Chain Reactions: Analyzing the Influence of Information Technology on Intelligence Systems

Olamide Samuel

Research Paper No. 22

ΚΕΔΙΣΑ KEDISA

ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ
CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

Chain Reactions: Analyzing the Influence of Information Technology on Intelligence Systems

Olamide Samuel

Senior Researcher at KEDISA

Research Paper No. 22

Abstract

Not much has been written on the influence of information technology on intelligence systems as a whole, with the aim of identifying specific underlying advantages and vulnerabilities that accompany the use of information technology in intelligence systems. The effects of information technology on intelligence are generally subtle and often overlooked, while only the more obvious manifestations such as intelligence failures; caused in part by inadequate information sharing and antiquated information technology infrastructure or leaks by whistleblowers appear to be granted significant attention by scholars and commentators. This article, takes a critical look at the significance of the influence of information technology on intelligence systems, and the advantages and vulnerabilities that accompany the utilization of information technology in Intelligence systems. This article also analyzes how these considerations influence the fundamental, organizational and strategic decisions that ultimately determine the fate of intelligence systems in the short and long term.

To determine how information technology has truly affected intelligence systems, the author analyzes the impact of information technology on intelligence as a product, the influence information technology has on intelligence as a process, and the benefits and drawbacks associated with the utilization of information technology in intelligence organizations. To achieve this, the author takes a rather substratal look at how information technology has altered the nature of source information, and the implications these alterations have had on the management of intelligence collection and processing. The utilization of information technology that allows intelligence organizations to cope with these new challenges associated with the management of collection and processing functions and the administration of intelligence product also comes with significant benefits and risks. The consequent demand for intelligence personnel who possess meaningful information technology skills as well as a perceived reliance on the private sector, eventually affect the administration of intelligence systems and dictates the nature of the relationships between intelligence systems and supporting industry.

At the end of this study, the author identifies and reveals these problems and opportunities associated with the application of information technology infrastructure in intelligence systems as a series of cause and effect, which bear resemblance to a chain reaction. A chain reaction which only reveals itself after a culmination of inconspicuous individual symptoms have been substantially ignored. The unique findings of this study are significant because they give readers a more precise understanding of the underlying causes of the changes taking place in intelligence systems, and an idea of what one might expect in the near future.

Table of Contents

Chapter 1- Introduction

Intelligence as a term is applied to certain kinds of information, activities and organizations that are relevant to a governments' formulating and implementing policy to further its national security interests.[1] Intelligence incorporates the identification and analysis of threats to national security. Intelligence also provides the government it serves with information that would equip policy makers' decisions with accurate information with respect to their national security interests. The United States' Federal Bureau of Investigation describes intelligence as *"information that has been analyzed and refined so that it is useful to policymakers in making decisions specifically, decisions about potential threats to our national security[2]"*.

Intelligence gathering as an activity comprises of the willful acquisition of information with the intent to inform policy making. Intelligence agencies are usually government agencies responsible for the collection, analysis, and exploitation of information and intelligence in support of law enforcement, national security, defence and foreign policy objectives of Governments[3].

The term "intelligence" can be viewed from three different perspectives:

- Intelligence is a product that consists of information that has been refined to meet the needs of policymakers.
- Intelligence is also a process through which that information is identified, collected, and analyzed.
- And intelligence refers to both the individual organizations that shape raw data into a finished intelligence product for the benefit of decision makers and the larger community of these organizations[4]

Governments have actively collected information on the intentions, capabilities and policies of friendly and rival states, and Intelligence gathering is accepted as a necessity in conducing foreign relations[5].

Counterintelligence refers to any activity, with the specific aim of protecting information about ones intelligence capabilities[6]. Counterintelligence, as defined in the United States National Security act of 1947, is "information gathered and activities conducted to protect against

---

[1] Shulsky, A. and Schmitt, G. (2002). *Silent warfare*. 1st ed. Washington, D.C.: Brassey's, Inc., p.2.
[2] Directorate of Intelligence, *Intelligence Defined*, Federal Bureau of Investigation (2014), Available at: http://www.fbi.gov/about-us/intelligence/defined , accessed 15th June 2014.
[3]Wikipedia, *Intelligence Agency*, Wikipedia The Free Encyclopaedia (August 2013), Available at: http://en.wikipedia.org/wiki/Intelligence_agency , accessed 16th June 2014.
[4]Directorate of Intelligence, *Intelligence Defined*, Federal Bureau of Investigation (2014), Available at: http://www.fbi.gov/about-us/intelligence/defined , accessed 15th June 2014.
[5]Crane, D. (2002). Fourth Dimensional Intelligence-Thoughts on Espionage, Law, and Cyberspace. *Int'l L. Stud. Ser. US Naval War Col.*, 76, p.311.
[6] Executive Order 12333. (1981, December 4). United States Intelligence Activities, Section 3.4(a). EO provisions found in 46 FR 59941, 3 CFR, 1981 Comp., p.1

espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities[7].

Information technology (IT) simply refers to the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data[8]. Interestingly, the very invention of what can be described as the first electronic, digital and programmable computer in the world was specifically developed to aid the cryptanalysis of British code breakers who were tasked with the gathering military intelligence within the German armed services enciphered code during the Second World War[9]. In recent years, the rapid pace of advancement in information technology's capabilities has introduced an era in which the creation, transmission, storage and retrieval of information is aided by powerful, cheap, accessible and sometimes concealable devices, capable of transmitting and intercepting information at speeds and complexities seldom imaginable in recent human history.

We all have witnessed the growing economic, social and technological role of information in the past decade. The information revolution has left in its wake an irreversible change in the creation and management of information. One would not have to look too far to notice the effects of the evolution of information technology in every sphere of human existence. Since the end of the twentieth century, globalization has spread dramatically, empowered in part by the ability of information and communication technology to permit people to consciously facilitate active real time communication between people, their respective governments and other non-state entities on a global scale.[10]

Not only have people, governments and organizations utilized information technology to improve connectivity and productivity in their day to day affairs, traditional threats to global peace and security have also seized the opportunity to utilize new capabilities provided by information technology to achieve their strategic and organizational goals. Conventional terrorist threats such as Al-Qaeda have consistently utilized information technology to improve the connectivity of their member cells over vast distances via satellite and conventional mobile phones.[11] Criminal networks and adversaries utilize communications infrastructure to enhance their illegal operations. Operations ranging from relatively simple personal communications to more advanced functions

---

[7] Van Cleave, M. (2005). *The National Counterintelligence Strategy of the United States*. 1st ed. [ebook] Available at: http://fas.org/irp/news/2005/03/ncix030505.pdf Accessed 9 Jun. 2014.
[8] Daintith, John, ed. (2009), "IT", A Dictionary of Physics, Oxford University Press
[9] Copeland Jack (2006): *Colossus: The first large scale electronic computer*, Oxford: Oxford University Press, Available at: http://www.colossus-computer.com/colossus1.html#sdfootnote96sym , accessed 25 June 2014.
[10]Wikipedia, *Technology*, Wikipedia The Free Encyclopedia (2014), Available at: http://en.wikipedia.org/wiki/Technology , accessed 4 July 2014.
[11] Mutegi Lilian, Al *Qaeda Using New Encryption Software to Defy US Intelligence Tracking*, CIO East Africa (22 June 2014), Available at: http://www.cio.co.ke/news/top-stories/al-qaeda-using-new-encryption-software-to-defy-us-intelligence-tracking , accessed 8 July 2014.

like digitally transferring funds from illegal sources of origin to points of expenditure[12]. Terrorist groups even utilize advanced encryption technology to thwart tracking efforts by intelligence agencies, geared towards monitoring and understanding their capability and intent[13].For intelligence functions to remain abreast of these emerging threats, collecting and processing information as fast as possible has now become a necessity for government and business organizations alike.

