CYBER-ATTACKS: THE LEGAL RESPONSE

Junaidu Bello Marshall, Esq.*  Mua’zu Abdullahi Saulawa, Esq.**

ABSTRACT

The paper focuses on cyber-attacks, its working definition, types and further examines some of the attacks in other jurisdictions. The paper aim at examining the cybercrime convention as the legal instruments to cybercrime and other computer related crimes. Today, the world of Information and Communication Technology (ICTs) today is facing great challenges in cybercrime related issues. Cyber-attacks become a continued act perpetrated by individuals, private companies, organizations and governments in different spheres of practices. The challenges posed to the ICTs become paramount as there is need to address the legal and regulatory issues for policy makers. The paper adopted doctrinal research method approach wherein the relevant data collected was analyzed and the findings brought out. The findings of the paper reveals that there is lack of cooperative measures within countries in addressing the menace of cyber-attacks and further recommends that the international community’s needs to strive hard in policy strategy so as to create measures in countering the endemic practices of cybercrimes.

Keywords

Cyber-attack, Cybercrime Convention, Legal Response

1. INTRODUCTION

The paper focuses on Cyber-attack, its meaning, types and legal framework and the issues surrounding it as concept, in different regions and jurisdictions. For the past few years, the global cybercrime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer ‘aptitude’ showcasing their talent to the world.

* Lecturer, Faculty of Law, Usmanu Danfodiyo University, P.M.B 2346, Sokoto- Nigeria, (Ph. D fellow), Email: jbmarshall82@gmail.com.

** Lecturer, Faculty of Law, Umaru Musa Yar’adua University, P.M.B. 2218, Katsina-Nigeria, (Ph. D fellow), Email: muazu.abdullahis@gmail.com.
These attacks, which were rarely malicious, have gradually evolved into cyber crime whereby syndicates use this opportunity by siphoning off money through illegal cyber channels. By 2010, political motivation in the cybercrime had infiltrated global cyberspace.\(^1\) In fact, weaponry and command and control systems have also transitioned into the cyberspace to deploy and execute espionage and sabotage, as seen in the example of digital espionage attacks on computer networks at Lockheed Martin and NASA.\(^2\) This has been transformed in which the use of cyberspace in controlling devices or chips in the weapons.

With the current advancements in modern technology have helped countries develop and expand their communication networks, enabling faster and easier networking and information exchange. Currently, there are nearly 2 billion internet users and over 5 billion mobile phone connections worldwide. Every day, 294 billion emails and 5 billion phone messages are exchanged. The majority of the people today around the world now depend on consistent access and accuracy of these communication channels.\(^3\) The growing popularity and convenience of digital networks, however, come at a cost. As businesses and societies in general increasingly rely on computers and internet-based networking, cybercrime and digital attack incidents have increased around the world.\(^4\) These attacks — generally classified as any crime that involves the use of a computer network — include financial scams, computer hacking, downloading pornographic images from the internet, virus attacks, e-mail stalking and creating websites that promote racial hatred.\(^5\) The first major instance of cyber crime was reported in 2000, when a mass-mailed computer virus affected nearly 45 million computer users worldwide.\(^6\)

2. CYBER ATTACKS

---

\(^1\)National insecurity, InformationAge, 26 January 2011.  
\(^2\)Stuxnet was about what happened next, FT.com, 16 February 2011.  
\(^3\)The cost of cybercrime, Detica, February 2011.  
\(^4\)It is time for countries to start talking about arms control on the internet, Economist, 1 July 2010.  
\(^5\)The worldwide crime web, BBC News.  
A cyber-attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.\(^7\)

Cyber-attack is any form of assault or retreat operation engage by individuals or organizations that focus on computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malevolent acts usually originating from an unidentified source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labeled either as a Cyber campaign, cyber warfare or cyber terrorism in different context. Cyber-attacks operate at a different range; sometimes can install a spyware on a Personal Computer so as to try to destroy the infrastructure of entire nations. Cyber-attacks have become increasingly sophisticated and dangerous as the Stuxnet worm recently demonstrated.\(^8\)

