Use of Internet and Associated Technologies in "Cyber-Warfare" and Issues Affecting its Investigation

Benson Otafu[1, a], Oluleke Bamodu[2,b], Liwei Tian[1,c], Ulagba Otafu[3,d]

1.Science and Technology Research Center Shenyang University Shenyang, China

2.Faculty of Computing, Engineering and Sciences Staffordshire University

Stoke-on-Trent, United Kingdom

3.Mechanical Department Federal Polytechnic Bauchi, Nigeria

a.besomn@ojooo.com;b.indomitablejnr@engineer.com

c.tianliwei@163.com;d.ulagba_otafu@yahoo.com

Keywords: internet; cyber-warfare; jurisdiction; investigation issues

Abstract. With the development of the internet and associated technologies like the World Wide Web, an information age was ushered in bringing a lot of benefits like ease of communication, speedy access to information, convenient business transactions etc. But these same technologies also brought along high tech criminal activities like internet fraud, cyberstalking etc. They also brought along another dimension in the art of war. This paper presents a brief history of the internet, its resources and how they are been applied in cyber-warfare, what constitute criminal and non-criminal act with the help of a case study. It also went further in comparing cyber-warfare to hacking and looks into jurisdictional issues relating to forensic analysis of associated attacks.

INTRODUCTION

War has traditionally been by military forces through the use of military weapons (small arms, bombs, shells, rockets etc.), with the aim of limiting or weakening opponents' military forces, but in this information age (invention of internet, WWW and other related technologies), warfare is beginning to change. A country like North Korea could threaten to disrupt or disable US infrastructures without the need of a fighter jet or as much as dropping a bomb.

In this report, the use of internet and other technologies for cyber warfare shall be looked into, and also issues surrounding investigation of such uses.

A. *Brief History of Cyber Warefare*

Major use of information warfare was in 1999 when hackers in Serbia attacked NATO systems in retaliation of NATO bombing campaign in Kosovo, although cyber threats can be traced further backwards even before the WWW era. In 1979 the first hacker forum was created using messaging board from crude electronics.

Further cyber warfare were recorded in 1994 with the stealing of millions of dollars from Citibank by Russian Vladimir led group of hackers, 1999 Chinese cyber attacks on and defacing of U.S governmental websites after the accidental bombing of the Chinese embassy in Belgrade, U.S military computer warfare on foreign bank account of Serbian leaders and Yugoslav president.

In 2003, series of assaults code named "Titan Rain" were launch against US government computer systems by hackers traced to China. In 2003 also, a slammer worm took down internet services in parts of South Korea and Japan and as well disrupted phone services in Finland.

More recent examples include 2007 attacks believed to be from Russia which brought down government, banks, newspapers and communication websites in Estonia; the 2008 cyber attacks on Georgian government and commercial websites during military conflict between Georgia and Russia, 2009 shut down of two Kyrgyzstan's internet service providers through attacks and 2010 Stuxnet malware attack on Iran's nuclear facilities.[1][2]

B. *Definition of Cyber Warefare*

There hasn't been any unified definition on cyber warfare despite the fact that many countries are engaged in it. Most countries formulate a definition from their own perspective, while others use the term interchangeably with other terms like information warfare, internet warfare, cyber crime etc. One of such definition is the Russian perspective on information warfare as: "The disorganizing or disruption of the functioning of key enemy military, industrial and administrative facilities and systems, as well as bringing information psychological pressure on adversaries' military or political leadership, troops and population through the primary use of state-of-the-art information technologies" [3]

Despite this non uniformity in definition, a good definition of cyber warfare is put forward by a security expect Richard A. Clarke is: "Actions by a nation- state to penetrate another nation's computer or network for the purpose of causing damage or disruption" another good representation is referring to cyber warfare as a form of information warfare involving politically motivated hacking to conduct sabotage and espionage.

C. *Definition of Related Terms in Cyber Warefare*

When cyber warfare is mentioned, other terms that come to mind include: information warfare, cyber attack, cybercrime, cyberspace, computer crime, hacking, etc. Information warfare and cyber attack are sometimes used interchangeably with cyber warfare, while the definitions of the other terms are presented below.