Interestingly, the effects of the incorporation of information technology into intelligence functions and structures have received little attention, and few works examine how information technology has directly influenced the input of human and material resources into an intelligence system. Why then, is information technology being granted the magnitude of attention which it receives in this study? Has information technology influenced intelligence to such a degree that deserves attention? And if it has, what are the benefits of studying the influence of information technology on intelligence? One may even ask if management personnel in intelligence agencies and government should be actively informed on the most recent advancements in information technology. Should the results of this study be of any significance to them as a relevant factor which should be considered when making fundamental, organizational or strategic decisions? These are the questions which bestow significance on this line of inquisition, and have prompted the author to embark on this study.

As Michael Warner rightly argues, a state's technological environment will have both direct and indirect causal relationships on the ways in which a state tasks and organizes its intelligence offices[14]. Whereas Warner treats the conventional technological environment of states as an independent variable in shaping an intelligence system, the case of information technology by virtue of its transnational nature, has proven to be different. Information technology wields an influence on virtually all intelligence systems around the world irrespective of the level of advancement in other technological fields, as it transcends borders, and acts as a mechanism which integrates functions of society, as well as functions of threats to the safety and stability of society.

Therefore, to effectively answer the questions at hand, this article aims to understand how far information technology is transforming the business of intelligence, by analyzing the effects of information technology on the characteristics of information that is obtainable, and how the resultant effects of the findings affect the management of intelligence processes and organizations. Analysis is presented in a linear fashion, with each chapter highlighting the causes that make the

---

[12]Solon Olivia, *Cybercriminals Launder Money Using In-Game Currencies*, Wired.co.uk (21 October 2013), Available at: http://www.wired.co.uk/news/archive/2013-10/21/money-laundering-online , accessed 19 August 2014.

[13] Mutegi Lilian, Al *Qaeda Using New Encryption Software to Defy US Intelligence Tracking*, CIO East Africa (22 June 2014), Available at: http://www.cio.co.ke/news/top-stories/al-qaeda-using-new-encryption-software-to-defy-us-intelligence-tracking , accessed 8 July 2014.

[14] Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.135 Available at: http://dx.doi.org/10.1080/02684527.2012.621604 accessed 12 June. 2014.

incorporation of information technology relevant to an intelligence function or structure and then analyzing the resultant effects of the application of such technologies.

Chapter 2- The Impact of Information Technology on Source Information

While information technology continues to evolve in scope and complexity, there are wider implications on intelligence systems. As the means of creating and storing information becomes ever so complex, one can argue that intelligence as a product itself evolves in direct proportionality with the nature and volume of information from which it is sourced. Intelligence systems have evolved to cope with changes brought about by the information revolution, and it is only from the knowledge of the changed nature of source information, and its resultant effect on the management of intelligence collection and production systems that an understanding of the severity of the changes brought about by information technology can be achieved.

Striving to understand the nature, volume and integrity of source information in itself, may not come across as an important undertaking. However, it is only when we realize the significant impact it has on Intelligence collection management, that it is relevant to an intelligence organization. Intelligence collection management is essentially the process of managing and organizing the collection of intelligence information from various sources[15]. Information technology has enabled the utilization of newer means and methods with which intelligence agencies gather information about their adversaries and immediate and long term threats to the safety and stability of the governments they serve. In addition to HUMINT and other collection sources previously used by intelligence agencies, the discovery of new digital means of sourcing information means that specific information about intents and capabilities appear in newer forms, such as metadata and programming code. These are forms of information which require some degree of familiarity by collectors and analysts to appreciate its value. The utilization of information technology in daily affairs means that specific kinds of source information can only be stored on copious digital databases. Databases that as we shall see in chapter 4, can only be managed on platforms developed by information technology experts.

Nature of Source Information

As information technology evolves, so does the data which these new technologies create. Any piece of data that has been collected and analyzed for the purpose of informing decision making to provide a strategic advantage over an adversary can take on many forms today. During the cold war era, data created and transmitted, manifested in forms such as, text, codes, radio waves, photographs, voice recordings, video recordings etc[16]. These pieces of data available at the time were analyzed and intelligence obtainable form these data made available to policy makers. Source information in the 'Analog revolution' ranged from text, photographs, maps, codes etc, and Analysts in demand at that time ranged from cryptographers to mathematicians with advanced skills in code breaking[17]. Evidently, the very nature of source information has transformed over

---

[15] Wikipedia, *Intelligence Collection Management*, Wikipedia The Free Encyclopaedia (June 2013), Available at: http://en.wikipedia.org/wiki/Intelligence_collection_management#CIA_collection_guidance, accessed 31 July 2014.
[16] Wikipedia, *Signals Intelligence in the Cold War*, Wikipedia The Free Encyclopaedia (2014), Available at: http://en.wikipedia.org/wiki/Signals_intelligence_in_the_Cold_War , accessed 27th July 2014.
[17] Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.141 Available at: http://dx.doi.org/10.1080/02684527.2012.621604 accessed 12 June. 2014.

the years in direct proportionality with the technology used to create, analyze, transmit and store them.

This means that today, information about an enemy's capability, intent or actions can be sourced from a vast range of newer forms of information, for example, financial records obtained from digital credit card statements of an adversary with an established intent to engage in terrorism, but no hitherto capability to carry out radical intentions could be regarded as actionable intelligence- assuming transaction records show that dangerous weapons (which amount to capability)have been purchased by such an individual or group. This source information might not be kept secret and could go unnoticed in the massive pool of financial transactions being recorded daily, and without the active functioning of adequate collection and analysis assets embedded in financial institutions, these threats could go unnoticed. Big-Data analytics aid the access and utilization of information, and analysts are charged with the task of deciphering such information. However, collectors and analysts would most definitely need to have a fundamental understanding of how to identify specific kinds of electronic transactions to make sense of the source information, and rise to the occasion. Infinite examples of unconventional forms of source data could be cited, such as Metadata and digital records of access to databases and one can deduce from this logical train that there is a correlation between advancements in information technology and the newer forms of source information that have been created as a result of this phenomenon. Therefore, there is a need for intelligence agencies to have the right assets to deal with these newer forms of source information that exist.