2.1 What is a Cyber-Attack?

The first challenge in evaluating how domestic and international law might be used to address cyber-attacks is to determine the nature and scope of the problem we face. Activities in cyberspace defy many of the traditional categories and principles that govern armed conflict under the law of war. This first offers a precise definition of “cyber-attack.” This step is not only necessary to the legal analysis that follows, but it also fills a gap in the existing literature, which often uses the term without clarifying what it is meant to include and exclude. We then offer three categories of activities that fall within this definition, illuminating the extraordinary range of activities that fall under even a carefully constructed and limited definition of “cyber-attacks.” This serves as a prelude to an analysis of what portion of cyber-attacks are governed by the law of war and other existing bodies of law.\(^9\)

A cyber attack is defined to mean ‘deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can

compromise data and lead to cybercrimes, such as information and identity theft. In addition cyber attack is also known as a Computer Network Attack (CNA)’. Further to this, the Cyber attacks may include the following outcome:  

- Identity theft, fraud, extortion
- Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses
- Stolen hardware, such as laptops or mobile devices
- Denial-of-service and distributed denial-of-service attacks
- Breach of access
- Password sniffing
- System infiltration
- Website defacement
- Private and public Web browser exploits
- Instant messaging abuse
- Intellectual property (IP) theft or unauthorized access

The recommended definition adopted in this paper is a narrow definition of cyber-attack, one meant to focus attention on the unique threat posed by cyber-technologies: that a cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose.  

This definition is composed of four salient important aspects which consist of:

a. ‘a cyber-attack…’
b. ‘…consist of any action taken…’
c. ‘…to undermine the function…’
d. ‘…of a computer network…’

Some of the potential cyber-attacks are speculated to have resulted out of factors, firstly, there is a fear factor, and this is the most common, where a cyberterrorist will create fear amongst individuals, groups, or societies.

3. COUNTRIES CONCEPTIONS OF CYBER-ATTACK

11 Ibid.
12 Oona A. Hathaway, supra note 9, page 10.
Some of the government perceived cyber-attacks in a different perspective. What the U.S. government perceived to be cyber-attacks is quite different with the perception of Russia- and China-led Shanghai Cooperation Organization, although to understand the scope of cyber-attack an active measure must be examine in defining it. Perhaps not surprisingly, they have arrived at very different understandings of the problem. Yet, no official definition offer by the United State military in definition of cyber-attack or cyber-warfare. Instead, the Joint Chiefs of Staff have defined forms of warfare closely related to cyber-warfare. For example, the Joint Chiefs explain that “information warfare” includes operations “to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting one’s own.”

They define a sub-class of information warfare, computer network warfare, as:

The employment of Computer Network Operations (CNO) with the intent of denying adversaries the effective use of their computers, information systems, and networks, while ensuring the effective use of our own computers, information systems, and networks. These operations include Computer Network Attack (CNA), Computer Network Exploration (CNE), and Computer Network Defense (CND).

---

14 Ibid, 8.
15 The Congressional Research Service does provide an official definition but it is not particularly specific: Cyber-warfare is “warfare waged in cyberspace. It can include defending information and computer networks, deterring information attacks, as well as denying an adversary’s ability to do the same. It can include offensive information operations mounted against an adversary, or even dominating information on the battlefield.” Steven A. Hildreth, ‘Cyber warfare’, CONGRESSIONAL RESEARCH SERVICE, 16 (19 June, 2001). The Department of Defense’s Strategy for Operating in Cyberspace utilizes the term “cyber threats” rather than cyber-attacks to describe the threats to cyberspace. See U.S. DEPT OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 2 (July 2011) [hereinafter DOD STRATEGY].
16 JOIN T CHIEFS OF STAFF, U.S. DEPT OF DEF., JOINT PUB.3-13, INFORMATION OPERATIONS, at ix (Feb. 13, 2006), [hereinafter JP 3-13] (listing five IO methods: (1) electronic warfare; (2) computer network operations, including computer network attacks; (3) psychological operations; (4) military deception; and (5) operational security).
The U.S. National Research Council defines cyber-attack as “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.”\(^\text{18}\)

The objectivity of this definition taken by the United States is preferable; but the difficulty of these definitions partially explains the lack of uniformity within the government. Moreover, the definition fails to distinguish between a simple cyber-crime and a cyber-attack. A simpler, uniform definition would avoid ambiguity, overlap, and coverage gaps; facilitate a cleaner delineation between cyber-attack and cyber-crime; and promote greater inter-agency cooperation.\(^\text{19}\)

