Global Scientific JOURNALS

GSJ: Volume 8, Issue 1, January 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

# CYBER ATTACK: AN EMERGING WAR

Lilian O. Aluede & Engr. Peace B. Biragbara

KeyWords
Cyber attack, Denial-of-service, Internet security, loophole, network, risk control, terrorism.
.

## ABSTRACT

This research work aims to review “cyber attack” being a significant global risk in terms of likelihood of occurrence stipulations; it will further evaluate the mechanism for attacks, and develop control measures for future attacks.

Using the Russia and Georgia cyber conflict in 2008 as a case study, this paper will elucidate the effect of cyber attack on a nation, designs a contextual diagram of the relationship between cyber attack and other World Economic Forum (WEF) identified global risks. This work identifies the possibility of cyber attack triggering terrorism, organised crime, global governance failure, massive incident of data fraud or theft and critical fragile state if left uncontrolled.

This paper implements the ISO 27001 ISMS Model of PLAN, DO, CHECK ACT to management of cyber attack risk; using reports, computer journals, peer reviewed articles and internet sources, will design a cyber attack risk control hierarchy strategy in organizational context to combat this emerging challenge.

## 1. INTRODUCTION:

One notable trend of the global age, is the emergence of Internet of Things (IoT), where the world is dependent on the merger of telecommunication and computers that are web-enabled, networked and vulnerable (Information Communication Technology) for financial transaction, shopping, communication, research and development and almost everything.

World Bank Group (2014) shows that daily 43.1% of adults worldwide use the internet, while (ITU 2014) estimated 39% of world's population. Averagely 41% of global population, who uses the internet daily, are prone to cyber attacks.

Internet is interconnected network, capable of sharing data and communicating with another network but owners of these data do not grants access and rights, rather it is done by administrators according to function (Fernadeze 2001).

Just like every open access, there is no restriction as to who accesses what information, thus, the Internet offers anybody, and any country, a deviated approach to assemble cyber-power, and as such, even terrorist depends on the cyber space to perpetuate cyber crimes.

Cyber attack dates back to the America Civil war in 1862, when Thomas Freeborn went ashore to truncate the Richmond and Federicksburg telegraph lines in other to disrupt their communication , and in 1905 Russia used the radio jamming mechanism in the Russo-Japanese war (The Economist (2008). Since the emergence of computer age, many nations have engaged in cyber war, like that of China and America, Russia and Estonian in 2007 and the 2008 Russia attack on Georgia, which will be used as case study for the purpose of this research. Scholars have tried to explain/ defined the context of cyber attack, linking it with cyber terrorism, cyber warfare, cyber exploitation and some just simply refers to it as cybercrime. Only a few have been able to give a standalone definition of the term 'cyber-attack'.

## 2. WHAT IS CYBER-ATTACK?

Cyber-attack is a "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks' (NATO 2010: 71, Owens et al. 2009 and Lin 2010). Joynal 's (n.d.) definition of cyber attack incorporated "potential to degrade national economic systems and communications networks as a means of breaking the enemy's will to resist and inflicting military and political defeat, at low cost and without the need to occupy territory" emphasising cyber attack as a tool for national war.

On one hand, KAMAL A. (2005) trivialized the magnitude of disruption of cyber attack with his definition "computer network related mischief, such as defacing websites or releasing a virus or a worm, without necessarily causing any serious disruption or widespread panic or terror for the general population" although still emphasizing 'network related mischief'. It seems cyber-attack is a deliberate or in-deliberate attempt to redirect, deny access, spearhead phishing, introduce virus and worms, disrupt and destroy an individual/ national computer networks.

Cyber-attack is one of the top five global risk having scored 3.80 in WEF's (2012) report in terms of Likelihood of occurrence. It ranges from denial of service, website defacement, password sniffing, malware, Trojans and virus attacks, identity theft, unauthorized access, cyber bulling…. This takes advantage of the vulnerability of computer controlled network system to attack system (network, computers and operations) which might have been introduced accidentally or as result of loopholes. There are numerous reasons for this act, being that attackers can order the assets to make assault vectors, keeping in mind the end goal is to accomplish their desired goals like fraud, theft against organizations, banks, countries, areas and even individuals. The nature of cyber-attack makes it difficult for a Government to verify if an individual or its enemy has launched the attack, since attackers can also support military operations when at war with counterpart nations (DSCI 2014). Cyber attack makes it easy for nations to engage in war without any physical destruction, and as such, attack from a rivalry nation can trigger cyber/ physical war. ISTS (2001) Concluded that there is a relationship between physical attack, political conflict and cyber attack, given that cyber attack instantaneously accompanies physical attacks.