Volume of Source Information

Virtually all humans utilize some form of information technology in their daily endeavors to transmit, create, organize, store and retrieve vast amounts of data[18]. It is estimated that a staggering 8.7 billion devices are connected to the internet, and that approximately one-third of the world's population are internet users.[19] The world contains an unimaginably vast amount of digital information which is getting larger ever more rapidly.[20] Almost all functions of civilization have moved documentation of their activities from pens and papers, to digital media. It is estimated today that more data crosses the internet every second than were stored in the entire internet just 20 years ago[21]. Specifically, as of 2012, about 2.5 Exabytes (approximately 2.5 billion Gigabytes)

---

[18] Information Technology, *Information Technology Strategic Plan*, Federal Bureau of Investigation (2010-2015), Available at: http://www.fbi.gov/about-us/itb/it-strategic-plan-2010-2015 , accessed 8 August 2014.

[19] Rob Soderbery, "How many things are currently connected to the internet to the 'internet of things' (IoT)?" (7 January 2013). Available at: http://forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot, accessed 30 July 2014

[20] Cukier Kenneth, *Data, Data Everywhere*, The Economist (25 February 2010), Available at: http://www.economist.com/node/15557443 , accessed 29 June 2014.

[21] Brynjolfsson Erik and Mcafee Andrew, *Big Data: The Management Revolution*, Harvard Business School (October 2012), Available at: http://hbr.org/2012/10/big-data-the-management-revolution/ar , accessed 14 July 2014.

of data are created each day, and that number is doubling every 40 months or so[22]. For instance, it is estimated that Wal-Mart an American retailer, collects more than 2.5 petabytes of data every hour from its customer transactions. A petabyte is one quadrillion bytes, or the equivalent of about 20 million filing cabinets' worth of text. An Exabyte is 1,000 times that amount, or one billion gigabytes[23]. One could only begin to imagine the implications of such an explosion in the volume of source information implications on the administration of intelligence systems. The most effective way to explain the impact of an increase in the volume of source information on intelligence would be to analyze the direct relationship between the size of the operational environment (source information), volume of data, information and the intelligence product.

The revised edition of the JP 2-0, Joint Intelligence report sheds some light on the relationship between raw data, source information and intelligence. It explains the process in which intelligence is extracted from source information. In the narrative, it is highlighted that unprocessed data by itself has relatively limited utility to intelligence consumers and that when data is collected from a sensor and processed into an intelligible form; it becomes information and gains greater utility. Information on its own may be of some utility to the consumer, but it is not until when information is related to other information about the operational environment and understood in the light of past experience, that it gives rise to a new understanding of the subject of analysis, this understanding may be termed "actionable intelligence."[24]

With the generation of information at unprecedented rates unimaginable in recent human history, it is no surprise that the acquisition of actionable intelligence from an infinitely vast and ever increasing pool of raw data is a herculean task to say the least. The sheer volume of data in a global operational environment made possible by the ubiquitous internet presents a unique challenge to intelligence agencies today.

Integrity of Source Information

The integrity of information being perceived by intelligence is a fundamental concern of both the producers and consumers of intelligence. Much like the problems associated with verifying human sources of information, the transmission of intelligence on newer technological platforms developed by information technology experts has some implications for the collectors, producers and customers of it. Threats to the integrity of information being perceived by intelligence, are not only vulnerable to interception and manipulation by adversaries while signals are being broadcast as was the case with radio and other transmissions in the world wars, the integrity of information is also at risk while data is at 'rest' because of the inherent nature of the data transmitted today, where there is always the possibility of 'secure' data being corrupted by an adversary from a remote location. The security of intelligence led-operations in today's world

---

[22] Brynjolfsson Erik and Mcafee Andrew, *Big Data: The Management Revolution*, Harvard Business School (October 2012), Available at http://hbr.org/2012/10/big-data-the-management-revolution/ar, accessed 14 July 2014.
[23] *Ibid*
[24] Joint Intelligence. (2014). 2nd ed. [ebook] Washington DC: Joint Chiefs of Staff. Available at: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf Accessed 6 Jun. 2014.

relies on the uncompromised integrity of the information which informs their actions. External manipulation of even peripheral information about intelligence or military operations, such as changing the co-ordinates of an extraction point, could have severe consequences. Although it is unlikely that such manipulation could occur in the most sophisticated intelligence agencies today, the presence of malicious software on a secure network renders the entire network suspect because of the fact that it is there, even if the malicious software has not tampered with sensitive or peripheral information. Michael Warner postulates a logically sound argument which equates data security with operational security referring to the principles of information assurance and his conclusions agree with the aforementioned point[25].

The adequate management of source information is a necessity in a world where massive volumes of data are created every second, and leading experts in the commercial information management, such as the Software Engineering Institute, Carnegie Mellon University propose that advancements in information technology can furnish intelligence operations and organizations with tools which aid them to manage source information, more efficiently than ever before.[26] One can understand that the increase in the volume of data and the predicament of intelligence agencies to cope with newer forms of data is a direct result of the effects of advancements in information technology on source information.[27] If intelligence must be efficient in such a dynamic environment created by advancements in information technology, it must direct resources to source information more efficiently than its adversaries in this global operational environment created by information technology. Thus, in-depth understanding of how information technology has affected source information would aid managerial staff in determining the operational environment of collection and production assets of an intelligence agency, in a manner that would source relevant information to satisfy the requirements of policymakers without unjustifiably exhausting scarce resources and would enhance the efficiency of strategic operations embarked upon by intelligence agencies.

Understanding how information technology has altered source information, is one of the inconspicuous individual ramifications of information technology's influence on intelligence systems, and the changes observed in the nature, volume and integrity of source information proves to be one of the important factors which scholars and commentators in intelligence studies have overlooked. By observing the impact of the changes in source information on the management of collection and production systems in intelligence, one would be able to identify and understand the underlying causes of the problems which are associated with the direction, collection and analysis functions of intelligence in the 21st century.

---

[25] Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.149 Available at: http://dx.doi.org/10.1080/02684527.2012.621604 accessed 12 June. 2014.
[26] Townsend Troy, Ludwick Melissa, McAllister Jay, Mellinger Andrew and Sereno Kate, *SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project*, Carnegie Mellon University (January 2013), Available at: http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf, accessed 5 September 2014
[27] Joint Intelligence. (2014). 2nd ed. [ebook] Washington DC: Joint Chiefs of Staff. Available at: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf Accessed 6 Jun. 2014.

Chapter 3- The Impact of Source Information on the Management of Collection and Production Systems

The increase in the volume of data and the predicament of intelligence agencies to cope with newer forms of data is a direct result of advancements in information technology.[28] The imperative need for intelligence agencies to consider data management with analysis and analysts to cope with increasing volumes and types of data is what authors such as Michael Warner and Melanie Gutjahr have laid emphasis on. [29]

The effect of information technology on the management of the collection of intelligence can be viewed from two standpoints. For ease of understanding, the intelligence process is in this article is divided into roughly two phases, The Collection phase, and the Production phase. The direction of collection assets in an operational environment, and then the specific skills and tools that need to be possessed by the collection assets to be effective in their collection tasks all fall under the collection phase. The production phase encompasses the analysis of intelligence, and examples of how advancements in information technology have affected intelligence analysis are revealed as well. The full effects of the utilization of information technology to manage intelligence functions can truly be brought to light after the examination of recent developments in intelligence collection disciplines, and attempts by intelligence organizations to enhance intelligence analysis through various means have been illustrated.