The Shanghai Cooperation Organization—a security cooperation group composed of China, Russia, and most of the former Soviet Central Asian republics, as well as observers including Iran, India, and Pakistan—has adopted a much more expansive means-based approach to cyber-attacks. The Organization has “expressed concern about the threats posed by possible use of (new information and communication) technologies and means for the purposes (sic) incompatible with ensuring international security and stability in both civil and military spheres.”\(^\text{20}\)

It defines an “information war” as “mass psychological brainwashing to destabilize society and state, as well as to force the state to take decisions in the interest of an opposing party.”\(^\text{21}\)

Moreover, it identifies the dissemination of information harmful to “social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other states” as one of the main threats to information security.\(^\text{22}\)

\(^{18}\)COMM. ON OFFENSIVE INFORMATION WARFARE, NAT’L RES. COUNCIL, TECHNOLOGY, POLICY LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (WILLIAM A. OWENS, ET AL. EDs., 2009) [hereinafter NRC REPORT].

\(^{19}\)Oona A. Hathaway, supra note 12, p. 9.

\(^{20}\)Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st plenary meeting (Dec. 2, 2008) [hereinafter Shanghai Cooperation Agreement]. The distinction between this interpretation and that of the United States is understandable in light of Matthew Waxman’s analysis of strategic differences in the cyber-attack context. As Waxman notes, “major state actors in this area are likely to have different views on legal line drawing because they perceive a different set of strategic risks and opportunities.” Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 YALE J. INT’L L. 421, 458-59 (2011).

\(^{21}\)Shanghai Cooperation Agreement, Annex I, at 209.

\(^{22}\)Ibid. at p. 203.
4. **TYPES OF CYBER ATTACK**

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Details</th>
</tr>
</thead>
</table>
| Viruses and worms       | Viruses and worms are computer programs that affect the storage devices of a computer or network, which then replicate information without the knowledge of the user.  
                          |                                                                                                                                          |
| Spam emails             | Spam emails are unsolicited emails or junk newsgroup postings. Spam emails are sent without the consent of the receiver — potentially creating a wide range of problems if they are not filtered appropriately. |
| Trojan                  | A Trojan is a program that appears legitimate. However, once run, it moves on to locate password information or makes the system more vulnerable to future entry. Or a Trojan may simply destroy programs or data on the hard disk. |
| Denial-of-service (DoS) | DoS occurs when criminals attempt to bring down or cripple individual websites, computers or networks, often by flooding them with messages. |
| Malware                 | Malware is software that takes control of any individual’s computer to spread a bug to other people’s devices or social networking profiles. Such software can also be used to create a ‘botnet’— a network of computers controlled |

---

23Cyber-attacks: from Facebook to nuclear weapons, The Telegraph, 4 February 2011.
24A Good Decade for Cybercrime, McAfee, 2010.
26Accessed from PCMeg.com on 10 March 2011.
remotely by hackers, known as ‘herders,’ — to spread spam or viruses.  

Scare ware Using fear tactics, some cyber criminals compel users to download certain software. While such software is usually presented as antivirus software, after some time these programs start attacking the user’s system. The user then has to pay the criminals to remove such viruses.

Phishing Phishing attacks are designed to steal a person’s login and password. For instance, the phisher can access the victims’ bank accounts or assume control of their social network.

Fiscal fraud By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits.

State cyber-attacks Experts believe that some government agencies may also be using cyber-attacks as a new means of warfare. One such attack occurred in 2010, when a computer virus called Stuxnet was used to carry out an invisible attack on Iran’s secret nuclear program. The virus was aimed at disabling Iran’s uranium enrichment centrifuges.

Carders Stealing bank or credit card details are another major cyber crime. Duplicate cards are then used to withdraw cash at ATMs or in shops.

5. EXAMPLES OF CYBER-ATTACKS IN SOME JURISDICTIONS

28Ibid.  
29The cost of cybercrime, Detica, February 2011.  
30KPMG, supra note 27, p. 2.  
31The cost of cybercrime, supra note 29.  
32Cyber-attacks: from Facebook to nuclear weapons, The Telegraph, 4 February 2011.  
33KPMG, supra note 30.
Recently, there are cyber-attacks in some of the countries across the globe and most of the attack affects the country as a matter of national security.