## 3. CYBER ATTACK MECHANISM

Cyber-attack varies depending on the attacker and methods of attacks are numerous, the major forms of cyber attacks are:

i. Identity Theft: this a fraudulent act perpetuated against individuals, by unauthorized collection of personal important data like pictures, passports, social security number and driving licence, to enable the attacker design a false profile and act as an imposter either on social network, accessing loan/credit or even tendering it to the police in case of criminal act (Kamal 2005).

ii. Denial of Service/ Distributed Denial of Service (DDOS): In this kind of cyber attack, the correspondence to some or all the server gadgets could be stuck by flooding the system with spurious packets (Douligeris and Mitrokotsa 2004). This can be network based, home based or even distributed based attack bringing about the loss of basic data exchange and hence influence long haul and element control abilities, this disrupt usually targets the enemy's communications and supply lines, jamming of telecommunications, financial and banking network.

iii. Virus: like computer codes, boot record infectors, file infectors, and macros that gains access into the network by attaching itself to infected file, distributing itself in the attacked network, in order to corrupt, disrupt and possibly steal secure data (Hansman & Hunt (2005)

Worms: These are destructive mechanism sent to targeted networks in order to disrupt, damage secure data for the attacker. ISTS (2001) analysis suggests that worms like Code red, Ramen, Lion might have been created as response to political conflict. There is a possibility of a worm attaining sleep state in other to affect significant number of host before becoming destructive, but worms like Warhol worms and flash worms become destructive as soon as they penetrate the network, giving administration little or no time to implement control measures (Weaver 2001)

## 4. Case Study: Russia's Cyber operations against Georgia in 2008

The attackers targeted the communication system of Georgia's military, aiming to destabilize, interrupt communication, and disrupt their plans. This cyber attack is similar to the one perpetuated against Estonia, but this specifically targeted the Georgia's military. Their websites (military, President Mikhail Saakashvili , Ministry of Information, Ministry of Foreign Affairs ) was attacked with denial of service (DoS), having authorized the C2 server bots to attack the targeted websites with ICMP, TCP, and HTTP flooding and also shutting down the emergency response service.

In August 2008, Government and private server was under attack, and the Russia's attack on Georgia became cumbersome involving volunteers on the stopGeorgia website, giving instructions, target list and DoSHTTP utility to assist in flooding the targeted websites (The Economist 2008). Although Korns & Kastenberg (2005) claims non-involvement of Russia government on this DoS attack, and Hruska J. (2008) believes the attack was a combined effort from the Russia government and organised crime facilitators, but the Ministry Of Foreign Affairs of Georgia (2008) blames the Russia government for this attack.

Georgia being vulnerable to the attacks (Tikk et al. 2008), resulted to physical shooting war, and seeking "cyber refuge" in United States (Korns & Kastenberg 2005). This has not only changed perception of cyber attack, also an eye-opening opportunity to analyse the overlooked facet of cyber conflict (A.F. L. REV. 2009). With the help of The US, Georgia responded unconventionally, which brought to the limelight the United States' failed approach to combating cyber war. Thus issued a statement to counterattack any cyber attack in the future "never again will we see major warfare without a strong cyber component executed as part of it" (LANGEVIN 2008).

## 5. Protective Mechanism

Protection of cyber space has become a global concern since humans depend on computers for everything ranging from assisted driving, human/object tracking, identification/ authorization, social networking, gaming, forecasting, and notifications/alarms (theft, burglary, fire, temperature etc) (Atzori Et Al 2010). If cyber attack is left uncontrolled it can result to terrorism, organised crime, global governance failure and critical fragile state as shown in Figure 1

.