The Collection Phase - Managing the Collection of Intelligence

During the decades of the cold war, information needs of intelligence agencies were directed at clear and specific adversaries, and collection efforts were targeted at assets of adversaries based on the need for tangible information to decipher for strategic purposes. Intelligence assets were optimized for collection in an operational environment in which Information was scarce and special collection skills were needed to gather intelligence from a relatively small operational environment in contrast with the volume of information one has to cope with today.

Consumer Requirements

In recent times, intelligence agencies have focused on obtaining intelligence on critical security and economic issues to inform better policy decisions, while also actively operating overseas to disrupt terrorism and proliferation of dangerous offensive weapons, amongst other things[30]. The requirements placed on intelligence agencies by consumers to collect tangible intelligence on an adversary by far outstretch the capability of intelligence agencies to allocate scarce collection resources today. Indeed, the information revolution has changed consumers'

---

[28] Joint Intelligence. (2014). 2nd ed. [ebook] Washington DC: Joint Chiefs of Staff. Available at: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf Accessed 6 Jun. 2014.
[29] Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.141 Available at: http://dx.doi.org/10.1080/02684527.2012.621604 accessed 12 June. 2014.
[30]Secret Intelligence Service, *SIS Strategy And Values*, Secret Intelligence Service MI6 (2010-2015), Available at: https://www.sis.gov.uk/about-us/sis-strategy-and-values.html, accessed 13 June 2014.

expectations about intelligence products[31]. The interesting phenomenon is that because Intelligence is increasingly seen to be the heart of international security, it now plays a more prominent role in the public affairs of western societies today than it ever has in history[32]. Policy makers are now demanding new kinds of information about new things from new sources delivered in new ways, and Information technology has now enabled policy makers and consumers to tap into volumes of open source information at speeds seemingly comparable to collection speeds of intelligence agencies. These policy makers whether rightly or wrongly, view open source information as a useful substitute source of intelligence[33]. To remain a relevant and viable option to influence policy making, intelligence agencies must increase the speed and accuracy of their collection resources to tap into both secret and open sources of information and make accurate analytical judgments of information in shorter periods of time. In some ways, one could argue that some sort of competition exists between intelligence agencies and other means which intelligence consumers now turn to, to satisfy their needs. To effectively boost the real-time collection of intelligence, it has been observed that numerous intelligence organizations now equip the various collection disciplines with advanced information technology to maximize the efficiency of these collectors.

Enhancing Existing Collection Disciplines

Traditional Intelligence Collection disciplines now utilize advancements brought about by information and communications technology to maximize speeds and volumes at which information can be collected. Human (HUMINT) collection disciplines utilize gadgets such as encrypted smart phones, satellite phones, emails, and data transfers etc to aid in collection. It is no surprise that virtually all intelligence personnel utilize some form of information technology in their daily endeavors[34]. Data transfers from Geospatial Intelligence (GEOINT) gathered from satellite, aerial photography and mapping/terrain have improved thanks to improvements in connectivity speeds and capabilities; Open Source Intelligence (OSINT) gathered from open sources has increased in volume and complexity and can be tapped into utilizing information technology, and a new intelligence discipline Cyber Intelligence or (CYBINT) gathered from cyberspace owes its very existence to developments in information technology[35].

While new dimensions and means of collecting intelligence have been influenced by advancements in information technology, one could also argue that information technology has merely served as a tool employed by intelligence agencies to extend the reach and capability of

---

[31] *Ibid*

[32] Scott Len and Hughes R, *Intelligence In The Twenty-First Century: Change And Continuity Or Crisis And Transformation?*, Routledge (2009)

[33] Lahneman William, *The Future Of Analysis*, Center For International And Security Studies At Maryland (2006) Available at: http://www.cissm.umd.edu/papers/files/future_intel_analysis_final_report1.pdf , accessed 29 June 2014

[34] Information Technology, *Information Technology Strategic Plan*, Federal Bureau of Investigation (2010), Available at: http://www.fbi.gov/about-us/itb/it-strategic-plan-2010-2015, accessed 8 August 2014.

[35] Wikipedia, *List Of Intelligence Gathering Disciplines*, Wikipedia The Free Encyclopaedia (2014), Available at: http://en.wikipedia.org/wiki/List_of_intelligence_gathering_disciplines, accessed 28 August 2014.

existing collection disciplines, without fundamentally altering the underlying motives and reasons for the collection of intelligence which existed in the world wars. Another conclusion which is more popular in news narratives is that certain developments in information technology are the direct cause of unconventional threats and new motives behind criminal and political activity such as 'hacktivism' are a direct consequence of advancements in information technology. This is a point of view which certain employees of intelligence agencies, such as Shawn McFeely of the F.B.I seem to agree with[36].

The Problem of Collecting too much Data

In a vast pool of information it is difficult to resist tendencies to siphon all available data on an adversary in such a manner that tangible intelligence would be lost or omitted during analysis of such information. In addition to traditional sources of classified information, intelligence agencies must also extract potentially critical knowledge from vast quantities of available open source information and the Intelligence community must devise ways to monitor open source information in 'transformed ways' a point that authors such as William Lahneman agree with[37]. Melanie Gutjahr contributes to this debate, by pointing out that even the United States national technical means of collection (from the operational environment), yields data vastly exceeding processing and analytical capabilities to extract timely and actionable intelligence[38]. She suggests that intelligence agencies continually attempt to shift collection resources and analytical focus to provide relevant intelligence.

The Processing Phase - Enhancing the Analysis of Intelligence

Intelligence analysis is perhaps one of the most dynamic fields facing reform in the profession of intelligence today. Several factors such as fundamental changes in analyst education, recruitment, training, management, organization and retention all play a pivotal role in the direction in which the future of intelligence analysis would take. However, one cannot overlook the impact of information technology on the management of intelligence analysis.

The problem of Dealing with too much Data

Gutjahr argues that while intelligence has invested in collection to meet an endless supply for requirements, analysis has been shortchanged. John M. Custer the former commander of the Army Intelligence Center US, believes that technology has conquered the problem of collection, but has created massive problems related to storing and analyzing data, and to disseminating useful

---

[36] The New Yorker, *Network Insecurity*, The New Yorker (20 May 2013), Available at: http://www.newyorker.com/magazine/2013/05/20/network-insecurity, accessed 13 July 2014.
[37] Lahneman William, *The Future Of Analysis*, Center For International And Security Studies At Maryland (2006) Available at: http://www.cissm.umd.edu/papers/files/future_intel_analysis_final_report1.pdf , accessed 29 June
[38] Gutjahr Melanie, *The Intelligence Archipelago*, Joint Military Intelligence College (May 2005), Available at: http://cryptome.org/2014/04/spy-coping.pdf , accessed 6 August 2014.

intelligence[39] or as Regina Dugan[40] dramatically puts it "We are swimming in sensors and drowning in data.[41]" "We don't have the analytic tools or the storage capability" needed to turn the all of the data into actionable intelligence", said Custer in an interview in 2012. Lahneman provides a comprehensive commentary on the effect of the information revolution on the intelligence process. He expounds that it requires intelligence agencies to shift the scale of their analytical focus. He talks of threats that are on a much smaller scale than those previously witnessed during the Cold War[i42]. His commentary highlights the significance of effective analysis of information as a critical asset to understand global dynamics as never before[43].