1) *Cyberspace: C*an be defined as the electronic medium of computer networks, represented as a visual virtual three dimensional domain in which communication takes place.

2) *Computer Crime:* Is any illegal act involving computers, its systems, networks or applications and which requires computing knowledge for its perpetration or investigation.

3) *Hacking:* Is defined as "The process of gaining access to computers or sites where no access was intended" [6].

4) *Cybercrime:* "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"[5].

CLASSIFICATION OF CYBER ACTIVITIES

Based on the use of the components of cyberspace (internet, WWW), cyber activities can be classified into criminal and non-criminal uses. In this section, through the use of case study (see appendices), an attempt shall be made in classifying the uses of the internet in cyber warfare into criminal and non criminal uses.

In classifying the uses, a question of what actually constitute a criminal act should be asked. "Crime is an intentional act or omission in violation of criminal law…"according to [6]; that is to say that there has to be a break of law for an act to be deemed criminal. In this case, the law is the cyber law and the criminal act is cybercrime.

Cybercrime as discussed earlier, despite not having a unified definition, generally include the following contents: systems and proprietary computer break-in, computer trespass and unauthorized access, data manipulation or destruction with criminal intent or purpose of intentionally creating damage and harm [4][5][7].

A. *Roles of Computers in Computer Crimes*

The role of computers in cybercrime is divided into 3 groups (computer as targets, computers as tools and computers as incidental to offense).

1) *Computers as target:* When computers themselves are the target of a computer crime, the computers, operating systems or applications are subjected to interference or damages (hacking) in order to obtain information, data or services illegally, possible data that might be accessed or stolen include, but not limited to credit card numbers, intellectual properties, trade secrets, military documents and secrets. Other reasons for the attacks on computers might be to use the hacked system to break into other systems so as to hide the identity and location of the perpetrator, or to use them as bots to attack other computers or just outright to denial the computers services (denial-of service) for mischievous reasons by sending voluminous amount of data to clog or crash the systems.

2) Computers as tools: Computers can also be used as tools in committing crime. Most crimes under this category are traditional crimes which are improved or advanced through the use of computers. Examples include; illegal drug sales, fraud, illegal gambling, spamming, commercial extortion, child pornography, money laundering, stalking (cyberstalking) etc. In these cases, the benefits such as convenience brought about by the use of computers are been exploited for illegal uses. For example, e-mail can be used to cheaply spam multitude as opposed to postal mail. Sale of pirated or illegally copied software can be sold and payments received quickly and conveniently as opposed to individually copying into each CD/DVD and moving about to sell them.

3) Computer as incidental to offense: In this category, the computers are not required for the crime, but are used in a passive way as a storage medium. This use is deemed as a computer crime, because it makes use of the computer to help in optimizing or increasing efficiency, thereby increasing these crimes (e.g. A terabyte of data, which would have required a large storage room can be stored and accessed efficiently on a hard disk). Uses in this category include; storing stolen passwords, credit card numbers, keeping records of illegal deals, storing proprietary information, data or files.[8]

B. Criminal and Non-Criminal Uses of Internet

1) CASE 1: Kosovo Crisis

TABLE I. USE OF INTERNET IN KOSOVO CRISIS

Use of Internet	
Criminal Uses	***Non-Criminal Uses***
E-mail containing viruses	
DoS attacks on Website	
E-mail containing viruses	E-mail (strike warnings)

The use of the internet by the Yugoslav hackers and Serbian supporters ("Black Hand" and others[10]) during the Kosovo crisis with the main motive of sending email infiltrated with viruses or massive data and launching DoS attacks against NATO and other non-military websites can be noticed to fit into the definition of cybercrime and also falls into the first role of computers (computers as the target) in computer crime making such uses of internet and other computer resources to be classified as "Criminal uses". Though, use of e-mail by same group to warn about pending strikes and to send support message, has no criminal intension and should therefore be classified as "Non-criminal use".

