new Artificial Intelligence weapons with more complex devices jeopardize the security as well as opens risk of cyber warfare in expanding and strategizing the cyber attackers to strategize their plans within the loop holes.

Previously, when strategic battle operations were performed manually on papers and then in action have further taken a step ahead where the new development of weaponry have substituted the older version with effective technological advancement of Global Positioning Satellite(GPS) and Smart computers. The operation which were once carried out by human operators with average success rate of 70% have exceeded to 99.9% with unmanned Artificial Intelligence and smart computers. The precision rate not only shows the success of artificial intelligence but reluctantly shows the great risk of control and management of such system.

The cyber space not only gives space for entertainment but on contrary shares the same with highly sophisticated weapons of mass destruction which are connected to each other by cyber space and relative technologies. So with just a loop hole, massive cyber attacks can take form of a cyber warfare where time ticks with no option except to wait for consequences.

Reality is we are gaining power in developing weapons of smart technology which are much more faster, efficient and precise but we fail to address the question at what cost or risk. We can calculate the damage that these weapons can result in but what if the table turns the way round and the same system which were develop to fight against terror goes in control of such people. This is an important question which hunts every security analyst and is a curial issue regarding cyber security.

Realizing, the technological advancement, cyber space has been the most happening business opportunity for any field from economy to finance to industries. Especially in developing countries where the booming of internet is being grasped with higher effectiveness, posses a high threat to the people of that region. As technological advancement are being adapted with greater effectiveness, the attacker (hackers) are also gaining technological advancement to the level where they are much faster, better and precise than any security system. The basic problem that has been encountered in most of the developing countries is acceptance of technology seems very easy but maintaining its substance is a question. The problem arises when the system gets manipulated by attackers in desired way due to lack of proper infrastructure. And in most cases the country lacks to address the issue of cyber policies and proper mechanism where problems like cyber exploitation, child abuse and pornography, Hacking and Virus and scam takes its toll. When not addressed with effective measures, it just results like giving a knife to a kid. The possibilities that can be imagined are endless. So the effectiveness of internet takes the form of threat where at times these vacuums of system loop holes can take the form of cyber attacks and the consequences can be irreversible and most damaging.

For example, hacking the main control system of a dam and opening the gates of a dam is a technological possible to the modern society where the technologies threats the society. The consequence can be carnage of thousands of innocent people. Similarly, releasing weapons of mass destruction may have catastrophic results.

Likewise, Two years ago, a political dispute between Russia and Estonia escalated when the small Baltic country came under a sustained denial-of-service attack which disabled the country's banking industry and its utilities like the electricity network.
This was repeated last year, when Georgia's web infrastructure was brought down on its knees during its conflict with Russia.
(Source: http://news.bbc.co.uk/2/hi/business/davos/7862549.stm)

Thus, Cyber warfare is a relatively a concern topic for all from developed to developing countries who are exploring the depth of advance weaponry and other facilities of cyber space. It needs to be well thought within the pros and cons which need to be restricted within the accessibility of its use and operation.

## 3. 1 Protection against Cyber Warfare

The main protection against cyber warfare is getting your prepared and secured with the necessary software and firewall that are available. Protection against cyber warfare in real sense means, being aware about the issues and happenings of cyber space. Every security measure that is performed by a non-human device in the digital world is a member of this group. From the emails that are being received or send to the antivirus that are installed as preventive measure everything needs to be operational and well working. One should also be focused on the happenings and the invention where keeping up-to-date is the key to protection against cyber warfare.

The current ongoing racket of Spam is also a perfect cyber warfare weapon. Spam is a low intensity, diffuse, and persistent attack which targets the desired segment and relocates the strategy according to their motive. In cyber war, the information infrastructure is the medium that is being targeted and impacts the most in retrieving the desired information or manipulating the system making it obsolete for its performance. So to prohibit this we need to focus on security systems that could stand against the attacks here are some of the options which are very much in use:

a. **Encryption:** Encryption is a set of coded algorithm that converts important data's into blocks of unrecognizable format which prohibits the information from any illegal use. It is a process of converting data using algorithm into secured form preventing it from any kind of abuse or use. Encryption is not a fully secured security system as algorithm codes can be channelized and manipulated in possible way but to a level they do prevent from illegal use and to certain option they do act as a saviors.