In Russia, the Russian presidency’s website was attacked on several times on Friday by Moscow hackers and that brought down the Central Bank website.\(^{34}\) That a powerful cyber-attack is under way on the (Kremlin) site and it appeared to continuous and there is no clue as to the attackers.\(^{35}\) In addition to this a report that Ukraine's prime minister blamed Russian intelligence on Thursday for a hacker attack against German government websites, for which a pro-Russian group claimed responsibility.\(^{36}\)

Also in Brussels/London that a group of Hackers brought down several public North Atlantic Treaty Organizations (NATO) websites, the alliance said on Sunday, in what appeared to be the latest escalation in cyberspace over growing tensions over Crimea. "It doesn't impede our ability to command and control our forces. At no time was there any risk to our classified networks," another NATO official said.\(^{37}\) The so-called "distributed denial of service" (DDoS) attack, in which hackers bombard websites with requests causing them to slow down or crash, also hit the site of a NATO-affiliated cyber security centre in Estonia.\(^{38}\)

A group calling itself "cyber berkut" said the attack had been carried out by patriotic Ukrainians angry over what they saw as NATO interference in their country.\(^{39}\)

In India, the city of New Delhi of India received a second-most cyber-attack on mobile devices prone country with a major chunk of these intrusions designed for


\(^{35}\) Ibid.


\(^{37}\) Ibid.

\(^{38}\) Ibid.

\(^{39}\) Ibid. The claim, made at www.cyber-berkut.org, could not be independently verified. "Berkut" is a reference to the feared and since disbanded riot squads used by the government of ousted pro-Russian Ukrainian President Viktor Yanukovich and Cyber warfare expert Jeffrey Carr, in a blog on the attacks, described cyber berkut as staunch supporters of Yanukovich and a "pro-Russia hacktivist group working against Ukrainian independence
phishing and stealing banking details, a report by security software maker Kaspersky said.\(^{40}\)

Also in China, the cities of Shanghai/Beijing, faced a cause of an Internet outage in China that rerouted millions of users to a U.S. website of a company which helps people get around Beijing's censorship remained a mystery on Wednesday, but experts weighed the possibility of a cyber-attack.\(^{41}\) Users were redirected to a site run by a company tied to the Falun Gong, a spiritual group banned in China which has been blamed for past hacking attacks.\(^{42}\)

The state-run China Internet Network Information Center (CNNIC) said in a micro blog post that the outage, which lasted for several hours, was due to a malfunction in China's top-level domain name root servers on Tuesday afternoon. Chinese Internet users were rerouted to a U.S.-based website run by Dynamic Internet Technology (DIT), a company that sells anti-censorship web services tailored for Chinese.\(^{43}\) A mistake made by the Chinese government could be at fault for the outage. "Instead of targeting a small list of websites the (Chinese Internet censorship systems) malfunctioned and targeted any domain.\(^{44}\) The malfunction is a result of a Domain Name Service (DNS) hijacking, said Bill Xia, founder of DIT, where even if people tried to go to a non-existing website they would be redirected to DIT’s.\(^{45}\)

At Israel, the city of Jerusalem: Hackers attacked Israeli computers including one used by the defence ministry department dealing with civilians in the occupied West

---


\(^{42}\)Ibid.

\(^{43}\)Ibid. “The Internet disruption appears to have taken place through changes to the Domain Name Service - the mapping between domain names and the IP addresses for the corresponding content servers - rather than through attacks on the underlying infrastructure,” said Jim Cowie, CTO of Renesys, which monitors global Internet activity.

\(^{44}\)Ibid.

\(^{45}\)It’s even clearer this is not an attack of all the Domain Name Servers in the world, but the same as the DNS hijacking technologies used by the Chinese government to block websites they don’t want. Said Bill Xia, founder of DIT, Ibid.
Bank, an Israeli data protection expert said on Monday. "At the beginning of this month a number of mails were sent to a number of companies in Israel, including security organizations," "There was an attachment... and whoever opened it was infected with a virus, a Trojan Horse, which allowed the attackers to control those computers. One of the computers belonged to the Civil Administration. And he further said that the virus allowed the attacker "complete control of the infected computers, the attackers could carry out any operation within that network."

The most recent cyber-attack is the Sony cyber-attack on November 24, 2014, personally identifiable information about Sony Pictures Entertainment (SPE) employees and their dependents, e-mails between employees, information about executive salaries at the company, copies of unreleased Sony films, and other information, was obtained and released by a hacker group going under the moniker "Guardians of Peace" or "GOP". The identities of the hackers are currently unknown. Currently, the available information is that whether or not individuals at SPE assisted in the system compromise. But that still is yet to be verified.