The digital revolution creates a much greater demand for analysts and analysis states Warner[44].He goes further to state that the collection of digital information by digital means can easily outstrip the ability of analysts to sort through information. Exhibiting his mathematical prowess, he cites an example of the Chinese hacking incident in which hackers had downloaded about 20 Terabytes of Data[45] from the Department of Defense's Non-Classified Router Network (NIPRNet)[46]. He suggests that at a good reading speed of 230 words per minute, it would take up to 6666 work years (each of 50 work-weeks of 40 hours each) just to read[47]. What one would observe from his comments is that the digital revolution compresses time intervals available to intelligence agencies to enable the recognition of relevant information, decision making, discrimination and action[48]. An inherent vulnerability intelligence agencies face is that, with the relative ease and speed with which adversaries can create and transmit data, adversaries can generate massive amounts of misleading electronic chatter from similar technology used to launch a Denial of Service attack, which could make it increasingly unlikely that analysts would be able to interpret warning signs of an attack, as enemies can disguise signals pertinent to an attack on targets, in massive waves of distorted or misleading information[49]. The management of analysts

---

[39] Matthews William, *Data Surge And Automated Analysis: The Latest ISR Challenge*, Government Business Council (January 2012), Available at: http://www.emc.com/collateral/analyst-reports/the-latest-isr-challenge-insights-gbc.pdf, accessed 19 June 2014.

[40] Director, Defense Advanced Research Projects Agency

[41] Matthews William, *Data Surge And Automated Analysis: The Latest ISR Challenge*, Government Business Council (January 2012), Available at: http://www.emc.com/collateral/analyst-reports/the-latest-isr-challenge-insights-gbc.pdf, accessed 19 June 2014.

[42] Lahneman William, *The Future Of Analysis*, Center For International And Security Studies At Maryland (2006) Available at: http://www.cissm.umd.edu/papers/files/future_intel_analysis_final_report1.pdf , accessed 29 June 2014.

[43] *Ibid*

[44] Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.146 Available at: http://dx.doi.org/10.1080/02684527.2012.621604 accessed 12 June. 2014.

[45] One Terabyte of Data is equivalent to One thousand Gigabytes of Data

[46] Dawn S Onley, 'Red Storm Rising', *Government Computer News*,

[47] Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.146 Available at: http://dx.doi.org/10.1080/02684527.2012.621604 accessed 12 June. 2014.

[48] *Ibid*

[49] Mahadevan Prem, *Intelligence Agencies: Adapting To New Threats*, Eidgenossiche Technische Hochschule Zurich Center For Security Studies (October 2010), Available at: http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-82.pdf, accessed 30 July 2014

and analysis therefore, has become a prime concern for intelligence agencies that wish to make reasonable sense of the information collected.

Automated Analysis Programs

Interestingly an observation of the US National Intelligence program's congressional budget justification's community management account of 2012, shows that a number of projects embarked on by the US intelligence community gear towards automated analytic tools to aid intelligence analysis as a solution to the problem of 'data glut'[50]. The debate as to whether automated analytical tools can be a viable substitute for direct human input is inconclusive. However, as we have witnessed in the past decade, the rapid pace of development in information and computational technology has shed light on the reality that almost any task could be subjected to mathematical processes with immense speed, volume and precision[51]. The United States Intelligence community seems to be taking this consideration very seriously as it has invested heavily in automated analysis programs.

The intelligence advance research projects activity (IARPA) in a heavily redacted management account, indicates its interest in developing automated technologies that will guarantee maximum insight from otherwise massive, disparate, unreliable and dynamic data in a timely manner. One example of such is a program[52] that would expose the underlying shared beliefs in a culture by analyzing shared metaphors in languages. The KDD or Knowledge Discovery and Dissemination program which aims to allow analysts rapidly produce actionable intelligence is also being funded by the US intelligence community. The ALADDIN video program, which stands for the Automated Low-Level Analysis and Description of Diverse Intelligence program, is an advanced information based technology which is to support rapid content-based event searches of large collections of video clips, among some other additional but fascinating features[53].

As impressive as these programs may sound, the intelligence community also invests in more complex automated programs to check and predict sense making and analytical judgments of analysts. Some of these programs include the ICArUS program, which stands for the Integrated Cognitive-Neuroscience Architectures for Understanding Sensemaking, which is working on brain based computational models and the SIRIUS program which is an automated program set to train analysts to recognize and mitigate cognitive bias during analysis[54].

These programs may or may not have been created to serve as a direct substitute for intelligence analysts, but some western intelligence agencies seem to believe that analytical programs would benefit intelligence analysis in an age where information exceeds the capacity for

---

[50] *FY 2013Congressional Budget Justification*, National Intelligence Program (February 2012), pg. 59
[51] Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.143 Available at: http://dx.doi.org/10.1080/02684527.2012.621604 accessed 12 June. 2014.
[52] Specific Name of the program was redacted in the report
[53] *FY 2013Congressional Budget Justification*, National Intelligence Program (February 2012), pg. 60
[54] *Ibid*

intelligence analysts to sort through information adequately. The dividends of automated analysis may not be felt for a while, but what needs to be understood is that if successful, intelligence agencies that possess such technologies at the time would once again be placed at a strategic advantage that would be difficult to lose.

The Constant Possibility of Failure

Conversely, the evolution of information technology and its incorporation in intelligence has not meant the elimination of strategic surprise, or other forms of intelligence failures either. While information technology and the proliferation of powerful technical surveillance platforms on an industrial scale appear to have maximized surveillance reconnaissance functions of the most powerful intelligence agencies, strategic surprises have proven to be unavoidable, and intelligence failures still occur. The near success of the Russian operation Anadyr in the early months of 1962, could in part be blamed on the lack of surveillance and reconnaissance platforms because of the unavailability of instantaneous photographic reconnaissance, which caused a delay in a reaction from US policy makers at the time, and some could argue that such a large scale operation would have been detected earlier than it had been, if information technology was as advanced as it is today, and it is not surprising that an NSA publication supports this argument[55]. But if advancements in information technology have indeed granted the most advanced intelligence agencies total surveillance capabilities all over the world, then what would we say about the success of the 9/11 terrorist attacks? Or the lack of credible intelligence on Saddam Hussein's WMD's in 2002? Or The Russian annexation of Crimea? Or the unexpected pace at which ISIS in Iraq is advancing? Is the problem of too much Data, as crippling to intelligence agencies as the problem of too little information? Are intelligence agencies merely reacting to capabilities of adversaries by investing in similar but more sophisticated technologies to merely maintain a narrowing strategic lead?