b. **Network Security:** Network security is a curial issue for any Network Administrator in safe guarding the networks and peers connected to the network. Network security is a broad term that encompasses issues likes proper infrastructures and policies that facilitates the successful use and control of network in the most prominent way giving equal opportunity for grow and expansion. Network security simply helps in protecting the boundaries of its limitation and excludes trespasser in safeguarding the valuable information. Network security is a very prominent option of security against attackers.

c. **System Security:** System security refers to the individual system that protects information and data from theft, tampering and abuse by any unauthorized use,

giving substance and flexibility to the desired users in acquiring the information as per their needs. For examples the antivirus, firewall etc.

**d. Application Security:** Application security is specifically related to an application life cycle process that takes effective measures in safeguarding the vulnerabilities that are open during the application process. The application security also prevents any breach in security policy while designing, development, upgrading and maintenance of the application process.

**e. Security Monitoring/Auditing:** Security monitoring and auditing refers to constantly watching and updating the policies, regulation and mechanism according to the need of environment. It results in creating effective and efficient environment for safe use of the system in every possible way prohibiting any manipulation and abuse. A system with its network security needs to be constantly watched with relation to global happening and update itself with the technological upcoming. It's the basic need where lack of update might result in system vulnerabilities. As attackers always seek for loop holes and once the system becomes vulnerable, they certainly don't miss their chance.

## 4. Cyber Terrorism

According to the U.S. Federal Bureau of Investigation (FBI), "Cyber Terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." Cyber terrorism is also referred as electronic terrorism or informational war where the diversion of information can create obstructing situations. Cyber terrorism attacks are strategically designed to maximize damage both physically or financial. The possible cyber terrorist targets are public interest properties like banking industry, television and communication station, military installations, power plants, malls and business centers, water systems etc.

Thus, Cyber terrorism is a criminal act of punishment subjected to wrong use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services in any possible way with the intention of damage to any sector in any possible way. Reality is the information that are easily available on

website can be wrongly used or manipulated in desired way to result in mishaps in a scenario of possibility.

Similarly, few years back a huge concern was raised regarding the satellite mapping images of Google earth to potential high profile places and its possibility of use by terrorist organization. Later the issue was hyped and took a form of a ban which was enacted highlighting the potential threat of terrorism. I believe cyber terrorism is such a vague topic where it threats human society in every step as internet has acclimatized 21st century in the most profound way.

Information of vital resources are easily available on internet, apart from that technical content of making bombs and other relevant terms are easily available on websites making it easy for cyber terrorist groups to harbor and train innocent people.

Apart from that Terrorist groups are increasingly attracted to modern communications technology for planning, recruiting, propaganda purposes, enhancing communications, command and control, fund raising and funds transfer, information gathering etc taking terrorism to the next level. This aspect of cyber terrorism materializes the flexibility of web information for expansion of terror around the world, which indeed is a slacking factor.

### 4.1 Reasons for popularity of Cyber Terrorism

Cyber Terrorism is the next step of terrorism adapting the advancement of technology and system which profuse in utilizing the flexibility by targeting the loop holes of cyberspace and materializes its substance. The basic attractions of Cyber Terrorism are high impact, use of less resource, cost effective, fast, untraceable and effective in every possible way that is yet to be discovered with the booming technology and advancement.

a. **Perceived Secrecy:** Cyber Terrorism gives an advantage to such groups in falsely creating an image in cyber space giving easy results to their bad intention in the most prominent way. The easy use of false IP and other flexible options that are readily available in the open network makes it easy to target others and attack them from safe distance. The accessibility of open source and easy hacking is also an option which facilitates cyber terrorism in opening the loop holes and utilizing it according to their personnel needs and wants.