2) CASE 2: NATO Air war against Serbia

TABLE II. USE OF INTERNET IN NATO AIR WAR AGAINST SERBIA

Use of Internet	
Criminal Uses	***Non-Criminal Uses***
	Computer attacks on banks

During NATO air war against Serbia, limited computer attacks were launched against computer and banks holding bank data of Serbian leaders and Yugoslav President by the US military. Such use of computers constitutes criminal acts, based on the definition of cybercrime and the roles of the computer in the activity. But in a war situation and going by the principles of the laws of war that states that "Wars should be limited to achieving the political goals that started the war…" [11], an exception can be given for such limited use by military personnel, whose main motive is not to cause harm or damage, prompting for the classification as non-criminal use.

3) CASE 3: Gulf War

TABLE III. USE OF INTERNET IN GULF WAR

Use of Internet	
Criminal Uses	***Non-Criminal Uses***
Network penetration and attacks	

During the Gulf war, information about movement of Iraqi forces through Radar systems and spy planes played decisive role in the war prompting hackers in the Netherlands to offer to help Iraq penetrate and attack collision information networks, which Iraq rejected. Such proposed use of computers and internet resources can be classified as criminal, although within the context of a war, this use might have been justified, but going by the goal of the use which is to cause damages and by observing the motive of the hacker which is for financial gain, the war laws justification should apply in this case.

EASE OF USE INTERNET RESOURCES AND E-EVIDENCE

Having considered cases of the use internet in warfare and classified them into criminal and non criminal categories, this section looks into other internet based resources used in cyber-warfare and the location for associated e-evidences. To aid understanding of these resources, a brief history of internet and WWW is presented.

A. History of Internet

A common misconception is that of the internet and World Wide Web (WWW), against much believes, the internet is not same with WWW. The name internet can be rewritten as inter-net (inter network), meaning a network connecting other networks. The internet contains large range of information resources, aids electronic mail (e-mail), file transfer, chat rooms etc. It also supports the WWW.

The internet originated in 1969 as ARPANET, commissioned by the US government to help in communication and collaboration among researchers and academic sites. In 1982, the internet protocol was standardized. In the 1990s the internet was commercialized making it available to a large user base. With the development of WWW, use of internet further expanded and currently estimated to have more than 2.1 billion users as of 2011. [4][12]

B. History of World Wide Web

Projects leading to the development of the WWW were done in 1980, but the WWW itself began at CERN as a way of exchanging technical papers among physicists in 1991. With help from Belgian computer scientist, Robert Cailliau, British engineer and computer scientist Sir Tim Berbers-Lee was able to publish a formal proposal for building WWW as hypertext documents viewable with browsers. WWW could be considered as an internet application, but not same as internet itself.[12]

C. Examples of Internet Resources

Having seen what internet is and examples of its uses earlier. Internet resources or internet based resources that have been used in cyber warfare include: e-mail, websites, instant message services, chat room/internet relay chat (IRC), file sharing network, message boards, newsgroups, ISP etc.

Of these resources, the common ones used in cyber warfare are email, IRC and message boards/news groups, which are used in launching DoS, email bombs and viruses.

1) Email: Allows the composing of messages and sending from one mail server (sender) to another (receiving). Copies of e-mails, depending on configuration can be found on the sender's server and possibly on the receiver's computer. When e-mails travel from the sender t the receiver, the route or message transfer path is recorded in the header of the e-mail. This can help in tracing the originating IP of the sender. Other places that might contain e-evidence of email crimes are the application logs which might show evidence of mail creation or evidence of spoofing (falsifying mail header), if such was done.

2) Message Boards: Can be used to post messages about a cyber target or give detailed direction about activities or cyber crimes to be committed. Evidence about message boards containing IP addresses, email addresses and header files could be obtained from ISP logs.

3) Chat Rooms: Allows for communication among a group of people in real time. E-evidence of chat room activities and communication could be found in chat session logs.

4) Internet Relay Chat (IRC): This is a type of gathering place like a chat room, made up of networked servers connected by clients through the ISP, allowing information to be shared in real time. The IRC is also known to aid in the launching of DDoS (Distributed Dos) attacks. Through the use of IRC, malicious codes can be sent to other servers which make them remotely controllable by hackers making them part of bot army awaiting command to launch DoS attacks. E-evidence of this type of attacks can be found in log files on the client computer and Fserv of hosts or ISP and network activity logs.

