# AN EVALUATION OF CYBER DIPLOMACY AGAINST THE THREAT OF CYBER CRIME: THE CASE OF THE US PRISM PROGRAMME LEAK

**BY**

**STEVEN JAMES DANDA**

**A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS OF THE MASTERS OF SCIENCE DEGREE IN INTERNATIONAL RELATIONS**

**DEPARTMENT OF POLITICAL AND ADMINISTRATIVE STUDIES**

**FACULTY OF SOCIAL STUDIES**

**UNIVERSITY OF ZIMBABWE**

**FEBRUARY 2014**

**ACKNOWLEDGEMENTS**

I would like to thank Dr. Chingono for her patient and diligent support and guidance without which this dissertation would have been possible.

Chamunorwa Madiridze, my compatriot through thick and thin, I really appreciate your relevant critiques and corrections to my ideas. Thank you very much.

**DEDICATION**

To my beloved mum and dad and my three siblings- Rachel, Walter and Sheila- I love you.

**ACRONYMS AND ABBREVIATIONS**

| | |
|---|---|
| AIDS | Acquired Immuno-Deficiency Syndrome |
| DPRK | Democratic People's Republic of Korea |
| HIV | Human Immuno-Virus |
| IMF | International Monetary Fund |
| UN | United Nations |
| US(A) | United States (of America) |
| USSR | Union of Soviet Socialist Republics |
| WB | World Bank |

**ABSTRACT**

The field of diplomacy and that of international peace and security are twin fields in constant flux and turmoil because of the latent dynamisms underlying the activities which make them worthwhile. Existing and emerging threats have necessitated numerous contributions towards a fuller understanding of these fields such that a lot of confusion too has emerged particularly in relation to the newer trends. One such trend is that of cyber diplomacy which has overtaken the traditional rules of etiquette of old diplomatic protocol which was largely limited to states and official state representatives. Cyber diplomacy, on the other hand, is characterised by a peculiar private society dimension, that novel encapsulation in information interchange through computer systems with the private spheres of national and foreign publics thereby causing a rapid decentralisation of certain information functions to the generality of civilians. Admittedly, cyber diplomacy has skated on the tide of globalisation-a staunch force reputed to have carpet-rolled and receded state borders and influence coupled with increasing porosity at international interfaces. Yet this has not been the final nail because increasingly complex cyber diplomacy has been attended with increasingly sophisticated cyber or computer crime which has posed unprecedented threats to the peace and security of states, private organisations and individuals. It was therefore the imperative chief focus of this paper to take time to study the nexus between cyber diplomacy and cyber crime and to draw applicable theoretical underpinnings from it. Much of the hubris for the research was obtained through content and thematic analysis of existing documents and purposive/judgmental techniques. This research concluded that there is an unmistakable connection between cyber diplomacy and cyber crime and also that cyber crime is rising as global communication network connectivity increases.

# CHAPTER ONE: INTRODUCTION

## 1.0 Background of the Problem

According to Melissen (2007:28) cyber diplomacy is the "development of public diplomacy or traditional diplomacy to encapsulate and utilise new dimensions of electronic information exchange within the realms of state interaction in the 21st century." This means that electronic information exchange now constitutes a sizeable and growing portion of modern information exchange where traditional diplomacy largely entailed an equal bulk of tangible exchanges. He goes on to posit that cyber diplomacy "links the impact of innovations in communication and information technology to diplomacy" and that cyber diplomacy is also termed or is part of public diplomacy, E-diplomacy and Virtual diplomacy. These distinctions are very important in later analyses because the very nature of their terminology will enable a more comprehensive definition of issues which are in constant flux - cyber diplomacy and cyber crime. According to Melissen (Ibid) cyber diplomacy "recognises that current communication systems offer novel opportunities to interact with a larger public by adopting network approaches and making the most of a more multi-centric, global and interdependent system." It can be surmised then that cyber diplomacy has shifted from state-centric diplomatic protocol to engage a larger audience of non-state actors in the form of private organisations and individual citizens within a nation and abroad.

According to the United States (US) Dept of State cyber diplomacy is the new tool in fulfilling the US public diplomacy mission. Accordingly the Under Secretary for Public Diplomacy and Public Affairs in the US stated in 2013 that US public diplomacy was instituted to support "the attainment of US foreign policy goals and objectives, to advance national interests and to enhance national security by informing and influencing foreign publics and strengthening US-global relations." Every nation engages in some form of cyber diplomacy though there might possibly be no official cognisance of this fact. The US officially launched its cyber diplomacy initiative in 2009 according to the Office of Electronic Information (Bureau of Public Affairs) in the US. This was in response to changes in international relations in order to extend the range of US diplomacy beyond inter-governmental associations and to transform its statecraft by readjusting national diplomatic protocol to tackle old problems in novel ways through innovation. Thus cyber diplomacy has grown to encompass US national interests in cyberspace

according to the Bureau of Public Affairs in the US which include "governance, military uses of the Web, innovation and economic growth." According to the First Quadrennial Diplomacy and Development Review of 2010, it follows that cyber diplomacy has become a hot issue in international fora and in relationships between states, civil society and industry.

Cyber diplomacy is an arm of preventive diplomacy where according to the US Department of State "it complements age-old foreign policy techniques with novel instruments of statecraft that leverage networks, the demographics and the techniques of an intricately interconnected world." This means that cyber diplomacy is an antidote to the natural atrophy of global communications whose unfettered development can result in chaos (First Quadrennial Diplomacy and Development Review of 2010). Lichtblau (2013:3) explains 21st diplomacy as "an adaptation to increasingly varied actors including states, corporations, transnational networks, non-governmental organisations (NGOs), foundations, religious groups and citizens." To date, according to Metzl (1999:177-178), the "US State Department has 230 Facebook accounts, 80 Twitter accounts, 55 channels on Youtube and 40 accounts on Flickr. Metzl (Ibid:178) states that the State Department also has cyber diplomacy initiatives such as Digital Outreach Team, Opinion Space, Dipnote, Civil Society and Democracy dialogues. The same amount of fixation with cyber diplomacy by states is also being experienced in developed countries such as Russia, the United Kingdom and China.

It should however be noted that cyber diplomacy presents a new dimension of threats to national security and individual citizens because of the vulnerabilities of databases to unauthorised access and manipulation. Melissen (2005:2) states that cyber diplomacy has brought in "increasing national cyber border porosity and thus the increased vulnerability of states to asymmetric attacks." He goes on to say that cyber diplomacy has also led to a growing need to create and nurture friendly relations between and among states, to enhance national security systems and to harmonise technologies in order to preserve information integrity. Of note has been the infraction against citizen privacy by state authorities worldwide as revealed in the PRISM programme leak of 2013 where the US has been accused of hacking into phone and internet records of its own citizens and those of foreign citizens much to the chagrin of countries chiefly in Europe. Not only states are involved in ulterior cyber activities but also individuals, groups and organisations are engaging in cyber crimes against states and private citizens.

The issues mentioned briefly above shall be discussed around the PRISM programme leak which has roused a lot of controversy and debate a long time after the actual incident and espionage charges against Edward Snowden. The PRISM programme leak was an insider leak of classified information about covert US spying on domestic and foreign citizens which was a humiliation of the Obama administration in 2013. It therefore follows that the vulnerabilities inherent within cyber diplomacy usually manifest in the form of cyber crime. Cyber crime is defined by Lichtblau (2013:3) "as one form of terrorism that uses computer resources to launch attacks on critical infrastructures that could cause widespread destructive impacts such as serious economic, social, political disturbances, chaos and damage on the targeted area either driven by political objectives or economic motivation." Cyber crime is thus the broad term for all the threats to the smooth flow of cyber diplomatic relations and private citizen/organisation information integrity. Evidence suggests that cyber crime trends have been on a steady increase presumably as a result of the ever-increasing networking or computerisation of international relations. Computer network internationalisation has resulted in the rapid amalgamation of a blend of disparate motives such that both harmony and disengagement have been the indispensable result. Cyber crime shall be discussed in relation to cyber diplomacy in the course of this study. The study shall constantly attempt to discuss the nexus between the two to verify whether the two variables affect each other in any way or whether they are independent of each other but are affected by other hidden external factors. Perhaps the most important reference point is that cyber diplomacy and cyber crime are becoming increasingly complex.

### 1.1 Statement of the Problem

According to Bar-Levav (in Coulbert, 2012:11) "national cyber networks are vulnerable to breaches using software such as Stuxnet." Coulbert (Ibid: 13) notes that "Stuxnet-style attacks on vital control systems are made worse because the motivations are much more political and ideological than economic." This means that "cyber-terrorist" attacks for instance, can have a horrendous impact such as offsetting a nuclear Armageddon. James (2013:1) states that "a nation such as the US, with thousands of information websites, whose military, financial or political systems are networked on the web, is more vulnerable to cyber attacks." How far will a few fundamentalist terrorists with meagre means but with computer access to US, Russian and Chinese weapons systems go in negatively altering the rather uneasy cyber diplomacy interface among these three nations?

Melissen (2005:3) states that "if the original intention of cyber diplomacy was to apply 'soft power politics' and to nurture progressive relations between and among states, or to promote and preserve national security, it has also exposed these same benefits of networking and communication to the vulnerabilities emerging from the potential weaknesses in E-diplomacy." Melissen (Ibid) then concludes that "a 'loosing' of unprecedented 'hard power' becomes a dire possibility as a result." Besides outright cyber terrorism, the hacking of national information systems and the selling of illegally retrieved information presents an ever-present threat in the form of cyber espionage. Edward Joseph Snowden, a former Central Intelligence Agency (CIA) and NSA employee leaked details of US top secret and British mass surveillance programmes to the media (US Department of State). This information according to the US Department of State pertained to programmes of telephone metadata interception in the US and Europe such as PRISM, XKeyscore and Tempora Internet Surveillance. US Pentagon papers have been leaked by Daniel Ellsberg in the past according to the office of Electronic Information, Bureau of Public Affairs in the US. In spite of espionage charges laid against Snowden by the US government on 4 June 2013, the culprit has been globetrotting first to Hong Kong then to an unspecified location in a Russian airport where he has been granted temporary asylum which is renewable on a one year basis while he remains in Russia.

According to Mclanahan (2013:1) some officials in the US have accused Snowden of having caused grievous damage to US intelligence systems through his leaks while others such as the former US president Jimmy Carter have praised his actions as heroic. The 2013 PRISM programme leak has certainly kindled healthy debate on mass surveillance, on government secrecy and on national diplomatic security and citizen information privacy (James, 2013). These debates will be explored during the course of this research.

## 1.2 Literature Review

The definition of cyber diplomacy given by Melissen in the introductory section of this paper, while admittedly correct in some respects, fails to encapsulate and appreciate the nexus between diplomacy and computerisation. He calls cyber diplomacy a "development" without regard to the fact that cyber diplomacy is an established field. This study has concluded that cyber diplomacy entails the comprehensive harmony and disharmony of all the dimensions of state-to-state or

private spheres among themselves or with states that is governed by the laws of computer networking and electronic information exchange. Cyber diplomacy is an established reality.

Melissen (2005:3) states that "after September 2001 much confusion still surrounded cyber diplomacy and that espionage (a form of cyber crime) is an aspect of most diplomatic overtures. This seems too simplistic given that cyber crime is much broader than the narrow delimitation to espionage alone. This study is focused on exposing all the possible dimensions of cyber crime and chart means and ways of averting their perpetration. Among other things it shall exposit 'phishing' or identity fraud, the use of malware or malicious software and hacking. Espionage has fast lost its esoteric form to become an electronic reality.

Joseph Nye stated that "countries that are likely to be more attractive in postmodern international relations are those that help frame issues, whose culture and ideas are closer to international norms and standards and whose credibility abroad is reinforced by their values and norms. In a realist sense this assertion does not ring true. Nations do not have to be 'big' to be influential. Small nations such as the Korean peninsula or Iran have inadvertently framed issues though their influence. For instance, the policies of sanctioning them had to emerge from the nature of contention they caused. This is not to detract from Nye's assertion that cyber diplomacy is dominated but not *exclusively* controlled by powerful nations such as the US, Russia and China.

Chernenko (2001:5) distinguishes between traditional diplomacy and public diplomacy stating that the former is about "relationships between representatives of states and international actors while the latter is about the general public in foreign societies and non-specific organisations and people. While this distinction is vital in understanding that cyber diplomacy embraces not only ambassadorial relations but also relations between states and foreign publics and organisations, it fails to explain the nature of the interactions. Friendly and unfriendly interactions occur and relationships are formed and destroyed with a great degree of simultaneity. In essence then it becomes clear why the US has relations with for example, the Afghan state and the al Qaeda terrorist organisation within Afghanistan and beyond.