The impact of information technology on the management of functions of the intelligence process is an indication of our lack of complete understanding of the characteristics of the new dynamics being introduced by information technology. The utilization of information technology to aid collection disciplines to simply collect more data is a premature response that merely passes on the bulk of the confusion about the dynamics of information flow, from the collectors of intelligence, to the analysts. Obviously, these Analysts do not have the capacity to cope effectively with exponentially increased volumes of information and some intelligence organizations seem to believe that these problems would be solved using automated analysis programs. While the methods of intelligence collection and analysis have significantly changed because of the emergence of information technology, underlying motives and problems associated with intelligence collection and analysis have remained constant. There are significant risks and

[55]National Security Agency, *A Reconsideration Of The Role Of SIGINT During The Cuban Missile Crisis, October 1962 (Part 4 Of 4)*, National Security Agency (2003), Available at: https://www.nsa.gov/public_info/_files/crypto_almanac_50th/reconsideration_of_the_role_of_sigint_part_4.pdf, accessed on 8 August 2014.

opportunities to be taken into consideration before intelligence systems can embark on large scale migrations to use information technology infrastructure as platforms for producing intelligence, but up until the time of writing, intelligence agencies have not successfully eliminated age old pitfalls in intelligence collection and analysis by continually reacting impulsively to the dynamics of information flow in the 21st century.

The next chapter focuses on the Impact of information technology on the administration of intelligence Organizations. We would look at the impact of information technology on the existing organizational structures of intelligence agencies, and how intelligence organizations so far, have tried to manage organizational structures to be as efficient as they can, while coping with the administration of various forms of intelligence product.

Chapter 4- Information Technology and the Administration of Intelligence Organizations

Understanding the requirements placed on intelligence organizations by policy makers because of the interrelated nature of threats in today's world is as important as understanding the impact of the increasing volumes of information on intelligence today. One would have to take a closer look at the considerations of intelligence experts, fueling the call for organizational reform to shed some light on the consequences of the evolution of information technology on the structure of intelligence organizations, and the complexities associated with managing intelligence product today.

The Management of Existing Intelligence Organizations

In response to previous intelligence failures many intelligence agencies have undergone structural reform, as an effective top-down reform may be an important first step in improving intelligence quality.[56] Till today, no nation or enterprise has fully solved the problems of productivity or accountability brought about by the new digital means, so it is not surprising that intelligence agencies have not been able to successfully tackle this management challenge as well.

Intelligence agencies are leaning towards making organizational shifts to achieve a flexible, responsive, business like enterprise akin to structural peculiarities of thriving multinational business corporations to effectively tackle the challenges in the digital age[57]. Rapid technological and organizational changes consider agility, adaptability and innovation as the most important qualities to be possessed by intelligence organizations today.

> *"Those who cling to old ways, or fail to take appropriate countermeasures, are defeated or pushed aside as their decreasing effectiveness becomes ever more glaring (and dangerous)"* – **Michael Warner[58]**

Influx of IT personnel

Intelligence agencies once more, have looked to information technology as a solution by applying information technology based solutions as the backbone for the storage, retrieval and classification of intelligence, as they seek to create a more flexible and adaptable workforce within existing hierarchical structures. Information security and clearance systems based on a standardized information technology platforms to aid in the management of intelligence have been adopted by the US and UK intelligence communities to improve the efficiency of retrieving intelligence from databases[59]. Intelligence communities have to adapt, in order to maintain

---

[56] The Changing Face of Intelligence: NATO Advanced Research Workshop – Report. (2005). 1st ed. [ebook] Available at: http://www.sant.ox.ac.uk/centres/Nato_conf_report_0106.pdf Accessed 16 Aug. 2014.
[57] *FY 2013Congressional Budget Justification*, National Intelligence Program (February 2012), p.45.
[58] Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.140 Available at: http://dx.doi.org/10.1080/02684527.2012.621604 accessed 12 June. 2014.
[59] Kenyon Henry, *Intelligence Agencies Move Towards Single Super-Cloud*, Breaking Defense (17 December 2012), Available at: http://breakingdefense.com/2012/12/intelligence-agencies-move-towards-single-super-cloud/, accessed 10 June 2014.

adequate control over their intelligence database and to ensure its security as well as its effectiveness. This permits people with expertise in large-scale information database management, as well as people with useful skills in information technology to be relevant in intelligence agencies. The creation of the Chief Information Office to support the US intelligence community to establish common IT standards, protocols and interfaces in the National Intelligence program 2013[60], signifies the increasing importance of information technology experts in the field of intelligence.

With highly skilled information technology experts in greater demand in all spheres of business and government, Intelligence agencies also have to increase employee incentives and improve human resource management in order to maintain a more flexible and dynamic work-force capable of responding to threats, in an era where highly skilled information technology experts are higher paid in the private sector and would more likely put their skills to use there if conditions for employment are more suitable for them[61]. The most interesting development that has received little or no commentary is the fact that Intelligence agencies have also turned to information technology to aid in the Recruitment of agents by advertising job openings and offers on the internet[62]. A little over a decade ago, intelligence agencies publicly advertising vacancies and recruitment criteria would not only have been unheard of, but would have been virtually counter-productive, online recruitment of intelligence personnel appears to be a desperate but effective means of attracting skilled labor and people with raw talent of use to intelligence agencies have been scooped up by intelligence organizations in this manner. It is also interesting to note that while traditional cold-war recruitment schemes of intelligence agencies may still be operational, Cyber specialists are the most advertised jobs online by intelligence agencies.

The organizational structure of intelligence agencies have decided to adopt has been greatly influenced by contemporary solutions available, that would enhance efficiency, and this is not unique to the emergence of information technology. In the World Wars, an increase in the demand for cryptologists linguists and code-breakers, were as a result of the strategic need for intelligence agencies to decipher encrypted information at the time[63]. This is the same phenomenon that is observable today, hackers and programmers are in increased demand because they are the best suited to function in a world where malicious attacks can emerge from a Cyber dimension, such as cyber-jihadists which Corera talks about in an interview with the BBC[64]. Technological shifts are forcing intelligence agencies to reshuffle resources, tasking and authorization on an

---

[60] *FY 2013Congressional Budget Justification*, National Intelligence Program (February 2012),
[61] Center For Intelligence And Security Studies, *Career Outlook*, The University of Mississippi (2014), Available at: http://ciss.olemiss.edu/students/careers/, accessed on 17 August 2014.
[62] Intelligence.Gov, *We Have Thousands Of Opportunities In All Kinds Of Occupations*, Intelligence.Gov (2014), Available at: http://www.intelligence.gov/careers-in-intelligence/, accessed 11 June 2014.
[63] The Bill Tutte Memorial Fund, *How Bill Tutte Won The War*, The Bill Tutte Memorial Fund (2014), Available at: http://billtuttememorial.org.uk/wp-content/uploads/2014/05/How-Bill-Tutte-Won-the-War.pdf, accessed 9 July 2014.
[64] Corera, G. (2014). The World's Most Wanted Cyber-Jihadist. *BBC News*. [online] Available at: http://news.bbc.co.uk/1/hi/world/americas/7191248.stm Accessed 10 Jun. 2014

organizational scale today, just as they have always done since the world wars[65]. It is safe to say, a race is on to figure out intelligence organizations and doctrines for the digital age, because at the moment, it is observable that intelligence systems are merely responding to demands created by information revolution and have no real control over dictating the pace of change in intelligence systems, but are merely being swept by the tide[66].