b. **Diverse targets:** Internet today is connected to every part of the world, and there is relatively a question about who or what is not associated with it? The diverse aspect and the dynamics of internet in growing prospect have certainly attracted all fields from life making it the most happening thing. From social networking to easy access online chatting internet is the most happening thing which certainly gives stance to target vulnerable groups as easy targets of cyber terrorism. The feasibility of the cyber space provides an advantage to the terrorist groups to harbor extort and train innocent people in desired way. The availability of easy accessibility certainly helps in manipulation making discrimination, racialism, enthusiasm, aggravation etc as a tool in expansion of their terrorist group. The Internet certainly has open doors for opportunity but on the same has invited inevitable risks which are tolling in for externalities. These factors are very progressive and efficient in many ways where the flexibility of internet has been an advantage for them and a curse for the innocent people online.

c. **Low risk of detection:** The Dynamics of internet is so vast and vague that the possibilities of its existence and application are yet to be discovered. Internet provides a vast ray of software and codes that can virtually make you vanish in cyber space and gives you the power of low risk detection. Apart from that these days the easy access of open network sharing can allow you to access the net imaging a false IP and further gives the accessibility to do stuff that can just be imagined.

d. **Low risk of personnel injury:** Cyber space certainly provides the advantage of low risk of detection using the help of different software where the risk of injuries to the resource are also very low or nil. Thus, it results in easy access and impact with just a touch of button which very efficient and effective in terms of strategy. With just the help of an attacker, devastation can be resulted in seconds using less resource. So low use of resources refers to low detection and low detection gives substance to low risk, and may be this is the reason why cyber terrorism is such of a threat. Likewise, it is said that impact can only create a damage of certainly level but experience can damage more than anything.

e. **Low investment:** Low Investment is a prominent factor that attracts cyber terrorism to cyber space. Previously, when millions of dollars were spend on

weapons and training on battle field and the output or damage was limited in battle field. Now, the impacts are very high and the use of resources is also very limited but the result can be very big and damaging. ***Cyber space provide a psychology of war mentality where people win by utilizing others weakness and vulnerabilities and to some extent that limits the use of resources and in so many ways makes it efficient***. Reality is with an efficient human resource and low investment in a hard ware and software, the impact could be immense which is an effective strategy.

**f. Operate from nearly any location:** The easy accessibility of internet certainly provides an opportunity to operate from any desired location virtually making you invisible is a simple trick. The possibility of sitting in a remote location and resulting damaging some thousands of kilometers away is an advantage of the open network.

### 4.2 Key Measures for Protection against Cyber Terrorism

1. All personal information and crucial data should be protected and should not be displayed
2. Effective password combining characters, numeric and strings should be used to protect all accounts online
3. Whenever the network encounters errors, the network then should be reconfigured and enabling all protection software
4. Timely update of the security system prevents from encountering new errors
5. The system administrator should keep a close eyes in the system logs and its uses

## 5. Key Players or Stakeholders of Cyber Warfare and Terrorism

Cyber security basically follows the combination of three aspects People, Systems and Procedures. Systems and Procedures are the key factors developed by peoples, so human resources play a pivotal role in controlling and operating the cyber-security and defense initiative. More often it's the human ambition and resources that makes the system work against each other creating conflict in fulfilling their selfish motives. The system certainly defines the role and scope where human ambition creates the opportunity, resulting in the possibilities of damage. The basic key player in cyber warfare and terrorism are listed as below;

1. **Policy System:** Policy System is an important mechanism that tackles the policy level in creating and defining scenario in and against the policy mechanism. The policy system is the most prominent system that setup the boundaries for the pros and cons safeguarding the rights of normal people who use the system with in the periphery of that location. Policy defines the role and scope of development and growth making the system secure from vulnerabilities and externalities.

a. **International Security Council:** International Security Council is the main body that sets standards in safeguarding the rights of its user from every angle possible. The council also involves in proper growth and development within the frame work of developing effective policy and regulation. It also monitors and further researches into issues of concern where its role is very prominent in policy design and further grow and development. For example some of the international Security Council is Internet Engineering Task Force (IETF).

b. **Government body:** Government Body is the main authoritative body that's responsible for the overall management of the internet infrastructure and other security issue in its periphery. Its responsibilities are very much dynamic to the changes and happening that affect the industry and should always keep an eye open.

c. **Country's home security system:** The country's home security is also an important system as it protects the system and network from hackers and intruders. If the system is not effectively protected then it certainly makes the entire network and its peers vulnerable and they most likely to become prune to attacks. Installing an effective security system is the utmost need where as updating and maintaining the security system is its priority.

c. **Intelligence System:** Information is the key to any system and especially about the enemy is a key winning factor which can make a huge difference in the battle or warfare. Gathering information about enemy tools and cyber-security systems is as valuable as maintaining a security system. Even at a company level it is important to know what kind of new security tools are being developed and its resourcefulness. So having an effective intelligence system certainly helps in safeguarding the country as it basically acts as a preparation of what can happen and what could be done?