Morris (2009:11) states that public-private diplomatic relations are poised to increase in extent and complexity given the ever expanding multiplicity of organisations in sectors outside states. What the above assertion lacks is an explanation of the driving force behind the increase in complexity of relations. This paper shall conclude that the continuous improvement of

communications technology and the latent force of globalisation are the chief drivers of complex interactions. Therefore in assessing cyber diplomacy against threats of cyber crime it is imperative to draw motivations behind and implications of state and non-state actor behaviours from the full range of possibilities in cyber interactions.

Melissen (Ibid:10) postulates that "rogue states are like non-state actors in international relations in that they have largely benefited from a decentralisation of information power." This question deserves more qualification since it means that the relations between states become more blurry where 'rogueness' comes into play. The debate on what really constitutes 'rogueness' would be an exciting aside however it could perhaps lead to a diversion from the issues at hand which pertain to cyber politics. Therefore notwithstanding the aptness of the label 'rogue state' in cases such as the US-North Korea cyber relationship, it becomes clear that relations between non-rogue states or non-state entities are easier to analyse. This paper shall discuss such relations in greater detail.

Metzl (1999:177) opines that information power has been decentralised to a high degree especially in non-rogue states such as the US which has numerous data accounts on the web and various electronic programmes and initiatives. But is this not also true for rogue states themselves? If the answer to the question just posed is in the affirmative then cyber diplomacy intelligence gathering techniques and cyber crime by state and non-state actors shall continue to proliferate for every country. Lichtblau (2013:1) concludes that it will be imperative in the near future to create cyber intelligence networks given the daring rise of cyber crime. Here countries and citizens must work hand in glove towards a more comprehensive outlawing of cyber criminal activities. Yet how far is this idea workable especially where citizen suspicions of covert state intelligence gathering through metadata interception have been roused to a high extent by revelations such as PRISM? Can European and American citizens for example fully participate with their respective governments in combating the cyber crimes against their governments without fear of state invasion of individual privacy? It is the main focus of this paper to discuss the issues posed above which it is felt, have not been adequately dealt with in existing literature.

## 1.3 Theoretical Framework

This investigation shall take into account realist perspectives in evaluating the relationship between cyber diplomacy and cyber crime. According to Steans and Pettiford (2001:28) realism assumes that "human nature is selfish, states are the central actors in the international system, power is the key to comprehending the international system and international relations are inherently conflictual." States, like individuals, are fundamentally self-centred according to the realist perspective. Steans and Pettiford (Ibid) state that "some realists assume that there are immutable laws which regulate individual and state idiosyncrasies such as self interest and aggression." It can thus be expected that cyber diplomacy is pursued by states and individuals with the propensity for selfishness and aggressiveness in mind. This means cyber diplomacy is conducted in a realm of anarchy without the possibility of reprieve attained possibly only through a central global governing authority (Ibid:23). In other words cyber diplomacy is essentially an attempt at a safeguard against the exigencies of an uncertain geopolitical order.

If it is to be firmly held that states are 'central' actors in the international system according to Carr (in Ibid:23), then cyber politics is limited to state machinery. However this does not ring true where "cyber diplomacy has gathered dross in the form of industry and civil society" according to Melissen (2007:58). Even terror groups have pervaded the grey areas of cyber diplomacy with, for example, instances of cyber attacks (purportedly by North Korea) on South Korea in early 2013 (Lichtblau, 2013:1). States are 'central' actors to a varying extent. Cybercraft influences and is majorly influenced by various actors outside the confines of individual states.

Realism according to Steans and Pettiford (2001:25) states that "power is the central element in understanding the complexities of international relations." In the realist school, power defines geopolitics. Carr (in Ibid: 23) states that those who wield this asset in its greatest proportions control the world. It seems then that in this information age intelligence translates to power in a realist sense and because power is vital in establishing cherished positions in the international political configuration, nations such as the US, UK, China and Russia have been on an inexorable scramble for it through cyber diplomacy initiatives.

Steans and Pettiford (2001:25) postulate that the "condition of anarchy" in international relations stems from "the lack of a central sovereign authority to regulate relations between states." Cyber diplomacy works behind a facade of anarchy. This means no single state can be said to solely control global cyber politics. According to Lichtblau (2013:1) the "accusations thrown between the US and China or between North and South Korea pertaining to cyber crime are difficult to mollify" given the almost nocturnal nature of E-diplomacy." Steans and Pettiford (2001:25-26) state that international law institutions do play a role in international relations but can only be effective if backed by an effective system of sanctions. It however seems very difficult to establish stable electronic diplomacy legal parameters because the realm of cyber politics is in constant flux. New software such as Stuxnet has been used to 'border jump' cyber borders without detection before it is transformed by software developers into more novel morphed threats (Colbert, 2012:16). In a Hobbesian sense the milieu of cyber diplomacy is in a state of nature. This finds support in Machiavellianism which regards "ethics or justice in international relations as simple states of preference of the already powerful" (Ibid:27).

### 1.4 Hypothesis

The increasing complexity of cyber diplomacy due to the computerisation of communication networks, the miniaturisation of technology and globalisation has made states, private organisations and individuals more vulnerable to cyber crime.

### 1.5 Objectives of the Study

- This study is fundamentally poised at evaluating the notion that cyber diplomacy inadvertently enhances cyber crime.
- In regard to the foregoing the study shall seek to examine the full range of cyber diplomatic activities entailing intelligence gathering through espionage and acceptable means such as overt research, its management and dissemination for use in maintaining state integrity.
- The study shall then seek to pinpoint the list of possible threats and weaknesses presented by cyber attacks in the form of cyber terrorism and cyber espionage and their possible implications. This shall be conducted in conjunction to an evaluation of current measures used in combating cyber threats and future prospects for cyber systems.

- Then possible diplomatic, legal and/or electronic (software) solutions and recommendations for combating cyber threats shall be provided. It is hoped that this study will help in a major way to fortify the present foundation for future research into the area of cyber diplomacy.

### 1.6 Research Questions

- What are the definitional parameters of cyber crime and what legal frameworks exist or can be instituted to safeguard against it?
- In what way does cyber diplomacy lead to enhanced cyber criminal activities and how can this link be abolished where it is held that the crime is deleterious to state integrity and citizen security?
- What are the current measures being employed to curb or combat cyber criminal activities and how successful have they been? What can be done to improve the current measures being used to reduce cyber crime?
- Since the study of cyber diplomacy is futuristic, what foundations can be laid to better facilitate future research?

### 1.7 Significance/Justification of the Study

This study will profoundly contribute to existing literature in a novel way. According to James (2013:1) “cyber diplomacy opens up nations and societies in ways that can either be fruitful or harmful.” This study will be an analysis of the strengths, weaknesses, opportunities and threats cyber diplomacy presents to states and individual citizens within the international community. Then apart from contributing to existing literature, this study will amalgamate and critique traditional, contemporary and current intellectual standpoints against a backdrop of ongoing trends.

Cyber diplomacy is a relatively new field that is little understood. This study shall attempt to come up with additional ‘patois’ for the discipline. This will help future researchers in understanding exactly where cyber diplomacy and cyber crime are going and also to accurately define their basic tenets. Such knowledge will be useful in articulating measures for diminishing

the strength of the connection between diplomacy and crime. There is little literature linking cyber diplomacy and cyber crime and this study, it is hoped, will present a brave attempt to merge the two for purposes of analysis. Then over and above everything this study seeks to accomplish, this research will give solutions to the problem of cyber crime.

## 1.8 Methodology

### 1.8.1 Research Design

The study will use both primary and secondary sources of information such as individuals and existing literature and both quantitative and qualitative methods such as simple random sampling and expert sampling techniques. This is because the field of cyber diplomacy is broad and multifaceted and somewhat novel besides its inherent dynamism which necessitates something of a holistic analysis of its present and future trends. Existing literature is vital in the sense that it forms the basis for even deeper analyses of the pertinent issues at stake. Existing literature shall therefore be used either to verify or refute certain claims that come with the study. Quantitative and qualitative information will be of paramount importance in that it bridges the subjective-objective dimensions of research through its utility in explaining ontological and epistemological issues.

### 1.8.2 Sampling Procedure

Sampling procedures will be as diverse as possible in order to encapsulate as many dimensional possibilities of cyber crime and cyber diplomacy as is possible. This research will use expert, systematic, simple random, and cluster sampling procedures since cyber diplomacy is highly specialised. This means experts, intellectuals, politicians, influential people and the general public will be approached for information. Expert samples will help define the course of research through the provision of disciplinary analysis and subject dialect. The didactic reasoning provided by experts will also prevent this research from going overboard and out of bounce. Systematic sampling will enable the researcher to cross-compare findings of parallel research. Simple random sampling will provide a ‘gung-ho’ facility for picking information without the limitations which naturally arise from careful planning which can be very constraining to

intuition. Cluster samples will help gather information more quickly and comprehensively given their nature of logically grouping sources of information to cover as much ground as possible.

### 1.8.3 Data Analysis

The study shall utilise documentary search, participatory and non-participatory observations in data analysis due to its scope and futuristic nature. Thematic and content analysis will therefore play a pivotal role in data analysis and they will be juxtaposed for comparison and reference purposes. Coupled with this, the analysed material will be compared with findings elsewhere in order to either accept or reject certain elements gathered from the research. Documentary searches will be useful for gathering information quickly and much of this work will be done on the internet. Participatory and non-participatory observations will enable the research to delve deeper into certain issues in a tangible manner for instance the researcher might want to be taught how to create a computer anti-virus and know its application. There are individuals who are tackling cyber crime and cyber diplomacy with equal care each day and their experiences could be obtained better in a practical sense.

## 1.9 Limitations

The research may face inadequate access to US state/public information due to security mechanisms in place since cyber diplomacy is a hot topic given the recent humiliating Snowden leaks and international despondency over the same fact. This means that misinformation by US state officials is a real possibility. Cyber diplomacy is a dynamic field and the rate of change within that same field can outpace research and cause bursting timelines.

## 1.10 Delimitations

This research seeks where possible, to ascertain the exact nature of the PRISM leaks and the extent of damage and/or benefits accruing to the international community at large as a result. This will require a combination of objective and subjective assessments within a lengthy timeframe because of the inherent complexity and dynamism within the domicile of cyber questions. It might however not be possible to access the actual textual or quantitative data for reference purposes because of the obvious reasons of possible state classification. However, a rigorous attempt to obtain pictographic and textual information and also actual interviews shall,

in as much as possible, ensure that research goes as deep as is permissible. There are no limitations to the depth and scope of this research.

## CHAPTER TWO: THE NEW PUBLIC DIPLOMACY

### 2.0 Introduction

To understand the path charted for diplomatic intercourse between nations from traditional diplomacy to its modern variations (entailing a broad spectrum of public diplomacy comprising e-Diplomacy, cyber diplomacy or cyber-craft), it is vital first of all, to deal with the definitional issues of diplomacy itself. Melissen (1999: xvi-xvii) outlines definitions of diplomacy according to *purpose* (art of resolving international disputes peacefully); according to *principal agents* involved (conduct of relations between states through accredited representatives); and according to *function* (the control of international relations through negotiation). This means diplomacy can be defined as the art of resolving and managing international problems peacefully though negotiation by accredited representatives.

However modern international relations are never conducted (even in the strictly most ideal circumstances) by symmetrical state representatives and neither are the participants limited to states actors alone nor are they neatly identifiable. This means that the definition of diplomacy within terms like 'cyber diplomacy' and 'public diplomacy' has to change to suit modern complexities. An example of such complexity is the growth of social networks such as Flikr, Twitter, Yookos and Facebook which have been increasingly influential in disseminating information to a wider audience. Public diplomacy (modern/cyber diplomacy) entails a multiplicity of state and non-state actors which means a definition focusing only on purpose, agents and function becomes too limited. The modern international system entails a plethora of diplomatic motivations driven by increasingly unconventional reasons and diplomatic protocol is no longer the preserve of state agents alone. The new public diplomacy therefore warrants a more encompassing definition and the historical outline below of the evolution of traditional diplomacy to its present form is hoped to provide a working definition.