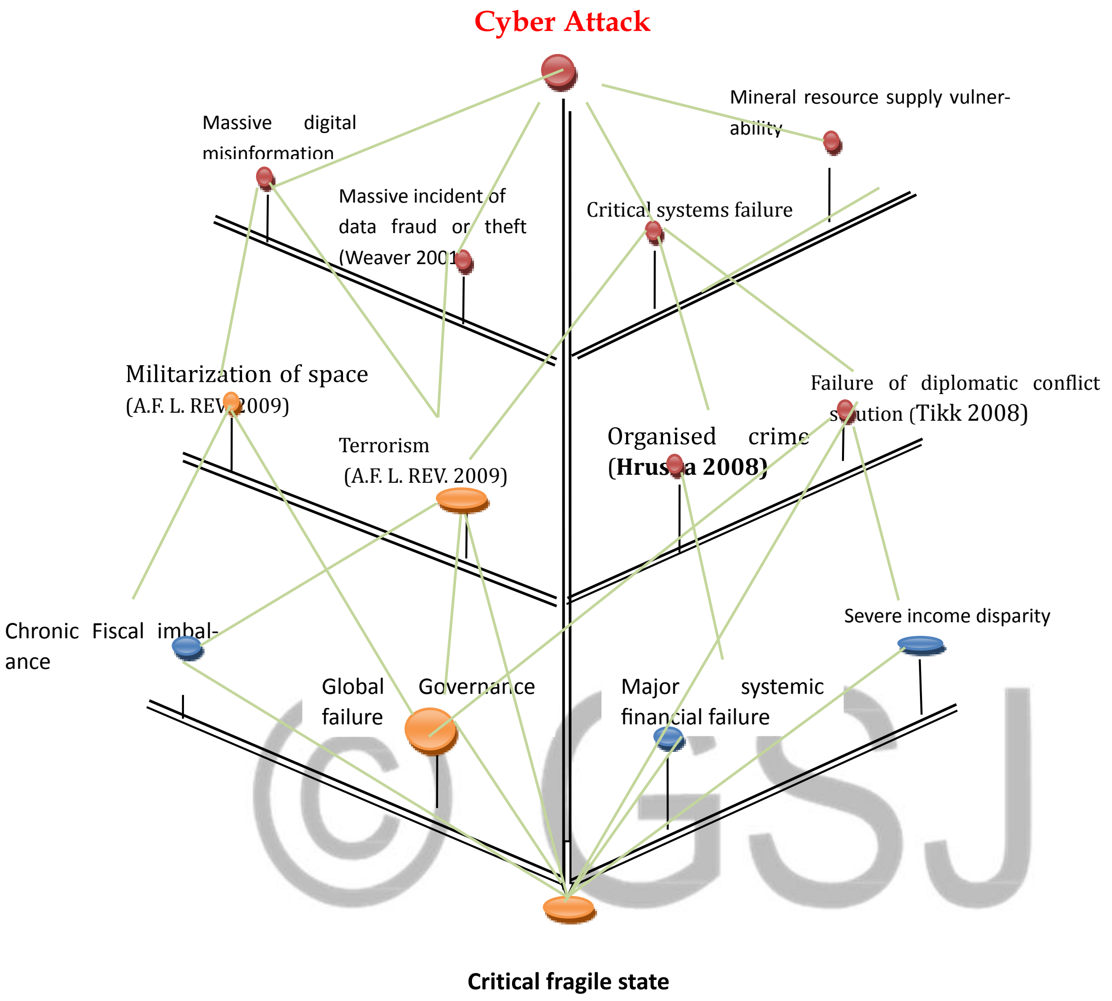

Cyber Attack
Massive digital misinformation
Massive incident of data fraud or theft (Weaver 2001)
Critical systems failure
Mineral resource supply vulnerability
Militarization of space (A.F. L. REV. 2009)
Terrorism (A.F. L. REV. 2009)
Organised crime (Hruska 2008)
Failure of diplomatic conflict solution (Tikk 2008)
Chronic Fiscal imbalance
Global Governance failure
Major systemic financial failure
Severe income disparity
Critical fragile state

**FIGURE 1: INTERCONNECTION OF OTHER RISKS TO CYBER ATTACK**

For individuals, following basic steps like: the use of encryption, passwords, antivirus, authorization codes, double checking URLS before imputing any personal data to avoid redirected websites and use of firewalls (DHS 2013) will beef up personal computer security which will in turn prevent/ minimize cyber attacks. However, there is no global approved definition for cyber security, and there is no objective measure for defending against cyber attacks (ITU 2012), Cyber security is very subjective because it is all about human perception of loopholes and prioritizing information to be safeguarded. This challenge makes it difficult for IT personnel, and probably underestimates risk/damage that can possibly be caused by cyber attacker to their computers/networks (CIO 2014).