2 **Key Players/Stakeholders:** Key players are the main stakeholders who play an important role in the industry. They are the main people who run and inhibit the industry bearing all the happening and consequences where they try to work their operation within the limitation of policies. They aspire the limitation

where they help the industry to expand and grow in the most effective and efficient way.

a. **Experts:** Security experts are the key players in the cyber-security defense force. They play a crucial role in designing and developing firewalls and other security measures. Without these people a country or a company needs to rely upon external help that may or may not be successful or viable.

b. **Systems Programmers:** Adapting the knowledge of security requirements and new security loop holes, system programmers are the essential key players who corrects the errors and try to integrate the systems effectiveness in the best possible way. The knowledge of system and skills in programming helps in taking effective measures and helps to progress the IT industry as well as cyber-security

c. **Hackers:** Hackers are the essential key players in the fight against the security issues. They play a very important role from both sides' protection as well as attacking. From protection side they help to understand the progressive psychology of their breed and help to understand their coding techniques and behaviors in cyber space. Hackers tends to do security consulting where they help the security experts in identifying the loop holes in the system and in collaboration they work their ways with security experts to cover them all.

d. **Cyber Terrorist:** Cyber Terrorist is a specific new term which in the verge of exploring its depth. Though the terms itself is not clear but the relative definition of a cyber terrorist is very dynamic and broad. A Cyber terrorist is a well equipped person with enough knowledge to act as threat to modern information systems, especially to the nation's defenses and critical infrastructure. His capabilities don't limit him from any specific definition but he is a top priority security threat to any country at national level.

3 **Target Group:** Target group are the vulnerable groups who are open for any sort of attack and have to bear the consequences in case of any attack. They are always the center of attraction where, it depends upon their initiation and alertness to tackle an attack. The target group can be of different level, country level, organizational level and individual level. It is the most important aspect of any attack strategy that suggests target group are instigates at different level according to the intensity of attack.

## 6. Prospect of Developing countries in Respect to Cyber warfare and Terrorism

Cyber warfare and terrorism are the growing aspect of threats to the developing countries where the chances of damages are very high and prominent. Though the technological advance have given us an edge in protecting & safeguarding our system and network in a more efficient and effective way; the same is also providing an effective medium for cyber attackers to develop further hard attack mechanism which are even faster, efficient and effective. Likewise, the ongoing discrimination of bandwidth, lapse of security policies, standardization, access and flexibility have resulted in a vacuum in between the developed and developing nation where internet acts as common medium for both but with double standards. These double standards are creating specific loop holes where the cyber attackers are manipulating and strategizing their obstructive motive that victimizes and facilitates the prospect of Cyber warfare and terrorism.

a. **Digital divide:** Wiki defines, "Digital Divide refers to the gap between people with effective access to digital and information technology and those with very limited or no access at all." So the difference in the technology makes the stronger fish eat the smaller fish where innocent people with limited technology and knowledge are 24/7 exploited by every means possible. The frauds emails, fake identities, fake websites, scams, hacking, viruses etc are some of the prominent products that are harbored due to digital divide.

b. **Lack of net neutrality:** Net Neutrality refers to the freedom in sense of accessing information or any means of communication in cyber space. It basically refers to no discrimination prioritizing the rights of information access. If there are discrimination maintain then it's certain that it will be wrongly used, so lack of net neutrality certainly plays crucial role in giving an upper hand to the exploiter to target the vulnerable groups in cyber space.

c. **Standardization:** Standardization is an issue that has been in question from the beginning. Standardization is the set of rules, regulation and policies that needs to be acquainted with the system. Lack of standardization results in conflict between users and parties which gives room for externalities. The lapses of policies and regulations are well manipulated in serving the selfish motives where the exploiters are always in search of such loop holes.