This chapter shall discuss the course traditional diplomacy took; that is from its traditional nature to its contemporary and more modern variations. This issue shall be tackled with the view of diplomacy as encompassing both 'hard' and 'soft' power politics. The salience of soft power over hard power shall be the main catch-point of the next section. Then the chapter shall delve deeper into the exact nature of the new cyber politics linking it to cyber criminal activities before a conclusion is reached which will b a tool to link the next chapter to the present one whose main

goal will be to discuss the nature of cyber crime. This section is hoped to rouse sufficient intellectual inquiry and to narrow focus on the relevance of cyber politics in the modern era.

### 2.1 From Traditional Diplomacy to the New Public Diplomacy

Melissen (2005: 4) states that it is tempting to see the new public diplomacy as new wine in old bottles. He goes on to state that the distinction between traditional diplomacy and public/cyber diplomacy is clear where "the former is about relationships between state representatives or other international actors and the latter pertains to the targeting of the general public in foreign nations consisting of non-official organisations and groups" (Ibid: 7). Cooper (2003: 76) states that image cultivation by nations through propaganda and overt diplomatic actions that is today labelled cyber diplomacy, is an age-old phenomenon. This means that traditional diplomacy stems from Biblical, Greco, Roman, Byzantine and Italian Renaissance times. He cites the Venetians who towards the end of the Middle Ages had already introduced a system of methodological dissemination of newsletters within their own diplomatic service and that Gutenberg's invention cleared the path for true international public relations for example the Cardinal Richelieu in 17th century France. The foregoing means that nations are bent on promoting their national images in a positive way for the obvious reason of geopolitical position fortification. Positive images carry forward power and relevance on the international arena hence the need to lobby for the national image abroad by even the biggest and most powerful nations in the world.

According to Kunczik (2003: 399-405) France under the *Ancien Regime* went to much greater lengths in promoting its national image abroad. In the aftermath of the Ottoman Empire, Turkey followed suit. For instance Kemal Ataturk's complete makeover of the face of Turkey enabled the possibility of the country's integration into the European Union (EU). In the 20th century Fascism and Communism were versions of "identity-creation and nation-building" which "challenged and gave direct impetus towards communication with foreign societies by democratic nations" (Melissen, 2005: 5). Today it seems vital to blend diplomacy with positive image building because globalisation means no single political actor can be a stand-alone factor since every action a political actor undertakes draws a positive or negative reaction. The globe is airtight with regards to political actions.

After the Second World War which saw the development of professional image cultivation across borders, the importance of "soft power" increased in salience according to Nye (1990 in Melissen, 2005: 5). Diplomacy emerged as the chief alternative to Machiavellianism. Interstate conflict intensified between the two world wars meaning that "power over opinion was no less important for political reasons than either economic or military power" (Carr, 1983: 132). This means that "hard power" (military/coercive confrontation) and "soft power" (diplomacy/politicking) are inextricably intertwined. This means hard power (coercive/military confrontation) and soft power (diplomacy/politicking) are inextricably intertwined. However the two world wars had proved disastrous with loss of lives in the millions. The barbarism of hard power could no longer be fathomed and as such, the Washington, San Francisco and Dumbarton Oaks conferences between 1944 and 1945 were affirmations of the need to confirm sentiments for peace as embodied in the United Nations.

From the foregoing Melissen (2005: 5) concludes that "soft power is growing in importance in the global information age and that the loss of soft power can prove to be very costly for hard power due to the ever-growing multiple transnational linkages." This raises the question of attraction in international politics where Nye (1990: 5-6) concludes that nations "which are likely to be most attractive in postmodern international relations are the ones that help frame issues, whose ideas and culture are nearer to the norms prevailing internationally and whose credibility abroad is solidified by their domestic policies and values." With this in mind it can be surmised that cyber diplomacy is one of soft power's chief instruments. During the Cold War, it became clear why the US, the former Soviet Union (now Russia) and the three major European powers (Britain, France and Germany) invested as heavily as they did in communications with the world.

The post-World War 2 communications revolution that increased in pace towards the end of the twentieth century according to Melissen (2005: 6), "enabled private citizens to get information about other countries rapidly or even faster than governments." The global media have become more intrusive and influential over public opinion such that public opinion has become a very important factor in international relations. Moreover, "the competition of ideas between and among states has intensified in ferocity and attained a particularly global dimension (Ibid: 6)." Newly emerging nations such as South Sudan have become both targets and practitioners of cyber diplomacy." Perceptions have therefore become as important as reality.

The post-World War 2 communications revolution which increased in pace towards the end of the twentieth century therefore enabled private citizens to get information about other countries and their people rapidly or even faster that governments. The global media have become more intrusive and influential over public opinion such that public opinion has become a very important factor in international relations. Moreover, "the competition of ideas between states has intensified in ferocity and attained a particularly global dimension" (Ibid:6). Newly emerging nations such as South Sudan have thus become both targets and practitioners of cyber diplomacy which means that cyber politicking has also been bottled down to their private citizens. Perceptions have thus become as important as reality. The public have been factored irreversibly into the political equation and anything going against such a stance has been increasingly viewed as retrogressive. This means cyber diplomacy is here to stay.

Melissen (1999: xvi-xvii) opines that the "democratisation of information access has conditioned citizens into becoming independent observers as well as active actors in international relations." As a result the new diplomatic agenda entails an addition to the leverage of loosely organised groups of private citizens. This means that as cyber diplomacy has gown, there have been problems which have also arisen because of the fact that diplomacy itself has been decentralised to responsible and irresponsible citizens alike. Potter (in Melissen, 2005: 7) argues that since global networks have intensified because of globalisation with the effect of transcending national borders, "publics distrustful of governments demand increasing transparency and input into policy-making such that it has become more difficult for governments to rely on 'spin' to curtail communication challenges." This is due to the fact that publics and governments have become more and more embroiled in a spirited battle for information control and interest articulation.

Whether globalisation has led to increased democracy is another issue but what is more apparent are the negative exigencies globalisation has brought in through its assurgency of global participants in information exchange. As such it can be better explained how cyber crime in the form of cyber terrorism, hacking (cyber espionage) and cyber attacks on national systems has become a constant dire possibility. Melissen (2005: 7) states that because of this, "there exists a global milieu where the divide between domestic and foreign policy is exponentially narrowing and image control has shifted from elite management to a wider 'mass' market." Cyber diplomacy is therefore poised to become a centre point in modern diplomacy simply because

information power has usurped hard power politics. This has made information transactions smoother especially where the cash medium is involved.

## 2.2 The Nature of the New Diplomacy

According to Technolytics (2013: 1) "cyber diplomacy is the ongoing evolution of contemporary diplomatic relations between states, virtual states and other related groups and bodies. This means that cyber diplomacy is very closely related to Public Diplomacy 2.0 Virtual Diplomacy and e-Diplomacy (Ibid). In 2006 the Bush administration engaged in its initial cyber diplomatic initiative although it was in 2009 that it officially launched its public diplomacy awareness campaign. This was followed by the 2011 government release of an international strategy for its cyber space programme which laid out US foreign policy priorities. Apart from the US government initiative, cyber diplomacy has become a new imperative for all governments around the globe. A spokesperson for the European Union (EU) opined in 2003 that a majority of very visible and damaging cyber incidents have become politically motivated.

Technolytics (2013: 1) states that the new cyber diplomacy expands, enhances and fortifies relations between nations, advances national security through futuristic electronic initiatives, promotes national interests and is a progressive embellishment of foreign policy goals and objectives. However the view that cyber diplomacy has become a common tool for peaceful interest realisation by many nations within the cyber space stands exposed to contestation. In a desperate attempt to control or to obtain information, certain sectors of modern society are using extremely roguish methods. As a result, it can be said that the new cyber diplomacy is being used in articulating and coordinating soft power in achieving specific national goals and objectives whether they be good or bad. The Snowden leaks are a fitting example of this fact. Cyber politics is anarchic in as much the same way the Hobbesian Leviathan was.

In influencing international relations, the persuasive approaches enshrined in the application of soft power are poised at achieving a "nation-state's" or "virtual-state's" goals without the use of force. While this means cyber diplomacy can be called 'indirect pressure' it is very difficult to see how all of a nation's goals and objectives can be achieved without the use of some form of force. Achievements by one party imply a loss of advantage by the other party. So if cyber diplomacy can be rightly called 'indirect pressure' that pressure involves disputation and contestation; contestation entails conflict and conflict settles both winners and losers in a cycle of

emotive battles. Therefore the idea of 'zero force' is an ideal only possible in heaven in the absence of the demons of mortal greed and ego. As more and more nations become involved in cyber diplomatic overtures in a complex way, the overall dynamism of cyber diplomacy is expected to increase.

The former US Secretary of State Hillary Rodham Clinton in 2011 articulated seven US international cyber policy priorities which can be used to describe an ideal state of modern cyber diplomacy. They have been articulated here simply to expose their fundamental idealistic flaws. These include the enabling of open, innovative markets; the enhancement of reliability, resilience and security of global information networks; the extension of international law enforcement collaboration; the enabling of a state of preparedness for the challenges of 21st century geopolitics; the increasing of support for inclusive and effective internet governance structures; capacity-building, prosperity and security through holistic international socio-political and economic development; and the support of individual privacy and fundamental freedoms. Such ideals are unattainable given the US's totalitarian aspirations on the global cyber diplomatic platform.

Global powers such as the UK, France, Russia and China have invested billions in initiatives such as the US cyber diplomatic initiative outlined above indicating not only the extent of importance of such an engagement, but also its futility. This means public cyber diplomacy can no longer be dismissed merely as "an attempt at manipulation of foreign publics through electronic means" (Melissen, 2005: 7). It has become an attempt at the impossible. It is thus advisable to let go of images of traditional diplomacy in the appreciation of modern diplomacy. Cyber diplomacy has become more than just propaganda and the new public diplomacy requires techniques, skills and attitudes different to those found in traditional diplomacy. Currently what exists is an innocuous mixture of traditional ribaldry with the modern, half-hearted attempts at goals which are constantly drifting off into an uncertain horizon.

Melissen (2005:8) opines that "in regions with a high degree of political and/or economic interdependence and connectivity at civic society levels", cyber diplomacy has become "essential in diplomatic relations." This describes the new public diplomacy as the process through which "direct relations with people in a country are pursued to advance the interests and extend the values of those being represented. In this sense therefore, the new public diplomacy is not a uniquely stately activity but is one in which "large and small non-state actors and supranational

and sub-national players develop public diplomacy policies of their own" (Melissen, 2005: 8). Obviously confusion is expected to emerge from the existing plurality of opinion even though it seems democratic.

What can be worrying where intentions are bad is that certain non-governmental organisations (NGOs) have proven to be particularly adept at influencing foreign societies. Organisations such as Doctors Without Borders (Medecins Sans Frontiers), Greenpeace and Amnesty International are operating in increasingly malleable international systems and networks. Converging interests between NGOs and states are very observable. International companies in the global marketplace are also observing the importance of cyber diplomacy to the extent of suitably altering their public diplomacy policies. This means cyber diplomacy functions better in a network/systems model rather than in a state-centric environment. This is a field within which the multiplicity of actors can draw valuable lessons through interacting with each other.

Public diplomacy can no longer be seen as a 'one-way information flow' from states to foreign publics. Melissen (2005: 10) calls the new public diplomacy "niche diplomacy" citing the diplomatic initiatives of Canada and Norway where an equal amount of the reverse process is taking place. Governments are learning from the private sector. In a traditional sense this can be viewed as espionage if taken to extremes. Public diplomacy pursues a wide range of objectives such as foreign investment and trade, political debates, establishment of links with private groups and organisations and other activities involving 'hard power' management in alliances, military intervention and conflict prevention (Ibid: 10). Cyber diplomacy is not entirely altruistic because the plurality of actors also has the potential to add an ulterior aspect to the diplomatic mix.

State terrorism, private terrorism, hacking/espionage and other cyber criminal activities such as information network sabotage and bank fraud have altered public diplomacy in uncertain and unexpected dimensions. Despite the 2004 visit to Muammar Gaddafi the former deposed Libyan leader by former leaders (British Prime Minister Tony Blair, French president Jacques Chirac and German Chancellor Gerhard Schroeder) in an ostentatious show of public support, the rogue Libyan leader had presided over successful state terrorism using cyber diplomatic initiatives. Terrorist organisations such as Boko Haram in Northern Nigeria and Al Shabbab in Somalia depend on efficient cyber diplomacy networks for the success of their activities. Hackers/spies such as the Russians, Artem Semenov and Peteris Sahurovs and the US Edward Joseph Snowden depend on the availability of efficient cyber databases. The early 2013 network sabotage by

North Korea (DPRK) on South Korea was facilitated by manipulating existing cyber network initiatives.