Speed and animosity of cyberspace favours cyber attacker (Miller & Kuehl 2010), utilizing “laundering” host to mask their location and identity (Lee 2002) enhances the possibility of going undetected after committing havoc.

For organizational targeted attack where a one-success can result to business loss, the information security team need to define risk tolerability level, develop/ implement a strategic defence mechanism using the hierarchy of risk control: elimination, substitution, engineering controls, administrative controls, and personal protective equipment.

i. Eliminating loopholes: The cyber security appraisal ought to be intensive, incorporating all refined digital assault situations, for example, information respectability assaults, timing electronic interruptions, DoS assaults, and facilitated digital assaults (Sridhar & Govindarasu 2012). The tests should be directed on distinctive vendors, bearing in mind that some software/hardware manufactured might have a defect or bug. System risk assessment, testing and identifying possible loopholes for cyber attacks can be done to eliminate loopholes using the following objective matrix

    a. Identifying Network Security Weakness
        - Weak firewalls rules
        - Network configuration/ design vulnerabilities
        - Continuous audit for vulnerabilities

    b. Identify Software Security Weakness
        - Credential management
        - Improper authorization, authentication, privilege, access and control
        - Bugs
        - Cryptographic issues
        - Code quality
        - Kernel Flaws
        - Continuous audit for vulnerabilities

ii. Substitution: Using the traditional method of risk matrix, which is impact x likelihood of occurrence (ISO 31000 2009), prioritize information to be safeguarded, depending on possible threat and vulnerability identified on prioritized data, in place of every loophole identified, substitute a security measure. For example easily spoofed protocols, User Datagram Protocol (UDP) packets, old *Rate Control Protocol* (RCP) protocols can be substituted with more secure protocol (Wheeler & Larsen 2003)

iii. Engineering controls: The organization should create Computer Security Incident Response Team (CSIRT) a committee that consist of technical professionals, which focuses on computer security incidents, coordinates and accelerate information exchange to the specific security incident (Yamaguchi 2002) Using the following technology approach to prevent, monitor and combat cyber attack:

    a. Querying: Different mechanisms can be utilized to query the network, to enable trace back of any data entering the network, Cooperative Intrusion Traceback and Response Architecture (CITRA) is an effective tool for tracing (Sterne et al. 2001), the observer network can also be reconfigured to detect changes. Pre-positioning of the routers to store logs, performing input debugging, and using combined techniques can help query the server for attacks, and using the force attacker self-identification technique can help unmask any dormant or active attack on network (Wheeler & Larsen 2003)
    b. Encryption: Deploy Virtual Private Network (VPN) to improve communication/ transmission protocols to provide enhanced security especially when communicating with unverified servers/network (Falco & Scarfone, 2008)
    c. Intrusion Detection Systems (IDSs) Firewall: This is a technique used for detection and filtering of computer network, although (Wheeler & Larsen 2003) critic IDS control measure due to its 'false positives and false negative' alerts, firewall is still a recommended security measure.
    d. Authorization, Authentication and access control: Despite the limited change ability and lengthy deployment challenges involved in remote authentication as suggested by Sridhar & Govindarasu (2012), this is still a reliable technique for limiting and controlling access to network servers and assuring data integrity .
    e. Use of external auditor (white hacker): After implementing all possible control measures, the engineering team, should audit their network server with an external auditor, by engaging a consultants known as white hackers to hack their severs in order to determine the solidification of the organizational network.