d. **Lack of effective technical human resources:** Especially in developing countries the lack of human resource impedes the systems. The technological transfer is very much in air but due to lack of proper human resource the systems gets underestimated where the exploiter benefit the loop hole in manipulating their selfish motives.

e. **Piracy:** Piracy has been a problem in internationally. In cyber space pirated software can cost you more than what it cost in real resulting in great security lapses. Specially in developing countries due to lack of awareness and rules piracy is very evident where people promote it unknowing jeopardizing their security in view of saving few bucks. The problem of piracy can be overcome by effective channelization of standardization giving stand to social responsibility of big software companies toward the developing country.

## 7. Current and Past events

The annual E-Crime congress is one the largest gatherings of those who work to combat cyber crime. Delegates included banking experts, police and IT industry luminaries, all keen to discover new ways to fight online crime.
The prospect of internet-based warfare has come to the fore after a series of high-profile international attacks. Last year, it emerged that a gang of hackers, believed to be from China, had infiltrated computer systems at the Pentagon and launched attacks on government networks in Britain, Germany, India and Australia. US officials, who have labeled the group Titan Rain, have accused them of operating under the auspices of officials in Beijing.

David Davis, said “Cybercrime is a growing and serious threat to individuals, business and government. It is a problem that will continue to escalate as technology changes,"

## Cyber Warfare 2010, is a event scheduled for January 27 - 28, 2010 CCT Centre, Canary Wharf, London, UK

- Insights into the evolving cyber threats to national security and information systems and evaluation of solutions to mitigate the threat
- Analysis of current and future legal issues, political pressures and challenges surrounding Cyber Warfare attacks and appropriate national cyber space activity

- Evolving national policy and doctrinal updates of Cyber Security and Cyber warfare from the UK MoD, US DoD, Estonian MoD
- Examination and lessons learnt from cyber attacks with insights from NATO studies and the Estonian MoD
- Latest technology updates in cyberspace and current research and development for both Computer Network Defence and Computer Network Attack

(Source: http://www.cyberwarfare-event.com/Event.aspx?id=228104)

## The 3rd International conference on IPRs, Personal Data Protection and National Security, October 20 – 22, 2009 in Beirut, Lebanon

The conference is co-organised by Lebanese Information Technology Association (LITA) and International Association of Cybercrime Prevention (AILCC) and hosted by University of Saint Joseph in Beirut. The event is held in cooperation with Interdisciplinary Center for Law and ICT , Belgium ; The Higher Council for Science and Technology, Jordan ; The Ministry of Administrative Reform, Lebanon and Microsoft Lebanon.
On behalf of the organizing Committee, we sincerely invite you to attend the conference and/ or submit your full research paper before 1st October 2009 focusing on Law, IT and Cyberspace issues such as, but not limited to:
Privacy issues in cyber society
- Cybercrime
- Intellectual property rights
- Consumer protection
- Internet security
- Bio technology
- Nano technology
- International trade law
- E-business
- Trademarks and domain names
- Patents
- E-commerce
- Jurisdiction in cyberspace
- E-banking and e-business
- E-signature and Computer forensic

## Call for Papers – ISSCRIM 2009, João Pessoa – Paraíba, Brazil (21 and 22 May, 2009)

Under the auspices of CCRC, International Association of Cybercrime Prevention (AILCC) in France and Universidade Federal da Paraíba (Brazil) invite you to participate in: **"International Conference on Cybercrime And International Criminal Cooperation"**

This conference is an opportunity for academics and consultants to exchange ideas and discuss most recent topics focusing on cybercrime and cyberlaw.

Bringing together leading academics, experts and professionals from all over the world, the conference discusses privacy, security, information technology and other cyberlaw issues.