5) DoS: Which is the disruption of target system's ability to function (provide access or service) normally by clogging it with excessive demand. Locally connected devices, network service providers, back up service providers and logs are locations where e-evidences like IP address, trojan and virus activities, ports opened and closed, files ad tools copied etc could be found.

6) Website: A collection of web pages stored on a server, usually written in HTML (Hyper Text Markup Language), web pages are available to clients on the internet through web servers. It is possible through the use of scripting languages and cookies (trackers) for same web page to produce different content to different users. To find e-evidence from websites, the website HTML source codes are probably a good place to start investigation. Web archiving tools could also be used to access past web content which might be changing frequently. The web server also contains files which might be useful as evidences (IP logs of access to and download from the website), since that is where the web pages are stored. [8]

CYBER-WAR VS HACKING

In order to draw a difference between the activities of cyber-war and that of an hacker, it is necessary to understand how hacking works and how hackers are classified.

A. *How Hacking Works*

Attracted by the amount of sensitive information (financial, trade secrets, etc) transmitted online through the internet. Criminals are drawn to the internet to use it as a tool in committing crime. Breaking into a system used to require sophisticated knowledge of computer systems and the internet, but that is changing now as hacking tools and training materials are cheaply available and in some cases freely.

Computers, in fact, all systems are built with flaws (some probably haven't just been found yet) which might have been as a result of trade-offs decisions made in the design or development. With this known fact, hackers try to find these flaws and exploit them to gain some advantage. Most hacking weapons used are viruses, email bombs, Trojans, computer worms, key loggers etc and these can easily be transmitted in cyberspace. [12]

B. *Classification of Hackers*

Hackers can be classified according to their motives as White hat, Black hat, Grey hat, Hacktivist and so on.

1) White hat hackers: Are referred to as ethical hackers; their breaking into system is mostly with permission and is usually for the purpose of testing the system for vulnerability.

2) Black hat hacker: Or crackers as some call it are hackers who break into computer systems for malicious or criminal goals. The activities of the class of hackers include destroying networks and data or stealing them. The process involved in this class of hacking are pre-hacking; where vulnerability is sort, then the launch of attack on the target exploiting the found vulnerability.

3) Gray hat hackers: Are a combination of both white and black hat hackers. Their activities involve breaking into a system, then later offering to repair for fees.

4) Hacktivists: Are hackers who crash systems with the main motive of passing across a message (political, ideological or religious). Their famous activities include launching DoS attacks and defacing websites.

C. *Investigation*

As mentioned earlier, the classes and activities of the hackers need to be known to effectively differentiate and investigate financially motivated hacking and cyber-warfare. For financially

motivated hacking, the focus classes are those of the black hat and grey hat, while cyber war activities will mostly involve the hacktivists.

Knowing these classes, their attitude, motivation and activities could suggest locations where evidence should be looked for.

Cyber-war hackers or hacktivist usually don't do much in hiding their tracks, and in most cases will usually leave messages showing involvement. Where e-evidence of associated activities can be found have be touched in an earlier section, although apprehending the perpetrators of these crimes or having access to the devices used for the crime can proof to be a difficult task due to the fact that countries harboring suspects or the suspects' computer systems are not usually will to cooperate in situation like this.

For the financially motivated hackers, the usually don't intentionally leave traces or evidences behind. Although, unlike the cyber war hacktivist, access permission or warrant to the suspects or their computer systems could be filled at the court and cooperation could be sort from other cross organization, when a trans-border crime of this category is being investigated. Other places where e-evidences useful for investigation could be found in addition to those discussed earlier are: ISP logs, firewalls, DHCP (Dynamic Host Configuration Protocol) logs, NAT/PAT logs, proxy logs, machine image, host network, database servers, antivirus/malware logs of victims' computer, RAM, ROM and hard disk of suspects' computer, browser cache, roots, internet history, temporary file logs, event viewer/security event logs, workstation logs etc.