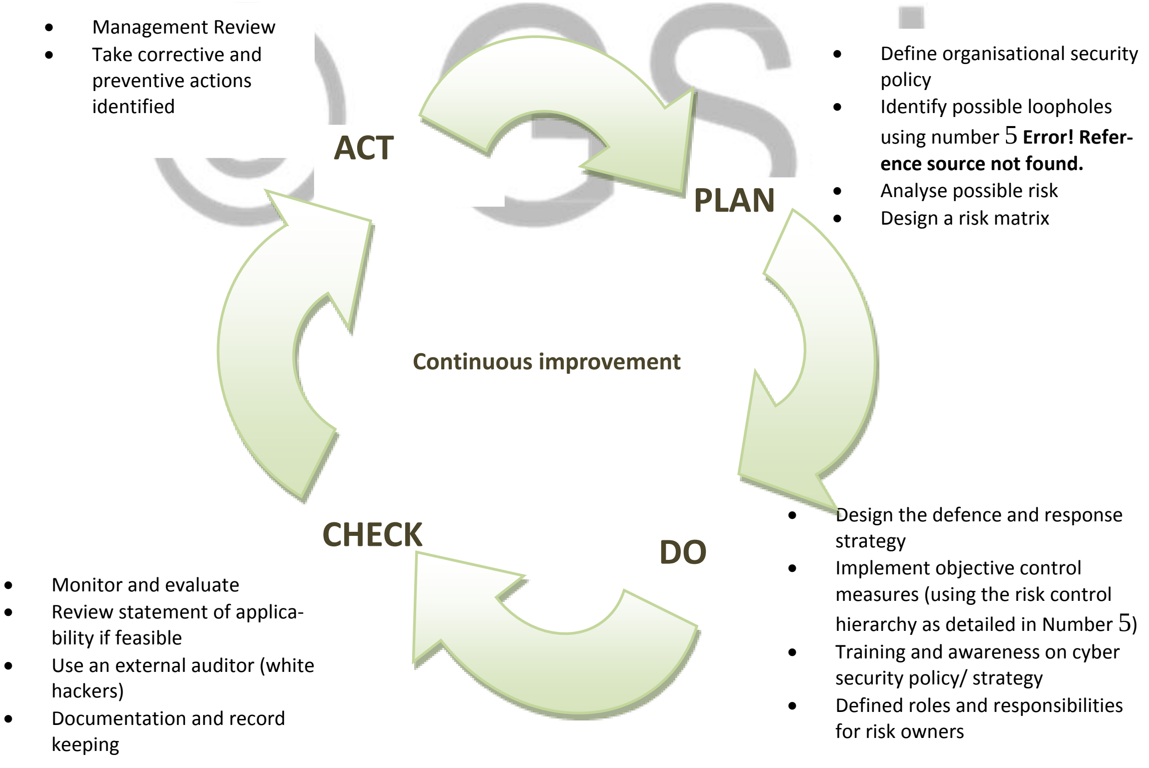
iv. Administrative control: the management team of any organization should define the 'security policy' and set tolerance level for cyber attack, and being that cyber attack is inevitable, management should insure the organization against any attack and implement the developed safety culture /policy

v. Personal protective measures: Training of individuals on internet security should be a regular occurrence in any organization, individuals should be mandated to comply with safety policy such as using strong passwords, protecting login credentials, requesting for authorization, identification and signature verification for any secured data, and as well sign / encrypt secure data being exchanged

## 6. Model for Risk Management

Using the ISO 27001 Internet Security Management System (ISMS) Model of PLAN DO CHECK ACT see Figure 2 for implementation strategy.

**Implementing the ISO 27001 ISMS Model in Cyber Attack Management**



- Management Review
- Take corrective and preventive actions identified

- Define organisational security policy
- Identify possible loopholes using number 5 **Error! Reference source not found.**
- Analyse possible risk
- Design a risk matrix

- Design the defence and response strategy
- Implement objective control measures (using the risk control hierarchy as detailed in Number 5)
- Training and awareness on cyber security policy/ strategy
- Defined roles and responsibilities for risk owners

- Monitor and evaluate
- Review statement of applicability if feasible
- Use an external auditor (white hackers)
- Documentation and record keeping

Figure 2: Model for managing Cyber Attack Risk

**Figure 3 shows risk, stakeholders, and applicable treatment to the identified risks.**

| Risk | Stakeholders | Treatments |
|---|---|---|
| Cyber attack loopholes | IT security response team | a. Identifying Network Security Weakness<br>b. Identify Software Security Weakness **(Sridhar & Govindarasu 2012)**<br>See 5**Error! Reference source not found.** for detailed matrix |
| Attacks | IT security response team | Installing and developing protective mechanism for the organisation as detailed in number 5 |
| Bad design and bugs in operating system | Technology Developer | Software developed should be made to undergo quality check, in other to detect defects before being released. |
| Financial loss | Management | Management should insure the organisation against financial loss **(Yamaguchi 2002)** |
| Negligence | Management | implementation of security policy/mechanism developed |
| Unauthorized access and identity theft | Technology operators | Use of passwords, encryption, safeguard login credentials and validation |
| Porous regulations | Government (Law enforcement) | There should be an international law on cyber attack, defining the<br>illegal and legal international acts<br>to enable an attacked state determine best response strategy **(Ophardt 2010)** |
| | | |

**Figure 3: Risk Management Table**

## Conclusion

This paper has critically analysed the chosen WEF risk, reviewed cyber attack mechanisms, and using a case study elaborated on possibility of cyber attack triggering physical war, and went further to design and implement control strategy for the risk management. Being that cyber attackers are constantly enhancing their technology and methodology of attack, suggests the interested stakeholders in network security to adopt continuous improvement to any control measures in place.