We invite contributions focusing on cybercrime issues such as, but not limited to:

- Organized Crime
- International Criminal Cooperation
- Child pornography on the Internet
- Cybercrime in Brazil
- Cyberterrorism
- Intellectual Property Rights on the Internet
- Online Tax Fraud
- Information Security
- Bio – Technology
- Consumer Protection
- Privacy and Freedom of Expression in Cyberspace
- E signature

## 3nd Annual Fraud &Corruption Summit, 18THth-20th March 2009, Brussels

Expanding on the unprecedented success of previous summits held in Copenhagen and Stockholm, the 3rd Annual Fraud &Corruption Summit focuses on the detection, prevention &investigation of fraud & corruption and related financial crimes. It brings together (as a team) the disciplines of corporate audit, security, fraud prevention, corporate responsibility and risk management and has the backing of various chapters of the IIA, ISACA, ASIS and ACFE.

## Global Fraud Summit 2008, 14-17 October 2008, Singapore


Date: 14th - 17th October 2008
Location: Singapore
Web
url: **www.globalfraudsummit.com**
Today, businesses are fraught with fraud. 90% of white-collar crimes are now committed by companies' own staff. Why the increase? Companies must boost their internal controls, compliance and anti-fraud framework. However, establishing one is tough. Training and awareness, gaining trust among employees are challenges the fraud manager has to tackle.

Furthermore, fraudsters have an international syndicate and they have also made use of technology as a means to defraud their organizations. Fraudsters these days get away without punishment as sometimes, companies do not wish to bear the brunt of losing their reputation. So how can there be a system to alert that the fraudster is on the lose? Do whistleblowing tactics work? What are repercussions of the whistleblower? Dare anyone be the whistleblower in the Asian context?

This summit will address strategies, theories and practical methodologies to prevent fraud, dismiss the idea of cheating and have policies for control.
Interested to participate, please go to www.globalfraudsummit.com/enquire.php for more information!
For priority booking, please quote priority code VHU715

## CYBER SECURITY EXPO October 16, 2008


Date: 16th October 2008
Location: Memphis, USA
Web url: **http://cfialab.memphis.edu/expo**

The University of Memphis Center for Information Assurance will host the 2008 Cyber Security Expo at the FedEx Institute of Technology on October 16th. Information Assurance and Cyber Security experts will be on-site for lectures, networking and training to address emerging trends in cyber security. We are proud to have a renowned keynote speaker for the event, Daniel J Larkin. The Expo will also feature many

relevant exhibits and booths from a variety of significant venues. Sponsors, exhibitors, and participants are urged to contact us as soon as possible.

**International Conference on Digital Evidence, 26th - 27th June 2008 -London, United Kingdom.**

This is the first conference of its kind to treat the subject in such a global context, and without the traditional sole focus on e-disclosure.


MIS Training has partnered with Stephen Mason, Barrister, Editor, Digital Evidence and Electronic Signature Law Review, Associate Senior Research Fellow, Institute of Advanced Legal Studies, London &Visiting Research Fellow, Digital Evidence Research, British Institute of International and Comparative Law (UK) for this timely conference.

Hear from the international speaker panel which spans over 17 different jurisdictions. Lawyers, barristers, IT investigators, in-house counsel and digital forensics experts will present you with the most current reports from around the world.

Judges, lawyers (in-house lawyers as well as lawyers in practice), digital forensic specialists, police officers &IT / security directors responsible for conducting investigations will find this of tremendous benefit - as the unique chance to compare the real &problematic issues that surround digital evidence.
(Source: http://www.crime-research.org/events/)

## 8. Prevention against Cyber Warfare and Terrorism

Stopping the attacker is the primary concern for any system. The top priority of any system is to keep itself sustained while in operation and when it rests. A system is more active when it's operational but on contrary it also becomes more vulnerable during its processing. If it is not protected with effective security programs, it gives advantage for attackers to try their luck. Most of the attacks are very simple and straightforward and a good prevention is to simply lock it, unless somebody expects an army trying to enter. So the bottom line is a system is never too strong or weak, it's the resourcefulness of the user to make the system more effective and efficient to fight against the loop holes of the system and to correct it with effective security program and mechanism.

Main tools in this category are:

I. Firewalls: Fire wall is a part of system encoded security access program that prevents from unauthorized access to or from a private network while permitting authorized communications. A firewall is a complete system that is implemented in a both computer hardware and software.