Still the motives for the hack have yet to be revealed, the hack has been tied to the planned release of the film The Interview, which depicts an assassination attempt on North Korean leader Kim Jong-un, with the hackers threatening acts of terrorism if the film were to be released. Further to this development investigators in the U.S. looking into the Sony Pictures hacking believe that North Korea hired hackers to

---

47 Aviv Raff, chief technology officer at Israeli cyber security firm Seculert told army radio.
48 Aviv further said in reference to the defence ministry department, which is staffed by the military.
49 'Israeli defence computer hit in cyber-attack: Data expert’, op. cit note.
52 Ibid.
wage the cyber attack.\(^53\) According to a Reuters report, it is believed that the hackers were hired from outside North Korea to aid in the cyber attack on Sony Pictures on November 24\(^{th}\) 2014. The cyber attack was likely "contracted out" as North Korea itself "lacks" the ability to carry out some of the elements required in the attack.\(^54\) The officials investigate whether North Korea recruited contractors from outside to hack Sony. Still, the FBI stands firm on its stance that the country was the orchestrator of the Sony Pictures attack.\(^55\)

In the early January of 2015, the United State Twitter and YouTube accounts were hacked on Monday 12\(^{th}\) by people claiming to be sympathetic toward the Islamic State militant group being targeted in American bombing raids, this account centrally oversees the United State military command operations in the Middle East.\(^56\)

United State officials acknowledged that the incident in which the accounts were "compromised" for about 30 minutes was embarrassing but played down the impact. The FBI said it was investigating. Also the Pentagon spokesman Army Colonel Steve Warren said the Defense Department "views this as little more than a prank, or as vandalism." \(^57\)

The hacked accounts display a post that "In the name of Allah, the Most Gracious, the Most Merciful, the CyberCaliphate continues its CyberJihad," Further to this the Twitter account published a list of generals and addresses associated with them, titled "Army General Officer Public Roster (by rank) 2 January 2014." \(^58\)


\(^{54}\) Ibid.

\(^{55}\) Ibid.

\(^{56}\) 'Apparent Islamic State backers hack U.S. military Twitter feed', Reuters Report, available at (http://www.reuters.com/article/2015/01/12/us-cybersecurity-centcom-hack-idUSKBNA0KL1UZ20150112/). (accessed on 12 January 2015). Further to this the hackers posted on the U.S. Central Command Twitter feed, using an acronym for the hardline Islamist group, which has taken control of parts of Syria and Iraq—'American soldiers, we are coming, watch your back, ISIS'.

\(^{57}\) Ibid. Warren in his press briefing further said 'It's inconvenient, it's an annoyance but in no way is any sensitive or classified information compromised'. The Central Command Twitter feed said after being hacked. The Defense officials said in a statement that "operational military networks were not compromised and there was no operational impact." That the Islamic State forces have been targeted in air strikes by the United States and international partners.

\(^{58}\) Ibid, the post in the account subsequently read, "Pentagon Networks Hacked! China Scenarios" and "Pentagon Networks Hacked. Korean Scenarios." Central Command said it was notifying Pentagon and
In a press briefing from the White House spokesman Josh Earnest said that the hacking was "something that we take seriously." But Earnest added, "There's a pretty significant difference between what is a large data breach and the hacking of a Twitter account." Even as the hacking was taking place, President Barack Obama on Monday announced new proposals aimed at bolstering American cybersecurity after high-profile hacking incidents including one against Sony Pictures Entertainment that U.S. officials blamed on North Korea.  

In a review of some of the documents by Reuters released by the hackers but could not immediately identify any that appeared to contain information that compromised national security. Some of the documents were easily found using Google searches. After the hacking, the heading of the Central Command Twitter account showed a figure in a black-and-white head scarf and the words "CyberCaliphate" and "I love you ISIS."  

6. THE LEGAL RESPONSE

The legal response in this paper is a discussion on the introductory part of the Council of Europe Cybercrime Convention. Which highlight the most important aspect of the Convention in relation to cyberspace and other related computer crimes.