Since cyber attack is an emerging form of warfare which is not negotiable, and research shows that hacker's control of Supervisory Control and Data Acquisition (SCADA) systems, can result to physical injury and death, then collaborative effort form government, organizations and individuals will be required if significant success story will emerge from the battle against cyber attacks

.

## References

[1] Atzori, L., Lera A., & Morabito, G. (2010) 'The Internet of Things: A survey' Computer Networks 54 (2010), 2787–2805

[2] CIO (2014) Targeted Cyber Attack Prevention with IT Security [online] available from <http://www.cio.com/article/2369978/cybercrime/targeted-cyber-attack-prevention-with-it-security.html> [18th August 2014]

[3] Data Security Council of India (2014) Cyber Attacks [online] available from <https://www.dsci.in/taxonomypage/242 > [20th August 2012]

[4] Douligeris, C. and Mitrokotsa A. (2004) "DDoS Attacks and Defence Mechanisms: Classification and State-of-the-art" Computer Networks 44 (2004) 643–66

[5] *Fernandez, E.* (2001) An overview of Internet security. *Proceedings of the World's Internet & Electronic Cities Conference (WIECC 2001),* May 1-3, 2001, Kish Island, Iran.

[6] Hansman, S. & Hunt, R. (2005) "A taxonomy of network and computer attacks". Computer and Security

[7] Hruska J. (2008) Russians May Not be Responsible for Cyberattacks on Georgia, ARS TECHNICA [online] Aug. 13, 2008, available on <http://arstechnica.com> ( 17 August 2014)

[8] http://www.tripwire.com/state-of-security/featured/preventing-cyber-attacks-identifying-top-risks/

[9] Institute for Security Technology Studies (2001) Cyber Attacks During the War on Terrorism: A Predictive Analysis [online] available from <http://www.ists.dartmouth.edu/docs/cyber_a1.pdf> [29th August 2014]

[10] International Organization for Standardization (2012) ISO 27001 IT security Management system standard [online] available from < http://www.iso-27001-it-security-management.com/what-iso27001-certification.htm > [25 August 2014]

[11] **International Telecommunication Union** (2012) WCIT Background Brief 6 [online] available from <https://www.google.com/url?q=http://www.itu.int/en/wcit-12/Documents/WCIT-background-brief6.pdf&sa=U&ei=LGoAVPziFYnlaLXQgvgJ&ved=0CAoQFjAE&client=internal-uds-cse&usg=AFQjCNEVn65ENXVhRwr5X9NndNUwL2X4uw > [25 August 2014]

[12] **International Telecommunication Union** (2014) The World in 2013: ICT Facts and Figures [online] available from <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf> [20th August 2014]

[13] Joynal P The Brave New World of the 5 Day War: Russia-Georgia Cyberwar, Where Cyber and Military Might Combined for War Fighting Advantage [online] available at <www.nationalstrategies.com/pdf/publicSafety_GovSec_5DayWar_Joyal.pdf> [02 August 2014]

[14] Kamal A. (2005) 'The Law of Cyber-Space'. United Nations Institute for Training and Research [online ] 2005), 81. Available from <www.un.int/kamal/thelawofcyberspace/The%20Law%20of%20Cyber-Space.pdf> [20 August 2013]

[15] Korns & Kastenberg (2008) Steven Adair, The Website for the President of Georgia Under Attack – Politically Motivated?, Shadowserver Foundation [online]supra note 1, at 64-65; July 20, 2008, available from <http://www.shadowserver.org/wiki/pmwiki.php/Calendar/ 20080720> (20 August 2014).