The above means one should caution too close a nexus between public diplomacy and foreign policy since other actors besides states play a profound role in the public diplomacy dimension of today (Ibid:11). Coupled with this there is a risk of confusing public diplomacy objectives with lobbying especially where it is assumed that public diplomacy activities are aimed at creating positive public opinion in a target country which will compel its leaders to formulate policies favourable to a state which initiates the public diplomacy initiative. This is because it exposes public diplomacy to the contradictions, discontinuities, fads and fancies of foreign policy. Sometimes public diplomacy is intended to create the reverse order for certain reasons. An example could be the diplomatic initiative of the DPRK with regards the US or South Korea. It is obvious that North Korea wants to portray itself as the careless rogue for purposes of fear-mongering and therefore its cyber politics will be inclined towards a tactic of ampersand.

### 2.3 Conclusion

From the foregoing analysis of public diplomacy and hence cyber diplomacy initiatives, it can be deduced that the future of cyber diplomacy could envisage various implications. It can be expected that a cyberspace milieu that rewards human innovation in an ideal sense will be not be created. Only as an ideal would the envisaged cyber diplomacy have the potential to empower governments, empower people, safeguard human rights and other fundamental freedoms, encourage public accountability, promote privacy and ultimately preserve and protect international and national security. This view is overly optimistic and in a realist sense it is most obvious that this optimism will be countered on the ground given past and current trends.

Diplomacy is not intended to be an entirely altruistic enterprise when self-interest is factored in. Man is by nature a selfish political animal. So what can we expect? We can expect an innocuous blend of the eternal vagaries and vanities of classical diplomatic protocol with the contemporary and modern half-hearted pursuits at the supposed ideal. Everyone wants an ideal state of affairs as long as it does not cut off their comparative diplomatic advantage and will give half-hearted support to any initiative which does not bring them some direct benefit. Such is the international system.

## CHAPTER THREE: OF CYBER DIPLOMACY AND CYBER CRIME

### 3.0 Introduction

It is indisputable that cyber crime has been inexorably attached to cyber diplomacy. The nexus has arguably grown stronger and gotten more influential in altering the foreign policies of states more directly involved in cyber diplomacy. This means that the incidence of cyber crime has risen exponentially as more effective cyber networks grow in gamut implying that cyber diplomacy has the adverse potential to militate against national and private security. The novelty of the threats to legitimate cyber politics has necessitated greater transnational cooperation at all tiers of state and nation. This is because cyber crime is insuperable from a single dimension. Yet this requisite cooperation has not been actuated because certain states, like terrorist organisations, are employing similar rogue techniques into the cyber diplomacy broth pot thereby causing or exacerbating international sensations of distrust, suspicion and secrecy. Coupled with this, historically divergent ideological propensities such as existed between the communist fraternity and capitalist blocs, have not facilitated international unison. This issue of ideologies shall be discussed in greater detail in the course of this chapter. This chapter shall trace the inverse salience between cyber diplomacy and cyber crime after defining the exact nature of cyber crime.

### 3.1 The Nature of Cyber Crime

According to Moore (2005:1) cyber crime is any crime involving a computer and a network. This means that the computer may be used to commit an offence or it can be the target of a crime. Cyber crime is also called computer crime (Ibid). Cyber crime is also defined as “offences done against people or groups of individuals with the criminal motive to harm the victim’s reputation using chat rooms, e-mails, notice boards, groups and mobile phones.” The very fact that much of this information can be readily found in national/centralised electronic databases such as the national registry for national identity cards or credit account numbers, means that the scope of insecurity to cyber crime becomes an issue of national security. According to Rousseau (2013:2) public diplomacy is a relatively young discipline which after the year 2000 became a central part of diplomacy. Revolutions in transportation and communication gave national leaders and diplomats the ability to see and be heard by more people globally than at any previous epoch in

history. When applied skilfully, public diplomacy can affect public opinion beyond a single country to support or oppose positions and policies, and can cause foreign publics to have a good opinion of the concerned country. On the other hand, weak public diplomacy can cause serious opposition even to those well-meant policy positions, and can send a very bad image of one's country (Ibid). Public diplomacy is therefore of paramount importance.

Diplomats actively look for and are quick to turn up speaking opportunities usually in media engagements, and always seek to work with other information-disseminating outlets in which they can get an opportunity to influence public views of their host country and the understanding of the sending nation's policies in a favourable way. Sometimes, host countries view such public diplomacy as meddling in their internal affairs. However, at other times, such public diplomacy may be seen as a legitimate aspect of a diplomat's function of representation. However, the diplomatic office has not always been that smooth sailing because recently a new, more malign type of diplomacy emerged without protocol.

In January 2010, Google suddenly announced that it had been majorly hacked since mid-2009 through to end of 2009. "Operation Aurora" as the attack was called was described as "high-level," and "sophisticated" being targeted at over 30 other organizations in the US such as Morgan Stanley, Adobe, Dow Chemical, and Northrop Grumman and Rackspace (Ibid). A 2011 report by Google stated that the cyber criminals, based in China's Jinan province, had stolen personal email accounts information of hundreds of top U.S. officials thereby compromising personal privacy. There has been no conclusive proof of the state-sponsoring of the attacks, and Google's Press Office stressed that the chief goal of the cyber criminals was to penetrate and access their computer databases to obtain the Google mail accounts of Chinese human rights activists.

The attack discussed above was not successful according to Google as user private data was never compromised. Whether this was a face-saving gimmick by the social network remains a matter of speculation. This is because it appeared that the attack could also have been conducted by the Elderwood Group—a Beijing based organization with links to China's politburo according to a U.S. State Department cable released by WikiLeaks in 2010 (Ibid). Security experts stated that they connected the attacks to university servers used by the Chinese military. Rousseau (2013:2) notes that numerous computer experts stated that the December 2009 attack was very similar in terms of the instruments and style used to the one of July during the same

year. The only difference was that the December attack was specifically targeted at specific individuals. Of note is that these attacks took advantage of some 'unknown' vulnerability of the Google software. This prospect of unknown software vulnerabilities is very unnerving since such vulnerabilities could extend to more classified state departments and weapons systems.

Just after a few hours of acknowledgment by Google of Operation Aurora, the U.S. State Department in an official statement asked the Chinese government for an explanation but official Chinese media countered stating that the entire incident was a clumsy part of a U.S. government conspiracy against China. Google then decided to relocate its Chinese operations going against Chinese regulations on censorship to Hong Kong, fearing that it would become a constant object of Chinese cyber attacks. The attacks caused serious diplomatic mudslinging between the US and China which till late has not quieted.

Issues of cyber security dominated the first summit when US President Barak Obama confronted the Chinese president on the cyber attacks perpetrated by China 2012 against close to 40 weapons programmes of the Pentagon which included aircraft, missile defence systems and ships (Ibid). Even though the exact level of official involvement by the Chinese government cannot be verified, the US government has called upon China to take a more tangible role in tackling violations of cyberspace by its private citizens. Where governments use new technologies in control of public opinion and espionage the wounds caused by a hacker attack can be considered the onset point of a novel type of diplomacy—Cyber Diplomacy. This means such new technologies will forever affect the geopolitical order of power.

A lot of useful deductions which would further a fuller appreciation of this study can be drawn from the US-China relations in cyber politics. The first is that social networks can also pose threats to governments. Google was hacked with the chief aim of accessing user data of high profile individuals some of whom were US and Chinese public officials. The second is that in their efforts to influence other nations, governments in implementing their cyber diplomacy, utilise the expertise of private agencies to avoid future recriminations when their policies fail. China failed to accept blame for actions directly pointing to state departments. The third is that the cyber diplomacy of less democratic nations is highly centralised and accountability is very difficult to obtain. China is one such case where the ruling elites control much of the cyber relations in the name of national security. The fourth is that nations are increasingly using cyber diplomacy in their quest for global dominance. Obama may have accused the Chinese in 2012 of

attacks on US defence programmes but the reverse is also true. No global hegemon can survive if it fails to obtain the classified developments within its closest rivals. Such a scenario drove the highly sophisticated spying networks between the USSR and the US during the Cold War which began in 1945 and ended in 1989 with the fall of the Berlin Wall. The fifth and final deduction is that nobody is safe from cyber attacks since the driving motives behind them are as disparate as the victims involved. Hostilities emerging from bad cyber diplomatic relations between two superpowers may, for instance, result in 'hot' war which can negatively affect even the remotest of global citizens.

According to Brenner (2010:90) in spite of the fact that 60% of cyber criminals are between the ages of 16 and 26 (according to a 2006 Australian survey), governments and other not state organisations have the potential to engage in cyber criminal activities. Such activities take the form of financial theft, espionage and other cross border crimes such as sabotage (also called cyber warfare and the International Criminal Court is attempting to create an international cyber law to try perpetrators) (Ibid). The US alone annually loses up to $100 billion because of cyber crime.

Crimes targeting computer networks and devices include malicious code (malware), computer viruses and denial of service attacks. Cyber networks are being used to advance phishing scams (attempts to obtain private personal details using legitimate looking electronic details for criminal purposes- Merriam Weber Dictionary), identity theft, information theft and cyber stalking. The sending of spam (unsolicited bulk mail) is unlawful in some areas. Fraud, which includes any dishonest misrepresentation, is prohibited under international cyber law. Bank fraud, extortion, theft of classified information and identity theft are a variety of internet scams used to target consumers (Telephone Computer Protection Act of the US, 1991).

The peddling of obscene and offensive content is prohibited in at least 25 US jurisdictions. This includes pornographic material, slanderous speech, politically subversive material, inflammatory, racist or prejudicial electronic communications. Harassment, drug trafficking and threats are also summarily prohibited (Brenner, 2010:91). According to Rothhacker (2012:11) governments and information technology specialists have documented a massive increase in "internet problems and servers since 2001." Cyber terrorists, intelligence services and other groups have demonstrated an increasing aptitude for intruding servers by mapping potential loopholes in critical security systems (Ibid). Cyber terrorists are coercing and intimidating governments,

organisations and individuals to advance their political and social objectives through computer based attacks.

The threats include market crashing threats such as internet propaganda that there will be a bomb at a specified location such as a holiday resort. In such a case the targeted government will have to issue a warning in advance against visiting the area thereby causes losses in tourism revenue. Another form of cyber terrorism is cyber extortion where "websites, e-mail servers or computer systems are subjected to continuous attacks taking the form of denial of service" (Ibid). Then the extortionists demand money in return for stopping such attacks. According to the US Federal Bureau of Investigation (FBI) at least 20 cases are reported to them each month (Ibid).

### 3.2 Documented Cases of Cyber Crime

According to Weitzer (2003:150) in 1983 a 19 year old UCLA student used his personal computer to hack into the Department of Defence international communications network. David (2012:10) states that Estonia's infrastructure was attacked by Russian hackers in 2007. This was a form of cyber warfare which includes attacks in cyberspace that have strategic significance. In a synergised kinetic and non-kinetic campaign against Georgia, Russia is also alleged to have attacked again in 2008 (Ibid). On 2 March 2010 Spanish investigators arrested three people for infecting over 13 million computers around the world.

Rodriguez (2012:1) states that in June 2012 LinkedIn and eHarmony were attacked exposing 65 million passwords of which over 30 000 were hacked and 1.5 million of eHarmony passwords posted online. In December 2012, Wells Fargo a US corporation, experienced denial of service attacks (Ibid). 24 million customer credit numbers and other private information of Zappos.com were compromised according to David (2012:2) South-western Bell suffered a $370 000 loss after Masters of Deception (MOD) attacked its subsidiaries, Pacific Bell and Nynex as well as universities, other telephone companies and large credit corporations (Ibid).

On April 23 2013 a Twitter account (Associated Press) was hacked releasing a hoax tweet that President Obama had been injured resulting in a 130 point drop in the Dow Jones Industrial Average (Ibid). As a result of the hoax, about $136 billion was removed from S & P 500 Index. These cases are admittedly just a minute percentage of cyber crimes taking place all over the

globe on a daily basis. This paper shall now discuss the impact of cyber diplomacy on cyber crime and vice versa.