The forty-one Nation Council of Europe (“COE”) drafted the Cybercrime Convention after four years and twenty-seven drafts. It was adopted by the Committee of law enforcement authorities about the potential release of "personally identifiable information" and work to make sure the people "potentially affected" are notified quickly.

60 Ibid.

61 Ibid. "Hacking a Twitter is about the equivalent of spray-painting a subway car," a former senior U.S. intelligence official said. But the chairman of the U.S. House of Representatives Committee on Homeland Security, Republican Michael McCaul of Texas, called the incident "severely disturbing."

Ministers during the Committee’s 109th Session on November 8, 2001. The Convention was opened for signature in Budapest, on November 23, 2001. Thirty-five countries have signed the treaty, with Albania and Croatia having ratified it as well. The Convention will come into force when five states, three of which must be COE members, have ratified it. The treaty is intended to create a common cross-border “criminal policy aimed at the protection of society against cybercrime . . . by adopting appropriate legislation and fostering international co-operation.”

6.1 Importance of the Convention

The COE’s Convention on Cybercrime is paramount important international legislation because it binds countries in the same way as a treaty. “An international convention, or treaty, is a legal agreement between governments that spells out a code of conduct.” Once a large number of states have ratified a treaty, then it becomes acceptable to treat it as general law. Treaties are the only machinery that exist for adapting international law to new conditions and strengthening the force of a rule of law between states. Thus, it seems very important for an international regime to be set up to combat these types of crimes in a growing and integrated global society, which is becoming ever more vulnerable to cyber-attacks.

6.2 Objectives of Convention

---

63 Convention supra note 61.
64 Ibid.
65 Council of Europe, Chart of Signatures and Ratifications, available at (http://conventions.coe.int/Treaty/EN /CadreL isteTraites.htm) (accessed 6 December 2002) (signatories include: United States; Albania; Armenia; Austria; Belgium; Bulgaria; Canada; Croatia; Cyprus; Estonia; Finland; France; Germany; Greece; Hungary; Iceland; Ireland; Italy; Japan; Malta; Moldova; Netherlands; Norway; Poland; Portugal; Romania; Slovenia; Spain; Sweden; Switzerland; South Africa; Ukraine; United Kingdom; and the former Yugoslav Republic of Macedonia).
66 Wendy McAuliffe, Council of Europe Approves Cybercrime Treaty, ZDNET UK NEWS (21 September 2001), available at (http://news.zdnet.co.uk/story/0,,t269 -s2095796,00 .html).
67 Convention, op. cit note 64, preamble.
70 Ibid.
The Convention is intended to be the “first international treaty on crimes committed through the Internet and other related computer networks.”\textsuperscript{71} The provisions in the articles, particularly deal with infringements of copyrights, computer-related fraud, child pornography, and violations of network security.\textsuperscript{72} Its main objective, set out in the preamble, is to “pursue . . . a common criminal policy aimed at the protection of society against cybercrime . . . especially by adopting appropriate legislation and fostering international co-operation.”\textsuperscript{73}

### 6.3 Parties involved in the Convention

The Convention is open to worldwide membership.\textsuperscript{74} Instrumental in its drafting were the forty-one COE “countries, which cover most of Central and Western Europe.”\textsuperscript{75} In addition, the United States, Canada, Japan, and South Africa also aided in its drafting.\textsuperscript{76} As stated earlier, as of the date of this publication, thirty-five countries have signed the treaty.\textsuperscript{77}

### 6.4 Scope of the Convention

The Convention is broken up into four main segments, with each segment consisting of several articles. The first section outlines the substantive criminal laws and the common legislation all ratifying countries must adopt to prevent these offenses.\textsuperscript{78} The second section delineates the prosecutorial and procedural requirements to which individual countries must adhere.\textsuperscript{79} The third section sets out guidelines for international cooperation that most commonly involve joint investigations of the criminal offenses set out in section one.\textsuperscript{80} Finally, the fourth section contains the articles pertaining to the signing of the Convention, territorial application of the