The Administration of Intelligence Product within Intelligence Organizations

The ability of the intelligence community to utilize technological innovations to administer intelligence is outstanding. The movement of digital data instead of paper has revolutionalized management of information[67]. Intelligence agencies have been empowered by information technology to move data at lightning speed thereby granting consumers of intelligence access to intelligence product in real time.

Finished intelligence products take on various forms depending on the needs of the decision maker and reporting requirements[68]. In recent times, the movement and storage of intelligence product hinges on information technology infrastructure, because of the speed at which any amount of information can be transmitted over vast distances to consumers of intelligence in a relatively secure manner. However, as intelligence agencies and policy makers continue to enjoy the benefits and efficiencies of information technology, one must be aware of the serious challenges associated with managing intelligence in Cyberspace. New threats associated with the utilization of information technology infrastructure means that intelligence producers and consumers must take specific steps to ensure that actionable intelligence of any form in their possession is protected from adversaries who wish to collect and exploit it.

Cyberspace in this context is described by The US Department of Defense as "a global domain…consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems and embedded processors and controllers."[69] Frank Turner II uses a functional framework approach to describe the interdependent elements that make up cyberspace, consisting of People, Data, Software, Hardware and Infrastructure[70]. Using the components in his functional framework as a reference point the author would explain the functional nature of cyberspace and how developments in information technology has altered the way intelligence is disseminated today.

---

[65] Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.135 Available at: http://dx.doi.org/10.1080/02684527.2012.621604 accessed 12 June. 2014.
[66] *Ibid*
[67] Gutjahr Melanie, *The Intelligence Archipelago*, Joint Military Intelligence College (May 2005), Available at: http://cryptome.org/2014/04/spy-coping.pdf , accessed 6 August 2014. Pg. xvi
[68] Wikipedia, *Intelligence Cycle*, Wikipedia The Free Encyclopaedia (August 2013), Available at: http://en.wikipedia.org/wiki/Intelligence_cycle , accessed 16th June 2014.
[69]Association of the United States Army, (2014). *The Army in Cyberspace*.
[70] *Ibid*

- User: Refers to the person who accesses cyberspace with the use of Hardware as the access tool, and Software as the interface to view data.
- Data: Refers to all information in whatever form they appear, such as Text, Images, Audio and Video.
- Software: Refers to the user interface, such as Word applications or Internet browsers for example, Microsoft Outlook, which is a program designed to receive and transmit emails.
- Hardware: Refers to any piece of technology, such as a personal computer, a cellular phone or transmission tower, which enables users to connect to information and communications infrastructure.
- Infrastructure: comprises of all telecommunications networks, the internet, hardware, software and users which are interdependently connected

Because Cyberspace is individual and user-centric[71], Individual intelligence personnel and consumers decide when and how to access it. Intelligence can be transferred to secure retrieval points for the consumer to access, such as secure emails, through encrypted lines over GSM networks, or to a digital storage facility. The threats against users of information technology are geared at exploiting vulnerabilities related to the nature of utilisation of these technologies[72]. As a matter of fact According to *the IBM Security Services 2014 Cyber Security Intelligence Index report*, over 95 percent of all cyber-based interception incidents investigated recognize human error as a contributing factor[73].

Interception and intrusion technology actively exploit errors made by users of technology, and such mistakes seem relatively mundane but can prove to be very costly. For example simple errors such as connecting to unsecured wireless networks, or making phone calls with unencrypted cell phones could cause significant damage to the progress of an intelligence operation and can be very embarrassing[74]. Several viruses can target and siphon large amounts of sensitive data from hardware that is connected to such networks, and all it takes is human error on the part of individuals to render sensitive intelligence vulnerable to such attacks.[75]

Governments have recognized the importance of developing the information technology skills of their administrating personnel and intelligence agencies are no exception. Intelligence agencies actively focus on the training of their personnel's cyber skills to ensure that they do not become

---

[71] Association of the United States Army, (2014). *The Army in Cyberspace*.
[72] Pinola Melanie, *Is It Safe To Use An Open Wireless Network?*, About Technology (2014), Available at: http://mobileoffice.about.com/od/wifimobileconnectivity/f/is-it-safe-to-use-an-open-wireless-network.htm, accessed 18 August 2014.
[73]IBM Global Technology Services, *IBM Security Services 2014 Cyber Security Intelligence*, IBM Global Technology Services (2014), Available at: http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf, accessed 6 August 2014.
[74]BBC News Europe, *Ukraine Crisis: Transcript Of Leaked Nuland-Pyatt Call*, BBC News Europe (7 February 2014), Available at: http://www.bbc.co.uk/news/world-europe-26079957, accessed 23 June 2014.
[75] Cuthbertson Anthony, *Ukraine Computer Networks Hit by Russian-based Virus*, International Business Times (10 March 2014), Available at: http://www.ibtimes.co.uk/ukraine-computer-networks-hit-by-russian-based-snake-virus-1439592, accessed 9 July 2014.

vulnerable to such attacks, for example in the United Kingdom, the GCHQ has invested in the CESG Certified Professional (CCP) scheme to address the growing need for specialists within the cyber security profession and is currently building a community of recognized professionals in both the UK public and private sectors [76].

> *"If we are to understand the world we cover and to provide policymakers with the intelligence that they expect, if not demand, we must immerse ourselves in that frontier and adjust our tradecraft accordingly,"* **John Brennan** [77]

Costs of Administering Information Technology Infrastructure in Intelligence Agencies

In the competition to possess information that would place intelligence organizations at a strategic advantage over their adversaries, intelligence agencies have had to change the way in which they organize and utilize assets and efforts and a fine balance must be struck in order to maximize collection capabilities. Interestingly, technology employed by the foremost intelligence organizations in the world, are built to specifications unrivaled by adversaries. To possess such capabilities, it is no surprise that intelligence agencies have to pay top dollar to the best information technology firms to fabricate customized technology and networks that are expected to be the most secure and efficient in the world.

While the percentage of budgetary allocations earmarked for investment into information technology may be substantially larger than in previous years, these budgetary allocations could be attributed to a long standing culture of intelligence agencies and military services to invest in innovative and more efficient means to conduct activities with superior capabilities in comparison with their counterparts in other nations of the world. An argument which can base its validity on parallel logical constructs employed by revered authors such as William McNeil who have engaged in studies to explain how technological evolution affects the capability of military and societal and societal institutions in existence at the time such developments were invented.

The financial costs associated with the administration of the intelligence product can be quite high for larger intelligence organizations, now that information technology infrastructure has been employed to manage intelligence, as we shall see in chapter 5. For instance, intelligence and security have become much more expensive for organizations such as the NSA, FBI and GCHQ as they utilize larger volumes of information. The NSA maintains an enormous data warehouse in Utah in the US, to cope with the huge volume of internet traffic it collects.[78] Several governments have also embarked on extremely expensive schemes to ensure the safety and integrity of the

---

[76] CESG, *Certified Professionals*, CESG (2014), Available at: http://www.cesg.gov.uk/awarenesstraining/certified-professionals/Pages/index.aspx, accessed 24 June 2014.
[77] Weisgerber Marcus, *Brennan: CIA Must Adapt For Future, Digital Threats*, Defence News(11 June 2014), Available at: http://www.defensenews.com/article/20140611/DEFREG02/306110034, accessed 29 August 2014.
[78] Smith Nathan, *The World Of Signals Intelligence And GCSB In Context*, The National Business Review (2012), Available at: http://www.nbr.co.nz/article/world-signals-intelligence-and-gcsb-context-ns-129503, accessed 5 July 2014.

intelligence they rely on. It has also been speculated that the GCHQ's monthly storage bill is a fairly hefty £11 million pounds[79].