### 3.3 Cyber Diplomacy and Cyber Crime

It would be overly presumptuous to assume at this juncture that cyber diplomacy facilitates cyber crime without full cognisance of the triggers inherent within the realm of cyber diplomacy which lead to the increased incidence of cyber crime. With this in mind, this paper shall discuss: (i) the effect of hegemony and influence, (ii) the rapidity of change in the cyber politics arena, (iii) the impact of ideology, and, (iv) the shifting geopolitical order in relation to cyber diplomacy and cyber crime.

#### 3.3.1 Hegemony and Influence

van Ham (2012:47) states that "the US invasion of Iraq and the March 2003 toppling of Saddam Hussein reinforced the view of US unilateralism driven by *realpolitik* and military supremacy." This also rekindled existing fears of Pax Americana (American Empire) (Ibid: 47) especially among nations such as Iraq and Afghanistan which detest US hegemonism and influence to the effect of titillating cyber terrorism against the US. Melissen (2005:7) states that "these nations accuse America of playing 'Globocop' and resist its global social engineering sometimes violently." The increase in 'rogue states' such as North Korea and Iran which are nuclearising for dubious reasons (according to right wing American sentiment) has been couple with cyber criminal activities even against the allies of global hegemons such as the US. The early 2013 cyber attacks on South Korea allegedly by North Korea are a case in point. US security barriers since 2002 have been elevated to withstand the counter-hegemonism posed by cyber terrorists (Ibid).

Moreover, 'empires' do not rely solely on military power or hard power thus they have constantly intensified cybercraft to suit the increasing exigencies of the new geopolitical order. Simes (2003:1) states that "empires rely on tools, policies and incentives to establish and maintain full-spectrum dominance." The law of inverse salience is such that in a realist sense a nation's aspirations are potential triggers of conflict with other nations. For example if Zimbabwe wishes to access covertly the electronic registry records of the United Kingdom (UK) for security reasons, acceptance of such an acquisition by the English authorities will not be

expected to be easily obtained. Resistance to such a move will be for similar but inversely opposed reasons.

Thus while the US seeks to successfully pursue a foreign policy of hegemonism in every conceivable dimension, the implied result is an equal opposition by offended parties (presumably those with similar policies). It can therefore be surmised that the 'roguish' foreign policy stances of Iran and the DPRK are simply a counter to US hegemonism. It can perhaps be concluded that counter-terrorism has the potential to stimulate greater terrorism. Actions countering cyber offences can help trigger more criminal activities of this nature. According to Beers (2003:1) the US has been on a course to defend its policies because the "millions of ordinary people around the globe have greatly twisted images of the US into negative, weird and hostile representations to the point of causing the creation of a young generation of anti-US terrorists." Such ideals according to US foreign policy makers must be neutralised if cyber crime rates are to be minimised (van Ham, 2012:49).

### 3.3.2 Dynamism of Cyber Diplomacy

Change in the field of cyber diplomacy has arguably been very rapid if not rabid; and correspondingly too, the transformation in intensity and extensity of cyber crime has been contagious at every level. Cyber criminals like cyber diplomats have had to keep up with change in order to remain relevant. van Ham (2012:50) states that "the modern international system is transforming from being anarchical to hierarchical with the US infirm control." How true this assertion is with regards to the growth of multipolarity with nations such as China and India being thrown into the mix becomes a salient argument.

There can be no doubt that multipolarity has diminished US full spectrum supremacy. However, the Cybercrime Prevention Act of 2012 (Republic Act number 10175) of the Philippines was drafted with the view of a hierarchically morphing international system in mind. Under the same Philippine legislature it was taken in consideration that criminal minds such as Onel de Guzman who created the ILOVEYOU worm could not be prosecuted under previous laws due to a deplorable lack of legal basis at the time of his arrest (Guelke, 2006:43). However that same provision had to be amended because of an outcry against its criminalising of libel which was perceived to be the ultimate curtailment of the freedom of expression (Ibid). This means

international cyber law has to be constantly altered to suit newer trends. Cyber crime is developing rapidly and so should cyber diplomacy.

The foregoing seems to suggest that a new 'race' between cyber crime and cyber politics has emerged simply driven by the uncertainties of future developmental trends of cyber technologies. At every point it will become imperative to redefine cyber crime and cyber politics in order to effectively encapsulate novel dynamics. Change has become a trigger with which international cyber law must contend by constantly transforming to cater for newer internet crime dimensions. This means that the rapidity of change itself impels a commensurately forceful negative reaction akin to the post-1945 Cold War.

### 3.3.3 Ideology

Ideology has been another push factor of cyber crime. Terrorists on fundamentalist religious missions have been known to perpetrate crimes to advance their beliefs. It can almost be guessed that the 1983 UCLA student hacking of US Department of Defence networks was driven by fundamentalism (Pew Global Attitudes Project). This assumption by no means overrules whim. It however should be noted that "influencing ideologies have shifted from being merely socialist or capitalist sentiments" according to Blake (1992: 58).

From an international economic relations perspective, Pijl (2006: 12) talks of "systemic and transnational rivalries." He goes on to state that "the process of speedy liberalisation, pushed by transnational capital causes great instabilities and the practise and development of privatisation and economic competition causes extreme precariousness and inequality." The current ideology seems to be one of more and more competition between and among groups of individuals/states seeking an edge over competitors through acquiring their confidential information using covert cyber means. Such underhand diplomatic practices, though decidedly nefarious and outright illegal at the extreme, have become common practise among mighty nations such as Japan, China, Russia and Singapore. Ideologies tied to ethnic, religious and moral grounds are themselves undergoing a facelift (Pijl Ibid: xi).

Pijl (2006: 12) goes on to cite the "deleterious effects of capitalist exploitation" stating that capitalism "exhausts society." This means that far from being enervated through pro-capitalism lobbying, counter-capitalism sentiments are rising in inverse salience to its hegemony. This

opposition has begun to show through cracks within the cyber politics framework manifesting as cyber crime. The rivalries latent in the geopolitical order are evolving "according to a particular historical scheme which entails, from the onset, the 'ultra-imperialist' moment in the form of a normatively unified West".

If France challenged the first British Empire; Germany, Italy and Japan fought the second British Empire and the US; the Soviet Union (USSR) contended against the wider West; and in the 1970's a coalition of Third World nations fought against the prevailing world system, then China is the chief ideological contender today. As can be expected thus, the level of cyber crime between the US and China is high. This means in a political economy sense, "the original 'West' offered capital accumulation a unique constellation of a transnational social sphere which is self-regulating and which became an 'internal extraterritoriality' within which it could grow" (Ibid). This "simultaneously expelled societies on the periphery into a defensive posture." The same 'contender position' exists manifesting as cyber crime among its multiple dimensions. This has become a threat to the world system envisaged rather despairingly by the likes of Wallerstein, Amin and Gunder-Frank.

### 3.3.4 The Geopolitical Order

The world order has been Hobbesian from the onset. Pijl (2006: 7) says that realism has found root in modernity because there is "a revolutionary ideology backing every foreign policy goal, concentric development and a host of foreign policies backing up claims of sovereign equality using powerful armies. Revolutionary ideologies have become propaganda in mainstream states which has facilitated the development of an 'opposition sector' comprising cyber criminals. It seems relatively easy to rouse active anti-western sentiment in a culture of right wing religious fundamentalism. Concentric global development has to date wrought a global 'core-periphery duality' according to Wallerstein and other system theorists. The immiseration of the global pauper, the Third World by capitalist systems has drawn anti-western sentiment leading in part to the precariousness posed by threats such as cyber terrorism. Even within the West itself, opposition has grown. How else would Snowden 'whistle blow' against his own nationality?

The Second World War was premised largely on the principle of sovereign equality. Powerful armies supported this un-provable dictum leading to war. The same feelings drove the almost 50-year Cold War. At present, the irredentist Middle East conflicts since 1948 have thrived on

sovereign equality rather than sovereign mutualism. This means if advantages are to be obtained and maintained in a modern Hobbesian system, modern methods must be employed (Ibid: 25). Yet the principles of sovereign equality and globalisation are increasingly becoming more difficult to reconcile. According to Kaarbo and Ray (2005: 97) "for about 300 years the pre-eminence of the state as the most important political organisation went unchallenged until recently in the wake of globalisation."

Globalisation negatively affected sovereignty by making borders more porous and states more liable to international scrutiny. Coupled with this, as stated in the previous section, globalisation also drew into international politics a whole host of actors who are riding on technology trends. Thus cyber diplomacy and cyber criminal activities have become inextricably enmeshed and this propensity is envisaged to perpetuate into the future. Guelke (2006: 12) notes that "the ending of bipolarity has led to the creation of opportunities to shape the world according to new principles."

The longstanding 'Globocop' stance of the US is facing daily onslaught. Networks of Islamic terrorists for instance have emerged to bring about change at the global level. This means that where the ideological predisposition of a hegemon is diametrically opposed to the fundamentalist ideals of small groups, then the national and international security of the power is thrown into a precarious state. Guelke (Ibid: 12) cites Huntington's appeal that "the ideological conflicts of the past are being overtaken and replaced by a clash of civilisations thus setting the basis of a global jihad against the West. What is horrifying about this jihad is its embrasure of the entire range of society. Globalisation increasingly makes everybody an affected party. Radicals have been encouraged to develop strategies which are global in both ambitions and theatre of conflict.

### 3.4 Conclusion

Cyber crime is compelled by the triggers inherent in cyber diplomacy. While the four premises discussed may not be exhaustive explanations for cyber crime, they form a broad basis on which to establish the contestation that cyber diplomacy and cyber crime go together. What perhaps has not received due attention is the fact that cyber crime itself can compel cyber diplomacy. For instance concerned international parties can bloc up to counter cyber threats in a more holistic manner thereby stimulating greater cyber diplomatic cooperation. At present such insinuations are situational and complementary. It is hoped that current trends will result in more

transformative gestures of cooperation between and among states which are more concrete. The idea is to envisage a united cyber diplomatic transnational protocol whose aims are embellished along a similar grain to Interpol (International Police) which is fighting international crime collectively. Yet one man's terrorist is another man's liberator. Snowden has been touted numerous titles- from 'leaker' to 'whistleblower' to 'spy.' It may be then that international cyber laws will have to embrace elaboration on such contentious transactions to curtail confusion.

The above notwithstanding, hegemonism, change, globalisation and ideology are some of the dialectics stimulating cyber crime simultaneously with cyber politics. Here sophistication has become prodigal to simplicity. A multiplicity of either philanthropic and or nefarious actors have been thrown into the blend leading to the constant need to redefine the relationship between the legal and the illegitimate aspects of cyber politics. It becomes easy to envision a duality- a dichotomy of dissonant motives within cyber politics. On one hand there are attempts to facilitate international concord and on the other, there are increasingly successful attempts at beguiling a certain kind of global order for particular purposes.

Terrorists and crime are hardly understood especially where their motives are not actuated through mutual dialogue and consensus but through an innocuous set of abstruse actions. In that case they are likely to be seen in an ambivalent light. This is when counter-cyber crime fighters appear to add more insult to injury and the cycle continues. Obviously somebody is benefiting from the latent confusion in the global order. To illustrate this dilemma a question can be posed. What motivated Snowden to 'sell-out'? Unless this posse receives a proper answer, there can be no reasonable presentiment that his inclination for what have been seen as 'subversive' actions by US departments can be thwarted. This entails a need to comprehend the criminal idiosyncrasy rather than incessantly barraging its environment with the tried, tested and failed J.W Bush 'cowboy mentality.' The bleak reality, however, is that cyber crime is here to stay because as long as there are `computers, networks and software, criminal motives are easy to channel against the existing global disorder. There can be no ultimate warrior against cyber crime. Rather international anti-cyber crime networks can be established to counter and foresee its extremes.

## CHAPTER FOUR:

## CYBER DIPLOMACY AND CYBER CRIME TRENDS

### 4.0 Introduction

Cyber crime and cyber diplomacy are becoming increasingly complicated and interconnected. This is because of rapid technical advances for instance the miniaturising of technical devices which has enabled cyber criminals to operate with less fear of detection. Gordon and Ford (2013: 3) argue that the issue is problematic in the sense that there is the confusion of trying to implement vertical solutions to what is essentially a horizontal problem. Cyber crime has become a global market problem. At each level there are numerous opportunities for the criminal to perpetrate a harmful crime. An example would be the creation of computer viruses and malware such as Stuxnet which occurs at various sources of cyber tools. This means cyber crime has a chain of possibilities.