Some tools that can be used for the forensic investigation include FTK (Forensic ToolKit) and EnCase.

JURISDICTIONAL ISSUES OF INVESTIGATING CYBER-WARFARE

One major limitation in the investigation of cyber crimes is that of jurisdiction. "Jurisdiction is the authority of a court to hear a case and resolve a dispute"[4]. But going by the fact that the internet is without boundaries and cybercrimes can involve inter-border perpetrators and victims, the question that immediately comes up is who has the jurisdictional power to solve the case or what laws should be applied. For example, distribution of porn materials is through the internet is considered a crime in China while it is acceptable in some other countries. If porn materials are distributed from a country where such actions are allowed to clients in China, who holds the jurisdictional power over such distributer? What about a more complex scenario like, a hacker in country A, hacks into computers in country B and directs them to attack another computer in country C, thereby destroying both computers in country B and C, which law should be used in such case (law of country A where the offender resides, or laws of country B or C where the offense was directed).

International laws addressing these situations aren't also uniform, in some countries, laws like that of the privacy act may restrict investigation into or access that can be granted to suspects' personal communication or files, where major evidences which might have helped investigation might be found.

Issues like these are of major concern in forensic investigations.

CONCLUSION

This report has looked into a new form of warfare and activities associated with it. It has also looked at how associated crimes can be investigated as well as limitations for carrying out these investigations. A brief history of internet and WWW has also been looked into with how they have been used in the carry of cyber warfare and cyber crimes. A point that was highlighted in the report is that of the difference between cyber warfare and hacking and where evidences associated with the activities of each can be found.

APPENDICES

Case Study

The Kosovo crisis was the first known major use of information warfare. In 1999, during the Kosovo crisis and NATO bombing campaign, Yugoslav hackers reportedly launched a DoS attack against a NATO Web site with viruses and thousands of e-mails daily. Serbian supporters clogged

non-military Internet sites in the United States. In the cyber-warfare, Serbian supporters also used e-mail to warn of NATO strikes and to send messages of support.

The US military has acknowledged that NATO's air war against Serbia included "limited" computer warfare. The Unites States used computer attacks on Yugoslav President Milosevic's and other Serbian leaders' foreign bank accounts.

During the 1990-1991 Gulf War, hackers in the Netherlands reportedly offered to help Iraq by penetrating and attacking coalition information networks, but Iraq rejected the offer.

REFERENCES

[1] Harry D. Raduege, Succeeding in a cyber world, 14th Annual New York State, Cyber Security Conference. Deloitte Center of Cyber Innovation, 2011

[2] Amber Corrin,"Some key events in the history of cyber warfare", 2009 Available at http://fcw.com/articles/2009/10/19/feat-dod-cyber-timeline.aspx

[3] Jeffrey Carr, Inside Cyber Warfare 2nd edition, O'Reilly Media, Inc, Sebastopol, CA, 2011

[4] Gerald R. Ferrera et al, Cyber law: Text and Cases. Thomson Learning Cincinnati,OH, 2001

[5] Halder, D. & Jaishankar, K, Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, 2011

[6] Frank E.Hagen, Introduction to Criminology: Theories, Methods and Criminal Behavior. Nelson-Hall Publishers, Chicago, 1998

[7] Fred Adler et al, Criminology, 4th edition. McGrawHill, New York, 2001

[8] Alberto R. Gonzales et al, Investigations Involving the Internet and Computer Networks, US Department of Justice, Washington, DC, 2007

[9] Clint P. Garrison, Digital Forensic for Network, Internet and Cloud Computing: A Forensic Evidence Gude for Moving Targets and Data, Elsevier Inc., Burlington, MA, 2010

[10] Kenneth Geers, Cyberspace and the changing Nature of Warfare, Tallinn, Estonia

[11] Wikipedia, Available at http://en.wikipedia.org/wiki/Laws_of_war

[12] Bamodu, Oluleke, Benson Otafu, & Liwei Tian., Secure Web Based System Development, Advances in Intelligent Systems Research, 2013