There are several types of firewall techniques:

a) **Packet filter:** Packet filter is technique of checking the packets of information that is sent in-between the network and accepts or rejects it based on user-defined rules.
b) **Application gateway:** Its s security mechanism that monitor the specific application like FTP and Telnet servers. This system is very effective but slow down the operation speed.
c) **Circuit-level gateway:** This technique is specifically used to monitor the flow of information during the connection of TCP or UDP. After the connection is made the information can flow without further security checks.
d) **Proxy server:** It helps to intercept all the information that goes between the network connection and effectively hides the true network address· Authentication systems.

II. **Authorization systems:** Authorization system refer to a mechanism which helps a user to access a system according to the priority level that he or she has been assigned to and effectively channelizes the mechanism in sustaining and accessing the resources according to authority that has been defined for him or her.

III. **Network scanners:** Network scanners are specified sets of software that analyzes a network to determine its exposure to unwanted intruders. It is also known as vulnerability scanners. These software checks the clients PC servers, routers, firewalls, network appliances, system software and applications for vulnerabilities that include open ports, back doors, poorly written scripts and blocks the operating systems from such threats.

IV. **System scanners:** System Scanners are individual scanning software that scans the system and its system files for security vulnerabilities that are implemented

in any form of email or code or any sort of cookies. The system scanner are completely update based which are directly interconnected to their host software which updates it on regular basis.

## 9. Allegation and Controversies toward Developed nation

a. Most of the developed countries transfer their technologies in motives of their business development but they fail to address the relative issues of standardization and policy.

b. The Digital divide and the discrimination of net neutrality is a concern of developing countries where they are bound to face the consequences.

c. Most of the acts of cyber warfare have been a result of power manipulation to showcase their presence in view of making the target fulfilling all the demand of the attacker.

d. Most of the attacks have been targeted from developed countries to developing countries where the developing countries pay the consequences of lack of proper infrastructure or policy.

e. Hippocratic mentality of developed countries in using net neutrality and digital divide as medium of political manifesto.

f. The international agencies related to cyber space are bias to developed countries in giving them an authority and manipulation where they rule their business.

g. Lack of effective human resource is subjected to developing countries where the attackers are one step ahead.

## 10. References


1. Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI, "Congressional Testimony, presented before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security," February 24, 2004, http://www.fbi.gov/congress/congress04/lourdeau022404.htm
2. Brenner, S. (2009). *Cyber Threats: The Emerging Fault Lines of the Nation State*.
3. "New 'cyber attacks' hit S Korea". BBC News. 2009-07-09. http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm.
4. Williams, Martyn (2009-07-14). "UK, not North Korea, source of DDOS attacks, researcher says". IDG News Service. http://www.networkworld.com/news/2009/071409-uk-not-north-korea-source.html?ap1=rcb.
5. "Pyongyang blamed as cyber attack hits S Korea". Financial Times. 2009-07-09. http://www.ft.com/cms/s/0/61bc6d22-6c1f-11de-9320-00144feabdc0.html.
6. "Governments hit by cyber attack". BBC News. 2009-07-08. http://news.bbc.co.uk/1/hi/technology/8139821.stm.
7. Markoff, John (2009-07-09). "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea". The New York Times. http://www.nytimes.com/2009/07/10/technology/10cyber.html.
8. "Cyber Attacks Hit Government and Commercial Websites". Foxreno.com. 2009-07-08. http://www.foxreno.com/news/19999665/detail.html.
9. "US State Department under cyberattack for fourth day". AFP. 2009-07-10. http://www.google.com/hostednews/afp/article/ALeqM5jnGA5yrkZlqmNHmhctub8FuA9TbA.
10. Jiyeon, Lee (2009-07-11). "Cyberattack rocks South Korea". GlobalPost. http://www.globalpost.com/dispatch/south-korea/090710/cyberattacks.
11. Kim, Kwang-Tae (2009-07-12). "S. Korea analyzes computers used in cyberattacks". http://www.google.com/hostednews/ap/article/ALeqM5jO5PtkM_1FjwMZjh3LS74g26yiUQD99CRCO80.
12. Zetter, Kim (2009-07-08). "Lazy Hacker and Little Worm Set Off Cyberwar Frenzy". Wired News. http://www.wired.com/threatlevel/2009/07/mydoom/.