The perpetrator can be a group of individual targeting Sri Lanka or London using kidnapping or harassment, targeting government or private officials, with actual or claimed affiliation and motivated by a perceived need for economic or political change. Cyber crime has become more complex in that location is not physically delimited thus an act can be "virtual/virtual, virtual/real or even real world/virtual" (Gordon and Ford, Ibid: 6). This means that the entire criminal activity can take place in virtual reality and vice versa and it can be a virtual attack on the real world for instance the 2013 North-South Korea attack on transport and exchange systems. Or it can be a real-world-attack on the virtual for example the 2001 bombings on the Pentagon which damaged computers and virtual information systems.

The foregoing means that cyber diplomacy has had to change in order to suit cyber crime trends otherwise stagnation could cause serious problems for the international community. What has emerged is a new 'arms race' between cyber diplomacy and crime whose future remains uncertain. What will future cyber terrorism look like? Will it be based on automation or robots in some instances? Computers are becoming more sophisticated and perhaps they may be developed to the point of attaining their own 'individuality' or consciousness. Movies such as I-Robot come to mind when this possibility is brought up. Yet does this mean that the future cyber crime could at times be waged by robots against mankind? Such is a daring prospect and a very

uncomfortable one. It appears then that measures must be put in place to counteract negative future possibilities and safeguard global security. The above questions therefore deserve prudent attention and this section shall hitherto attempt to give recommendations based on the findings of this research.

A focus on future prospects brings to light the new concept of "pure cyber-terrorism" (Ibid: 8). Pure cyber-terrorism is activities done entirely in the virtual world. This means that as the virtual world becomes more complex, virtual crime is expected to follow suit. Coupled with this, there could be changes in the perpetrator, place, action, tools, targets and affiliation. For example where the manpower of criminals had to be great to suffice, technical advances would reduce the need for numbers. The virtual place could become less cordoned off to other interfaces. Actions could become less violent but with much more violent results.

In this age suicide bombers have been witnessed for their sheer self-sacrifice. Yet what would be the new terrorism when terrorists (cyber criminals) have apprehended the technology for drone warfare? Tools could therefore shift from being merely computers to robots. Targets could become more global in extent. Affinities or affiliations of criminal groups could become more transcontinental. This means that the response to cyber crime has to suit these emerging and transforming trends. Criminals will certainly continue to fight for control. Motives are therefore expected to persist into the future because of the dynamism of the world system. With this brief background in mind this discussion shall now focus on current findings before discussing the possible future prospects of cyber diplomacy and cyber crime and giving concluding remarks.

### 4.1 Findings

If recommendations are to be given beyond this point, it is paramount to chart the current scenario and make suggestions on what the future may be. Therefore this section will detail all the findings gathered from content analysis and personal surveys. Infographic (2013) states that cyber crime is a growing trend such that by 2017 the cyber crime security market will shoot to over US$120 billion. Currently the cost of global cyber crime worldwide is around US$100 billion. This means that governments worldwide should invest more in combating cyber crime and where investiture is to be increased in this regard there would inevitably be social costs in the form of reduced government expenditure in health and education. To some extent, government expenditure in combating cyber crime would result in the militarising of the globe

thereby turning into 'police geopolitical system.' This is because to combat cyber crimes of the magnitude of 556 million victims annually or 1.5 million victims per day or roughly 18 victims per second (Ibid), governments would have to be more intrusive than ever before. Around 600000 Facebook accounts are compromised daily. Nationals everywhere are vulnerable because the proliferation of social networks has exposed diverse nationals worldwide. The internet has become a virtual pathway for miscreants to access the private information of individuals. Cyber criminals are using many techniques to attack. Even governments are not secure. For instance, despite the fact that US government computer systems are 'air-gapped' for protection, inside operators like Snowden are still able to access classified information and release it to the world. This means counter-cyber crime measures should encapsulate all these possibilities. There must be an implementation of internal vetting mechanisms to prevent an escalation of 'internal' cyber criminal activities. Below is a table detailing the percentages of various cyber criminal attacks.

| **ATTACK TYPES** | **PERCENTAGE** |
|---|---|
| Viruses, malware, worms, Trojans | 50 |
| Criminal insider | 33 |
| Theft of data-bearing devices | 28 |
| SQL injection | 28 |
| Phishing | 22 |
| Web-based attacks | 17 |
| Social engineering | 17 |
| Other | 11 |

Source: *Infographics* (May, 2013) Available at www.infographics.org [Accessed 17 January 2014]

It is a curious fact that men are more vulnerable (at 71%) to cyber attacks than women (at 63%) (Ibid). This is probably because of the different access rates between men and women. This statistic is also telling in an indirect way in the sense that the more people access computer systems is the greater their vulnerability to cyber attacks. At the onset of this analysis this fact was stated to explain why cyber crime is on a constant increase since the inception of the web and software. The internet has increasingly become the path of least resistance for criminally-minded people wishing to even scores illegally. Computer use is proliferating worldwide and networks are becoming more intricate in linking publics and individuals for benefit and for

detriment and as such measures should be implemented to cater for the unforeseen. It therefore seems expedient for governments to form holistic cooperative arrangement to deal with all exigencies in the present and near future.

In China in 2013, medical/healthcare experienced 39.8% cyber criminal attacks with a corresponding 35.1% for businesses, 10.7% for education, 3.9% for government/military and 5.3% for the banking/credit/financial sector (Infographics, 2013). Around 59% admitted to stealing company data in 2012 China (Ibid). Infographics (2013) the main motivating factor for such activities has been 40% cyber crime and 50% hactivism (the use of computers and networks for political purposes), 3% cyber warfare and 7% cyber espionage. These statistics prove that governments are less vulnerable than the private sector and individuals to cyber crime.

However, when governments are attacked pose greater security risks. Hacktivism can take on the form of terrorism for instance especially when it is driven by a fundamentalist religious mission incompatible with the extension of a certain government policy. As stated previously in chapter one, terrorists would love to control, even for a moment, the defence systems of powerful nations such as the US, Russia and China. There can be no telling how far terrorists can go in causing an Armageddon. It is therefore vital to outline the chief sources of cyber crime activity by country so that global priorities can be focused in that regard. Below is a table presenting the top 15 countries by rank as of February 2013 in terms of the number of cyber attacks and therefore the level of vulnerability.

| **SOURCE OF ATTACK** | **NUMBER OF ATTACKS** |
|---|---|
| Russia | 2 402 722 |
| Taiwan | 907 102 |
| Germany | 780 425 |
| Ukraine | 566 531 |
| Hungary | 367 966 |
| USA | 355 341 |
| Romania | 350 948 |
| Brazil | 337 977 |
| Italy | 288 607 |
| Australia | 255 177 |

| | |
|---|---|
| Argentina | 185 720 |
| China | 168 146 |
| Poland | 162 235 |
| Israel | 143 943 |
| Japan | 133 908 |

SOURCE: *Infographics* (February 2013) Available at www.infographics.org [Accessed 17 January 2014]

The information above presents very interesting facts. It would be expected that countries with the means such as the USA and Japan would feature higher on the log but this is not the case. Why Russia would be the largest source of attacks is unclear given that it is a relatively isolated territory without as many global escapades as the USA. China also ranks very low despite it being the most populous nation coupled with the fact that it presents as a technical polity. However, there are some underlying trends which could partly explain these questions. According to Infographics (2013), in terms of malware attacks, the USA and Russia are the largest contributors making up 39.4% and 19.7% of attacks respectively. The USA navy alone experiences over 110 000 cyber attacks hourly or about 30 per second meaning that these nations should be the chief points of focus in combating cyber crime.

### 4.2 Analysis of Present Cyber Crime Trends

Denning (2004: 10) states that the threat of cyber crime has been overrated because no single instance of cyber terrorism has been recorded and only minor incidences of cyber crime happen each day. He goes on to argue that US intelligence systems are "air-gapped" and are thus separate from the internet. Yet what he fails to take into consideration is the fact that threats do not necessarily always have to come from outside the system. There have been numerous attacks from within the latest being the Snowden incident. This means that the system is not foolproof against threats which can ultimately bring it down. Moreover, he is merely talking about the United States. How far are other nations as 'safe' as the US? The fact that private companies are more vulnerable to cyber attacks does not suffice it to say that similar threats cannot be extended into the future because given the overwhelming evidence of cyber attacks at an individual and organisational level, this view seems complacent. The threat of cyber crime is constant and cyber terrorism is an ever-present possibility which every nation must strongly guard against. The 2013

attacks on South Korea bear testimony of this. Air-gapping does not prevent internal threats and there is every possibility that an attack can happen from *within.* Nobody can safely say that the information technology interfaces of public intranets will never be breached using newer and more sophisticated software. Verton (2010: 42) goes as far as saying that the September 2001 attacks in the US were actually cyber terror attacks since no coordinated attack of such calibre can succeed without the use of computer information systems

Denning (2004: 11) states that the majority of criminal offences are perpetrated by groups or individuals with nil or few political aspirations or the desire to cause mayhem only terrorists can dream of. Therefore according to him cyber attacks are a minor threat. But given the figures indicating the rate of attack on government installations worldwide, this belief seems flawed. If one is to consider the numerous illegal organisations with political motives (La Cosa Nostra, Janjaweed militia, Boko Haram, Al Shabbab, al Qaeda, Mujahedeen) then it is not inconceivable to see the possible threat such organisations can perpetrate using computer technology to meet their objectives. The few 'hackers' who have been documented have simply been 'minor' in the sense of the size of their crimes. Major attacks remain a constant possibility and governments and private society cannot afford to be complacent to this reality. The only guarantee is that there is no guarantee from cyber threats.

### 4.3 The Future of Cyber Crime

Denning (2004: 12) states that "cyber terrorism and cyber attacks are sexy right now...cyber terrorism is novel, original...it (cyber terrorism) captures people's imagination." He gives this as the chief reason why cyber crime has been overrated. But if cyber crime threats are novel and original then who is to guess how far they can go? The very fact that such crimes have become more and more prominent is a threat to human security which must be promptly tackled. If terrorists could obtain the means to meet their ends then mayhem is a possibility. Developed nations at the moment fear the nuclearisation of smaller states not aligned to their objectives of global domination. Nuclear weapons cannot be operated without computer technology thereby making their user, if they are a terrorist, a cyber threat. Such a reality will certainly capture people's imagination. If the other reason for complacency is the failure by the media to distinguish between hacking and cyber terrorism coupled with an exaggeration of the latter based on false analogies (such as that if a 16 year old can do it, what can a well-funded terrorist group

do?), then the media has become supranational. The very fact that a 16 year old can do it is ample reason to worry that cyber crime is a fact to reckon with because it transcends normal capacities at a certain point.

The foregoing means also means that current systems are not secure enough to assure international peace of mind. And if according to Green (2003: 1) ignorance is another reason for the almost irrational fear of cyber crime since there is a convergence of two spheres -crime and technology- that many administrations do not fully comprehend, this very standpoint is presumptuous and fallacious. Technocrats are employed on merit. Moreover, such supporting agencies as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency in the US or Scotland Yard in the United Kingdom are littered with very highly qualified computer experts. Therefore the ignorance would rather be of what exactly the criminal mind capable of and when it wishes to perpetrate a misnomer.

Denning (2004: 11) states that the fear of cyber crime has been caused by politicians who seek to advance their own political ends and that for most people the real meaning of cyber crime is abstruse and vague. While the former reason contains some truth, the latter is presumptuous. The vast majority of people everywhere understand that computers can be used to cause them harm. It is difficult for politicians to merely threaten and act like ‘prophets of doom’ without tangible reference to existing scenarios. Exaggerations and lies are possible with politicians but this does not mean a level of truth is impossible. The foregoing aptly describes the current confusion surrounding cyber crime but what are the possible future prospects?

It can be envisaged that the future will drag with it the current confusion. In the course of rapid technological advancement even more confusion is to be expected. Perhaps a major cyber attack will amalgamate global interests and therefore global cooperation and coordination of anti-cyber crime efforts. This means that transnational networks may be embellished to this end. It is also expected that as technology advances, cyber crime will also advance. The majority of computer crimes taking place today would have been inconceivable 50 years ago. Public and private spheres are likely to become more vulnerable to attack. There is likely going to be public outcry in many nations clamouring for the implementation of security systems to protect citizen interests against the threat of cyber crime. This would certainly push governments into increasing public expenditure on cyber security systems and feedback information systems thus enhancing anti-cyber crime technology. However, this can also negatively impact on citizen privacy. A case

from which this assertion finds support is the post-9/11 scenario where US and foreign citizens in America were subjected to new forms of biometric technology security systems. A possible outcry against this could force governments to use alternative systems. A situation where people will be implanted with tracker microchips is no longer a pipedream. This is because of the changing nature of cyber crime.