\footnotesize{\textsuperscript{71}Convention, supra note 67, preamble.\textsuperscript{72} Ibid.\textsuperscript{73} Ibid.\textsuperscript{74} Lawrence Speer, Computer Crime: Council of Europe Cybercrime Treaty Attacked by ISPs, Business at Hearing, 6 COMPUTER TECH. L. REP. 100 (16 Mar 2001).\textsuperscript{75} Robyn Blumper, Cyber fear Leading to International Invasion of Privacy, MILWAUKEE J. SENTINEL, June 6, 2000, at 17A\textsuperscript{76} Ibid.\textsuperscript{77} Council of Europe Convention, Chart of Signatures, supra note 73.\textsuperscript{78} Ibid, Preamble.\textsuperscript{79} Ibid.\textsuperscript{80} Ibid.}
Convention, territorial application of the Convention, declarations, amendments, withdrawals, and the ever-important, federalism clause.\textsuperscript{81}

The substantive offences of the Convention

- Offences against the confidentiality, integrity and availability of computer data and system
- Computer related offences (fraud/forgery)
- Content related offences (child pornography)
- Criminal copyrights infringement
- Additional protocol concerning acts of racist and xenophobia nature committed through computer system.

- A number of cybercrime are not included in the Convention. For example
  
  i. identity theft  
  ii. grooming  
  iii. spam  
  iv. cyber terrorism.

The procedural laws

- Expedited preservation of stored computer data /expedited preservation and partial disclosure of traffic data.
- Production order
- Search and seizure of store computer data
- Real-time collection of traffic data
- Interception of content data

International cooperation

\textsuperscript{81} Ibid.
Jurisdiction
Mutual assistance
Extradition
24/7 network

Article 23: Parties shall cooperate with each other ‘to the widest extent possible’.

7. CONCLUSIONS AND RECOMMENDATIONS

Cyber-attacks on vital infrastructure are already becoming a widespread activity, where reports are filled in by the cyber security that computer infrastructure has become vulnerable. Speaking of computer vulnerability in the sense that today even the private organizations, countries and other responsible bodies are not free from the eminent cyber-attack to military, central banks, defences. Therefore the paper recommends that political commitment from the Heads of Countries would be a key precondition for successful law reforms in support of Nation ICT strategies within a specified timescale. The threat of cyber-attack has rapidly grown, the response and approach has not closed the gap. This paper indicates that those countries with strong cyber laws and the international community yet, failed to address, respond and update to the legal framework in combating cyber-attacks. It also recommends that it is essential to formalize countries with the legal and regulatory implication arising from the use of ICT and e-commerce. Generally, the continuous of new methods of this endemic threat of cyber-attacks, if governments continue to rely on limited bodies of law and not fully designed to meet with the modern trend of threats, a historic catastrophic cyber-attack will reveal itself. The paper further recommends expanding the reach of domestic law abroad and developing a system for utilizing limited countermeasures where appropriate and stakeholders should partake in the effective used and enforcement of cyber laws. According to Valerie Mac Niven, the cybercrime is growing at $105 B, total revenue of cyber criminals in the world is higher than for drug trafficking. The continued emergence is inevitable, as statistics pour out how much cybercrime costs the world. Hackers have been able to have free run from the internet, only being brought in if they make a silly mistake. That it become paramount
to provide a software tracker of internet service provider ISPs to monitor cybercrimes and make used of Patrol Unit so as to strategize the trace and track of the criminals. Adequate counter measures will not only help deter attacks when they happen but more importantly, deter hackers from launching them in the first place by organizing a training for the law enforcement agencies across the globe, region and sub-region.

"The scenarios—ranging from a virus that scrambles financial records or incapacitates the stock market,\(^{82}\) to a false message that causes a nuclear reactor to shut off\(^{83}\) or a dam to open,\(^{84}\) to a blackout of the air traffic control system that results in airplane crashes\(^{85}\)—anticipate severe and widespread economic or physical damage. While none of these scenarios has thus far occurred, numerous smaller incidents happen regularly. However, there is no agreed definition for identifying these incidents as cyber-attacks,\(^{86}\) much less as cyber-warfare. Only if the government will be able to come up with an accepted definition, then analyst be able to develop coordinated policy recommendations and will countries be able to act simultaneously to address the growing threat posed by cyber-attacks. It is when there is a coordinating and existing definitions, then a cyber-attack will be analyze in a wide range in order to identify the activity that lies at the heart of the concerns raised over cyber-attacks.\(^{87}\)"

---


\(^{84}\) Barton Gellman, ‘Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say’, WASH. POST, June 27, 2002, at A01.


\(^{86}\) As distinct from cyber-crime.

\(^{87}\) Oona A. Hathaway, supra note 19, p. 7.