[16] LANGEVIN, J. (2008) 'U.S. Urged to Go on Offense in Cyberwar'. Washington Times [online] September 29, 2008. available from <http://www.washingtontimes.com/news/2008/sep/29/us-urged-to-go-on-offense-in-cyberwar> [26 August 2014]

[17] Lee, S., & Clay S. (2002) "Technical, Legal, and Societal Challenges to Automated Attack Traceback." IEEE IT Professional 4(3), 12-18.

[18] Lin, H. (2010) 'Offensive Cyber Operations and the Use of Force' Journal of National Security Law &Policy 4 (63)

[19] Miller, R., & Kuehl, D. (2010) 'Section 4: Protecting Our Cyber Borders Cyberspace and the "First Battle" in 21st Century War'. US Army Combined Arm Centre Newsletter 10-52 [online] July 2010 available from <http://usacac.army.mil/cac2/call/docs/10-52/ch_4.asp> [30 August 2014]

[20] Ministry Of Foreign Affairs of Georgia (2008) Cyber Attacks Disable Georgian Websites [online] available from<http://georgiamfa.blogspot.com/2008_08_01_archive.html> (30 August 2014).

[21] NATO Standardization Agency (2010) 'NATO Glossary of Terms and Definitions (English and French)' Allied Administrative Publication (AAP) [online] 6 (2014: 71) available from <http://nso.nato.int/nso/zPublic/ap/aap6/AAP-6.pdf > [29th August 2014]

[22] Nickolov, E. (2008) Modern Trends In The Cyber Attacks Against The Critical Information Infrastructure[online] available from <https://www.google.com/url?q=http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolov-modern-trends-sofia-oct-08.pdf&sa=U&ei=LGoAVPziFYnlaLXQgvgJ&ved=0CBAQFjAJ&client=internal-uds-cse&usg=AFQjCNHkDl0rlRAftPKhSkkri_Ldp-7k4A> [18 August 2014]

[23] Ophardt, J. (2010) Cyber Warfare and The Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield' Duke Law & Technology [online] Review 3 available from < http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1198&context=dltr > (29 August 2014)

[24] Owens, A., Dam, k. and Lin (2009) Technology, Policy, Law and Ethics Regarding U.S Acquisition and Use of Cyber-Attack Capabilities. Ed. Committee on offensive information warfare, National Research Council: National academic press: Washington

[25] Reich P., Weinstein S., Wild, C. & Cabanlong , A., (2010) Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity in European Journal of Law and Technology 1( 2) 2010

[26] Sridhar, S. & Govindarasu, M. (2012) Cyber–Physical System Security for the Electric Power Grid 'Proceedings of the IEEE' 100 (1), 210-224 held January 2012

[27] Sterne, D., Djahandari K, Balupari R, Cholter W, Babson B, Wilson B, Narasimhan P, Purtell A, Schnackenberg D, Linden S. (2002) "Active Network Based DDoS Defense." Proceddings of the DARPA Active Networks Conference and Exposition (DANCE 02). ISSN 0-7695-1564-9/02. IEEE Computer Society.

[28] Stouffer, K., Falco, J. and Scarfone, K. (2008) NIST SP 800-82: Guide to industrial control systems (ICS) security, National Institute of Standards and Technology, Tech. Rep.,

[29] The Air Force Law Review (2009) 'Sovereignty in Cyberspace: Can It Exist?' Cyber Law Edition 64 (2009) 46-48

[30] The Economist (2008) "Marching off to Cyberwar." [online] 4 December 2008 available from <http://www.economist.com/science/tq/displaystory.cfm?story_id=12673385> [30 August 2014]

[31] Tikk, E. (2008) "Cyber Attacks Against Georgia: Legal Lessons Learned," presentation at the NATO Cooperative Cyber Defence Centre of Excellence. Held August 2008

[32] Us Department of Homeland Security (2013) Protect Myself from Cyber Attacks [online] available from <http://www.dhs.gov/how-do-i/protect-myself-cyber-attacks> [15th August 2014]

[33] Weaver, N. (2001) Warhol Worms: The Potential for Very Fast Internet Plagues, University of California Berkeley

[34] World Bank Group (2014) Internet users (per 100 people) [online] available from <http://data.worldbank.org/indicator/IT.NET.USER.P2> 20th August 2012]

[35] Yamaguchi, S. (2002) Cyber Attack: Urgent Demand for Protecting our Infrastructure [online] available from <httpss://www.itu.int/itudoc/itu-t/workshop/security/present/s2p1.pdf> [20 August 2014]

[36]