Frank Cillufo of the Office of homeland security in the US remarked that "while bin Laden may have his finger on the trigger, his grandchildren may have their fingers on the computer mouse." Such is the dire scenario of the future. Cyber crime will eventually replace overt force meaning that counter defences will have to become more technical. For instance computer-controlled satellites and drones will be used more and more in locating and neutralising hidden terrorist bases. But terrorists and cyber criminals might also soon have the ability to hack into national computer systems and turn drones, laser beams and robots against their creators.

### 4.4 Conclusion

There is an indisputable nexus between cyber diplomacy and cyber crime judging from the trends presented above. As it stands, policymakers worldwide should come up with strategies of reducing or eliminating this connection since it is very costly globally with nations such as the US running bills in the order of close to $120 billion annually in an attempt to ensure national security. Cyber crime has also made nations billions of dollars however, with large corporations such as Microsoft coming up with antivirus software to protect computer systems. This could mean that those who must take action might not be willing to incur the opportunity costs of eliminating crime in the short run. However, it is the view of this paper that policymakers also stand to gain by studying the criminal mind. They should ask the why behind criminal behaviour. This means working in lieu with anti-crime agencies and psychologists to discover this. It seems for example that the terrorist mind, while seemingly irrational to many worldwide actually has certain motivations which can be eliminated if some sort of compromises can be reached. This means there is need to dialogue with criminals at some level and come up with solutions. The warnings of much greater disaster in the future should never go unheeded and rubberstamped using the current piecemeal 'solutions.' Something must be done fast to curb the growing threat of cyber crime.

# CHAPTER FIVE:

# CONCLUSION AND RECOMMENDATIONS

## 5.0 Conclusion

Cyber diplomacy, like cyber crime is there to stay. Globalisation has brought nations closer together in a multiplicity of issues ranging from the environment to terrorism or from socio-economic issues such as gender advocacy, poverty, HIV/AIDS and migration to geopolitical ones such as nuclearisation and the polarity of states. Globalisation has therefore transformed diplomacy making it more intricate and sophisticated technologically and operationally. The crux of the matter has been the corresponding increase of cyber crime in tandem with the increasing complexity of cyber diplomacy. Cyber criminals have had to either intensify the rapidity of their attacks, their level of complexity, and their range in order to be successful. This has conversely increased the complexity of counter-crime responses by state and civil authorities resulting in some kind of information 'arms race.' As the range of issues dealt with by cyber diplomats has increased due to globalisation, so have the threats that come with it. Interstate cooperation or communication ha exposed more and more vulnerabilities not only between states themselves but also between private and public corporate machinery.

Of importance is the fact that cyber crime cannot be confined in nature, time and place. A hacker in Nigeria can illegally access files of a British denizen via the internet. This idea that cyber criminals can attack anywhere anyhow is not palatable with global security agencies; and the notion that individual citizens are at risk any time has reduced the amount of confidence vested in the traditional state. Globalisation has led to a gradual 'carpet-rolling' of state borders and on its back it has borne the tide of cyber crime and cyber diplomacy. As a consequence, cyber crime has become one among many reasons which have diminished confidence in state supremacy. States have been compelled by reality to swallow their pride and assign some of their sovereign security functions to private agencies. This is because admittedly, the multifaceted nature of cyber crime is beyond the ambit of any one state or centralised agency to tackle exclusively. It is thus no doubt reasonable for states to actively decentralise their collective counter-cyber crime machinery while at the same time enhancing intergovernmental cooperation at state and private level. This recommendation will be discussed in greater detail in the course of this chapter. At

the moment however, the hostile and cunning relationship between cyber diplomacy and cyber crime merits deeper analysis.

Cyber criminals are human. Cyber criminals use private and state machinery or systems. Their targets can be anything or anywhere and their motives are unlimited. This means that the universal nature of the perpetrators themselves makes it near-impossible to define cyber criminals. And where there is no comprehensive definition means a comprehensive response becomes less certain. It has been argued in this discussion that perhaps the lack of an understanding of the criminal motives of cyber offenders has actually facilitated the perpetuating of cyber crimes. An example is the September 2001 attacks on the US by al Qaeda which in spite of concerted, vengeful responses by the Bush administration, failed to prevent the Bali bombings a few years later. A punctuation of this fact is the hitched-up security at entry points into the US since 2001. The increasing use of biometric technology by major powers is rather a response in paranoia than perficience. This has caused unprecedented attacks on counter-attacks and increasing measures of tightened security systems which has further reduced citizen privacy and confidentiality.

The foregoing implies that there can be no telling to what extent the nature and intensity of cyber crime will go. Will the concept of a 'receding state' be inversely salient to the perpetrations of cyber criminals; or in other words will a less visible state diminish the hatred international cyber criminals usually have against states? It has been agreed in numerous circles that globalisation has the twin effects of enhancing state porosity and causing the recession of state influence. However, one could argue that globalisation has only increased state porosity but has not diminished state influence because states are engaging in a multiplicity of novel dimensions. Such porosity means that global and domestic security systems will constantly face threats from unprecedented angles. In this regard, globalisation can be said to be driving cyber diplomacy and inadvertently facilitating cyber crime. This is true in the case of cyber crime in the sense that globalisation is inexorably opening up the doorways and channels of interstate and intra-organisational cooperation by remodelling and relaxing traditional border interfaces.

If cyber criminals can attack anywhere and at any time does it then follow that they can cause any kind of mayhem? For example can they cause wars between nations? As stated above, if cyber criminals cannot be defined accurately simply because they can do anything then the democratic peace theory propounded by Francis Fukuyama about mature and stable democracies

never going to war fails to become an absolute. If cyber terrorists were for example going to covertly manipulate the nuclear weapons systems of France against England and a nuclear attack were to occur, is it not plausible to expect an irrational response from the latter? This is just a presumption but it is a possibility. This assumption may at the moment seem improper if not impossible simply because there is no existing model on which to base it directly. The destruction of nuclear weapons systems in a nation such as India will certainly cause problems for surrounding nations and citizens. Radiation from the explosive package could cause international mayhem especially where there are existing tensions as between India and Pakistan.

The Taliban was unseated in Afghanistan as a direct result of the al Qaeda attacks on the US hinterland. Saddam faced demise when 9/11happened meaning that cyber attacks can be engineered to have permanent ripple effects. So who is to say that clever cyber criminals cannot cause effects originally unintended by ultimate responders to an attack such as war between 'mature and stable democracies?'If this possibility stands then the world is a very unsafe place indeed. In a realist sense, cyber crimes are escalating towards a final endpoint, a conclusive denouement so to speak which should offset a global Armageddon. Cyber crime is akin to a virus aimed at the heart o a living system and whose end is incurable infestation manifesting in collapse and death. Yet that possibility exists only unless governments and private agencies cooperate and counteract the spread of cyber crime in all its forms.

Another possibility is a global attack using malicious software (malware) capable of bypassing air-gapping systems. This could be used to cause disorder of any kind such as war and sour relations. When South Korea was attacked by cyber criminals in 2013 it never became clear who the attacker was or what their motives were even though allegations and suspicions were levelled against the DPRK. So even if the attack was perpetrated by private saboteurs the effects it caused were akin to those of an official attack. Viruses, worms and Trojan horses are constantly being advanced and the US has emerged as the chief culprit. It remains reasonable to envisage a scenario of malware, powerful and subtle enough to cause a stalling or malfunction of national security and information systems. Existing systems can be hacked and infested leading to problems or the information they contain may be misused or exposed by insiders or outsiders.

The foregoing seems to be a jumble of presumptions and assumptions but their possibility stands. This discussion has been poised at shattering existing false screens of complacency. Nations need to be aware of existing threats to global, national and individual security and act

accordingly. Cyber criminals, especially those on a religious mission incompatible with the extension of the security of certain nations, are working tirelessly to bring down the existing orders of the nations they find unpalatable. This means blacklisted nations should respond through actions and interrogation of the reasons behind their precarious security. It appears from research that so much of cyber crime is motivated against individuals for selfish criminal reasons which are not usually of a political nature. However, anti-state attacks are more serious and widespread despite their lower incidence. The next section will discuss the possible recommendations for governments and individuals in greater detail.

Nations and individual organisations or people should be aware that cyber crime can affect anybody directly or indirectly. If the motives are purely personal and apolitical and insinuated without due cause then anybody is vulnerable. The effect can be felt everywhere for instance where banking and communication systems are disturbed. It means individuals indirectly connected to the attack may find it difficult to access their funds or information. The heightened security response scenario in the US is an apt case in point which affected both domestic and international citizens who were indirectly connected to the 2001 attacks. Snowden's leak obviously affected other government employees in terms of accreditation, security demands and access to personal information.

It appears that the only limitation to cyber crime in the form of cyber terrorism seems to be is caused more that a dearth in craft capacity and craft competency. The major limitation is pecuniary even though terrorists are sometimes very highly sophisticated in their understanding of technology since some of them are reputedly connected to government departments. This is not to say that some terrorist organisations such as al Qaeda do not have the financial means to perpetrate the more heinous crimes. What crimes can be perpetrated? Terrorists can hack into US drone systems and perpetrate attacks on areas of their choice. Weapons systems can also be hacked and the weapons activated against a target of their choice.

If the cyber crime motives are political, then it is conceivable that their effects can transcend socio-political and economic dimensions. Political motives behind cyber crime therefore affect anyone. Governments therefore need to act in order to protect everyone either from outright military attacks or from the more subtle attacks on individual information integrity. This means that given the extensity and seriousness of politically-driven cyber attacks on governments and nationals, a political, social and economic response is a grave necessity. Yet governments and

national citizens cannot respond to cyber attacks and threats alone since there is basically need for intelligence from everywhere. This means all information is vital before comprehensive and effective actions can be undertaken. With sufficient information even UN mandates are easy to obtain and the counteracting response can be undertaken more legitimately otherwise accusations will be thrown around even if cyber crime has been effectively thwarted. The US and its 'coalition of the willing' have been accused of irrationality and unilateralism in their trigger-happiness after the military debacles in Afghanistan, Iraq and Libya even though the last case was not attached to counter-terrorism.

Coupled with the necessity of legal sanction is the need to work within coalitions in order to place limits on extremes which are more likely when a single offended party acts alone thereby taking the law into their own hands. Coalitions minimise the risk of abuse of state power. Even individual organisations and citizens should be thus constrained otherwise the same abuse would become difficult to contain. Nations and individuals should work within the ambit of international law receiving the full sanction of bodies such as the UN and the ICC. An understanding of the criminal mind is a prerequisite. Its importance shall be discussed in greater detail in the next section since it can act as a plug to future criminal motivations. For instance if cyber criminals are attacking national information systems because of a grievous domestic law against their citizens, then perhaps for the sake of peace within reason, a compromise can be reached. Fundamentalist Islamic cyber criminals have been known to attack churches protesting against laws which they feel impede their freedom of worship. If amendments to those laws are within acceptable limits then perhaps they should be instituted to curb continued instability and hostile criminal actions.

A final scenario could be about the rather controversial perception of the 'leaker.' Certain leakers are not always criminals. Some do it for philanthropic reasons meaning that one man's leaker can be another man's hero. It is no wonder Snowden is being accepted in Russia. Leakers can actually be called 'whistleblowers' because in such cases they would be trying to expose the criminality within the systems within which they work. Snowden is one such case. The stealing of global telephone and metadata by the US government is a crime of espionage under international law. So does this mean leakers should be awarded asylum in certain jurisdictions to protect their person against vindictive state power? Such issues have not found sufficient

international redress because those who are most able to make such decisions are not willing to be bound by their own rules in future.

### 5.1 Recommendations

Given the forgoing hubris, it is expedient to proffer recommendations which will work as guidelines for policymakers in governments and private organisations and also for individuals. Forbes (2014) give means and ways of preventing cyber crime at an individual and corporate level and these methods can also be adopted by governments. The first method they cite is prevention, education and training of employees to protect computer systems. Employees must be taught how to protect themselves and the people they work for against cyber criminals and the organisation in which they operate must clearly define its security policies and priorities.

The Forbes Group (2014) state that employees must be made to understand the common hacking methods, such as phishing, social engineering and packet sniffing among many more. Securing computers, networking and digital assets must be a top priority item for all organisations. All software housed within a business network should be up to date. All office workstations and servers should have up to date business-class antivirus software installed. This is in order to protect computers by detecting and removing malware. This means not only network servers should be continuously scanned for malware but also website servers since these are also susceptible to malware. Critical data should be constantly backed up because it is vital for system recovery after an attack and not backing up data is a significant liability. Business networks must be able to handle network-specific attacks because certain attacks are targeted at overall network infrastructure. When it comes to cyber crime information is power. Unsolicited access to personal information is what gives hackers the power to tap into accounts and steal money or people's identities. However, having the correct knowledge can also help empower and protect individuals and organisations from cyber crime.

Not only cyber criminals can gain power from right information. Individuals and organisations need to continue educating themselves on the types of scams found on the Internet and how to avoid and safeguard against them which is a means of putting one's security a step ahead of the cyber criminals (Ibid). Phishing is prevalent which means that security systems must constantly be upgraded on the newest scams and learn how to recognize and counteract a phishing attempt.

Personal and organisational information must be protected through multiple tier security systems to withstand breaches and where people are well informed they are more likely to recognise a phishing attempt.

The use of firewalls is of paramount importance since they monitor information traffic between personal computers or network systems and the information streams on the Internet (Ibid). This means that they serve as first lines of defence which help to keep intruders out. It is however very important to use the firewall that comes attached to computer security software. Home wireless networks should be protected by enabling the firewall that comes with the router. Coupled with the above it is vital to 'click with caution' especially when checking chatting on instant messenger or checking email. One should be very careful not to click on any links in messages from people one does not know. Such links could take users to fake websites that ask for private information such as user names and passwords or it could actuate malware downloads onto your computer. Caution is vital even if the message is from a known source because some viruses morph and spread through email which means it is always paramount to look for legitimating factors that prove the safety of the information.

When surfing the Internet individuals and organisations need to take serious precautions to avoid dodgy websites that normally ask for personal information coupled to that they must realise that such pages usually contain malware. The use of a search engine will help surfers navigate to correct web addresses since they are always configured correct misspellings in all websites. Phony websites are those similar to the real sites and are created through a process called "typo squatting" (Ibid). Surfers may also want to use products such McAfee or SiteAdvisor software when navigating. SiteAdvisor for example is software that is configured to tell a surfer if a site is safe before they click on it.

Software must be constantly updated because hackers and other cyber criminals globally have a wide range of ways to access computer systems which means there is a need for comprehensive security software that can protect computer systems. Software such as SecurityCenter can help protect users from phishing, malware, spyware, and other new threats. Users should ensure automatic security software update by using the automatic update function on computer security control panels (Ibid). Regular computer and system scans should be promoted. Latest security

patches should be used to update operating systems (OS) and browsers. In Microsoft Windows systems the automatic update function can be used.

The US government has instituted a system of 'air-gapping' its computer networks. This is to prevent unsolicited outside intrusion and theft of classified state information. Yet more can and should be done to safeguard *internally* against leaks. Snowden was able to leak information for better or for worse simply because of the weaknesses inherent within the US security systems. Employee accreditation must be performed at deeper levels and information fragmentation and coding should be done with greater care to prevent leaks. If employees do not receive proper accreditation then government systems face not only the risk of leaks but also that of having their systems 'infected' from *within* something which could be equally detrimental to their operations. An interesting instance of information security is the often-cited Coca Cola case where only two employees, who do not know each other, know half each the recipe formula for the production of the soft drink and are not allowed to travel together in the same plane. Data should be fragmented and coded beyond normal classification methods and one part should never make any sense without the other parts.

It is also recommended that organisations and individuals understand the motivations behind the criminal mind. Are criminals attacking them simply because they can or are there real, solicited causes which are pushing criminals to do so? What are the results of vulnerability? For example will the criminals use the information they access for malicious reasons alone or for the benefit of people affected by the system. An understanding of this could in fact go a very long way in assisting policy-makers in dealing with criminals such as terrorists. What really does the terrorist want? Can it be given to them or can compromises be reached to settle the dispute? It seems like the powerful nations such as the US have not fully answered these questions in their quest to stamp out terrorism. Terrorists and cyber criminals may not be so irrational after all meaning that for other people, one man's cyber criminal may be another man's hero and liberator.

### 5.2 Implications for Future Research

It is hoped that this research has broadened the vista for future research by stimulating intellectual inquiry in a novel way. Admittedly no single research, no matter how enterprising, can cover all possible grounds meaning that there is need for even more research in other

dimensions of cyber politics. Cyber crime and cyber diplomacy are both futuristic and it is expected that the nexus between the two will shape-shift far into the future. There is therefore need to constantly explore newer and more probing hypothetical conjectures in order to broaden the present understanding of the multifaceted cyber world. This research is therefore not exhaustive since the field of cyber politics is novel and dynamic but it is hoped that this study will be a stepping stone of sorts into a more comprehensive understanding of future trends given the current available information.

The available information is very limited and much more must be done in order to add on to it. This can only be done through basing research on existing findings. It is the opinion of this paper that cyber diplomacy is an emerging discipline whose mainstay at the moment is a disparate jumble of information from other fields. Therefore this study has been undertaken to coalesce some the disparate entities of cyber politics in order to help the field of anything 'cyber' to begin to take comprehensible form. The importance of cyber politics is of global proportions and this study is expected to be a useful reference point in the near future because of the analysis it has made of existing trends. Cyber crime is arguably one of the chief threats to global security such that careful and meticulous studies of it will become a prerequisite in the larger field of international peace and security. This paper therefore is hoped to become one among an increasing number of related works being penned to describe this new and dynamic field.

Underlying this study has been the issue of self-actuating computer systems which can actually begin to fight against their creators. While this has been largely inspired conjecture, the future certainly holds in store such technical advances as have not been dreamt of. This means the reality of 'I-robots' can only be verified by time and current trends at the moment, but with drone and robot technology already in the picture, these trends seem to point towards this possibility. It therefore remains for future research to delve deeper into the exact nature of cyber diplomacy and cyber crime. Are we heading for a computer-controlled future where man almost loses agency to machines and software? Are we heading towards a reality of mechanical masters who are going to feed and manage entire societies? If that is a possibility, what then would be the nature of cyber diplomacy and cyber crime?

At the there can be no knowing whether a machine-governed globe will be more unified than at present. Yet such are the prospects of a new world order. What is certain is the fact that diplomacy will continue to be scaled down, to be decentralised and surrendered to more and

more private individuals and information can be more fluidly accessed as illustrated by the Snowden leak which was made possible as a result of existing structures for information exchange. This is because the US departments responsible for unauthorised access to private telephone and internet metadata could only do so because of the current and increasing global interconnectedness. So with the likes of Snowden in the picture, there is greater likelihood of accessing previously classified information through official and unofficial means. The questions posed above can only be answered as time goes on.

What is certain at this juncture is that future studies, while modelled along existing lines will be very different in their nature and gamut to the current ones. At the moment we are studying cyber relations among people but given the versatility of cyber politics, the future could mean studies of the *psychology of cyber machines!* This means that we can expect vast changes in the way cyber technologies are studied. It will in effect be a future of pure cybernetics comprised perhaps of diplomatic relations between and among governing androids.

Even the nature of the diplomatic relations themselves might be very different to ours. This is exemplified with increasing clarity at the moment through the miniaturising of electronic gadgets which is incontestably heading towards the merging of human and animal consciousness with machines resulting in the actuation of our present conceptions of the cyborg and the hologram. Electronic transactions could even end up meaning vulnerabilities of human, intellectual consciousness. While this hubris seems to be rather unseemly at the moment, present trends are heading towards that kind of a lofty future and if no future has ever been built without a history then maybe this paper might in future become one among many such historical accounts in times to come.

## BIBLIOGRAPHY

### Books


Carr, E.H. 1939. *The Twenty Years Crisis (1919-1939). An Introduction to the Study of International Relations*. Basingstoke: Macmillan

Cooper, R. 2003. *The Breaking of Nations: Order and Chaos in the Twenty First Century*. London. Atlantic books Melissen, J. (ed). 1999. Innovation in Diplomatic Practice. Basingstoke: Macmillan

Guelke, A. 2006. *Terrorism and Global Disorder*. IB Tauris & Co Ltd. London

Kaarbo, J. & Ray, J.L. 2005. *Global Politics*. Wadsworth. Cengage Learning

Melissen, J. Ed. 2007. *The New Public Diplomacy: Soft Power in International Relations*. Palgrave Macmillan. Houndmills, Basingstoke, Hampshire RG216X5. NY.

Melissen, J. 2005. *Wielding Soft Power: The New Public Diplomacy.* Netherlands Institute of International Relations. Clingendael

Moore, R. 2005. *Cyber Crime: Investigating High-Technology Computer Crime*. Anderson Publishing. Cleveland, Mississippi

Olins, W. 1999. *Trading Identities: Why Countries and Companies are Taking on Each Other's Roles*. London: Foreign Policy Centre

Pijl, K.. 2006. *Global Rivalries. From the Cold War to Iraq*. Pluto Press. London. Ann Arbor, MI

Steans, J and Pettiford, L. 2001. *International Relations: Perspectives and Themes.* Pearson

Education Limited. Essex England.

Van Ham, P. 2012. *Power, Public Diplomacy and The Pax Americana*. Macmillan Distribution Ltd. Houndmills, Basingstoke

Verton, K.P. 2010. *Cyber Diplomacy for the Future*. Houghton Mifflin, New York

Weitzer, R. 2003. *Current Controversies in Criminology*. Upper Saddle Valley, New Jersey: Pearson Education Press.

**Journals**

Metzl, J.F. 1999. *Popular Diplomacy*. Daedalus, volume 128, no.2. pp 177-9.

**Reports**

Beers, C.L. 2003. *Prepared Testimony Before the Committee on Foreign Relations of the US Senate on 'The American Public and Islam,' Spring 2003*. ABC Global.

Brenner, S.W. 2010. *Cybercrime: Criminal Threats From Cyberspace, Annual Report 2009-2010*. ABC Global.

David, K.L. 2012. *Zappos Cyber Attack, Autumn 2012*. London: Marks & Spencer.

Gottlieb, A. 1991. *"I'll be with you in a minute, Mr Ambassador" Quartely Review1991*. Toronto: Toronto University Press.

James, R. 2013. *The Report Indicates More Extensive Cooperation by Microsoft on Surveillance, Annual Report 2013.* New York: Giffith.

Kunczik, M. 2003. *Transnational Public Relations by Foreign Governments, Annual Report 2002-2003.* London: Lawrence Erlbaum Associations

Lichtblau, E. 2013. *In Secret, Court Vastly Broadens Powers of N.S.A, Quartely Review*. New York: Houghton Mifflin

McClanahan, M. 2013. "*Rep. Todd Rokita: No Government Snooping Without Probable Cause, Annual Report 2012-2013.* Washington: Mclanahan & Parks.

**Websites**

The US Department of State 2013. *Bureau of Public Affairs*. [Online]. Available at: http://www.state.gov. [Accessed: 14 July 2013]

Humphrey, J. 2012. *Cyber Warfare and The Crime of Aggression: The need for Individual Accountability on Tomorrow's Battlefield*. [Online] Available at: http://www.law.duke.edu [accessed: 20 October 2013]

Technolytics 2013. *Fake Tweet Erasing $136 Billion Shows Markets Need Humans*. [Online]. Available at: http://www.technolytics.net.org [accessed: 20 October 2013]

DHS 2013. *Secretary Napolitano and the Attorney General Holder Announce the Largest US Prosecution of International Criminal network Organised to Sexually Molest Children.*[Online, 10 July]. Available at http://www.dhs.gov.us/files [accessed: 20 October 2013]

Rothhacker, R. October 12 2012. *Cyber Attacks Against Wells Fargo*. [Online] available at: http://www.fc.org [accessed: 12 January 2014]

Green, M. 2003. *Behind the Facade of Officialdom.* [Online]. Available at: http://www.infoset.officialdiplomacy.org [accessed: 15July2014]

Lichtblau, E. 6 June 2013. *In Secret, Court Vastly Broadens Powers of N.S.A.* [Online]. Available at http://www.newyorktimes.org/story. [accessed: 8 July 2013].

McClanahan, M. June 9, 2013. *Rep. Todd Rokita: No Government Snooping Without Probable Cause.* [Online]. Available at: http://www.washingtonpost.org/story. [accessed: 12 June 2013].

James, R. June 11, 2013. *The Report Indicates More Extensive Cooperation by Microsoft on Surveillance.* [Online]. Available at: www.newyorktimes.org/story. [accessed: 12 June 2013].

## TABLE OF CONTENTS