The United States 2013 'Black Budget' released by Edward Snowden shows just how much intelligence agencies are investing heavily in information technology. About 8% of the overall US intelligence budget for 2013 was spent on enhancing cyber security, greater than what was spent on counterintelligence in the fiscal year[80]. According to the IDC government insights report, 22.5% of the US intelligence budget covers Information Technology solutions[81]. In the CIA's 2013 budget, Information technology enterprises had more funding than mission management functions, and the general US community management account revealed that expenditure on Information technology was more than three times larger than expenditure on intelligence analysis[82]. The UK government has also put in place a 650million pound four year National Cyber Security Programme NCSP[83], and around half of the total sum would go to the GCHQ[84]. US Government agencies devote about 15% of their annual budgets to information technology costs, and although information technology security spending continue to climb steadily, the move by US intelligence agencies to cloud based solutions for managing intelligence will make costs of cloud computing rise sharply from $213 million in 2012, to over $541 million in 2017. It is interesting to note that as much as 85% - 91% of information technology security spending goes into paying staff salaries.

The problem here is that, as the mass production of various technologies that can be employed for intrusion and exploitation purposes in cyberspace, such as computers and smart phones, as well as hacking software has made these technologies much cheaper and accessible. Such as eavesdropping and surveillance technology, like laser based eavesdropping software, or satellite phone decryption technologies such as GMR1 and GMR 2 decryption can be bought by adversaries for as little as $2000[85] . Attackers can now embark on opportunistic espionage activities with minimal risk or cost to themselves as a result. Such activities could include the use of bystanders' computers to launch botnet attacks on considerably larger and more sophisticated

---

[79] Mills Chris, *How Much Taxpayer's Money is GCHQ Spending Watching Your Cat-Porn Videos?*, Gizmodo (24 June 2013), Available at: http://www.gizmodo.co.uk/2013/06/how-much-does-all-that-spying-cost-gchq/, accessed 29 July 2014.

[80] FY 2013 Congressional Budget Justification. (2014). 1st ed. [ebook] Available at: http://cryptome.org/2013/08/spy-budget-fy13.pdf Accessed 12 Jun. 2014.

[81] Malykhina, E. (2014). What all that NSA intelligence costs. *InformationWeek*. [online] Available at: http://www.informationweek.com/government/cybersecurity/what-all-that-nsa-intelligence-costs/d/d-id/1113132 Accessed 1 Jun. 2014.

[82] FY 2013 Congressional Budget Justification. (2014). 1st ed. [ebook] Available at: http://cryptome.org/2013/08/spy-budget-fy13.pdf Accessed 12 Jun. 2014.

[83] The UK Cyber Security Strategy. (2014). 1st ed. [ebook] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf Accessed 12 Jun. 2014.

[84] *Ibid*

[85] Williams Christopher, *Satellite Phone Encryption Cracked*, The Telegraph (3 February 2012), Available at: www.telegraph.co.uk/technology/news/9058529/satellite-phone-encryption-cracked.html, accessed 2 July 2014.

intelligence agencies[86]. Information technology, in some ways has put larger intelligence agencies at a disadvantage by making intrusion technologies cheaper and more available for smaller tight knit adversarial groups such as Al-Qaeda, in comparison with the costs of securing and managing information used in large scale intelligence agencies. As a response, Intelligence officers place a premium on the modification of tradecraft techniques to understand and cope with threats and intelligence collection possibilities in Cyberspace, and it is no surprise that intelligence agencies consider in-depth understanding if information technology and appropriate modification of tradecraft employed by its personnel as a strategic advantage, as explained earlier in this chapter.

We can see that the review of intelligence organizational structures, as well as the management of intelligence product, has largely been affected by the emergence of new requirements to enhance productivity in an atmosphere of competition whilst coping with new responsibilities placed on intelligence agencies by policy makers, as well as new threats to peace and security, and new means with which adversaries employ to achieve their goals as a result of developments in information technology. Intelligence functions have been dragged into cyberspace in response to these emerging threats in the cyber realm. As cyberspace becomes increasingly integrated into personal and governmental affairs, and the protection of assets in cyberspace is becoming increasingly important to most entities around the globe, Intelligence agencies have understood the importance of integrating information and communications technology, and some have taken proactive and reactive steps to enhance productivity and protect themselves from the threats associated with the utilization of information technology to aid intelligence functions and organizational needs.

Most of the leading intelligence agencies in the world, because of several considerations have forged relationships with leading technological organizations in order to effectively utilize information technology to achieve their strategic and organizational goals. The next chapter focuses on these relationships between intelligence agencies and industry as well as the benefits and pitfalls that come with it.

[86] Arthur Charles, *Alleged Controllers Of 'Mariposa'Botnet Arrested In Spain*, The Guardian (3 March 2010), Available at: www.Guardian.co.uk/technology/2010/mar/03/mariposa-botnet-spain, accessed 17 August 2014.

Chapter 5-Relationships between Intelligence Communities and Industry

As various elements of intelligence functions, including collection, processing and management are increasingly moving into cyberspace, intelligence agencies are increasingly becoming reliant on information technology to carry out their functions. Information technology has proven to be the most efficient enabler of information sharing between intelligence communities. However, a sizeable amount of functions are increasingly being outsourced to service providers who maintain and upgrade these information technology infrastructures in intelligence organizations.

Information sharing within Intelligence Communities

Information sharing is a critical enabler of integration among intelligence communities. Although intelligence sharing and co-operation has been in existence before the digital age, transnational and decentralized enemies to global security with increased operational and communications capability have necessitated an increase in intelligence sharing and co-operation amongst national intelligence agencies. In the executive summary of a NATO Advanced research workshop report, researchers insist that intelligence sharing between national intelligence agencies must increase in the context of the fight against terror[87]. James Clapper, introducing a US Congressional Budget Justification, emphasizes on the need to implement an information technology infrastructure to enable greater intelligence community integration, information sharing and safeguarding of networks[88]. Little information on the details of intelligence sharing between national intelligence agencies exists In the public domain, however, one could reasonably argue that the ease and speed of intelligence dissemination brought about by information technology would enable already existing intelligence sharing partnerships to be more efficient and reliable, such as the UKUSA agreement which is a multilateral agreement for cooperation in signals intelligence between the United Kingdom, the United States, Canada, Australia, and New Zealand[89].

This is not to imply that obstacles and barriers to information sharing have been completely eliminated today because of information technology. In fact, in most cases, issues such as organizational norms and values, political and bureaucratic considerations, legal barriers and the utilization of incompatible information storage platforms impede information sharing.[90] While information technology has no solution to the non-technical barriers to information sharing, the United States' 2012 National Strategy for Information Sharing and Safeguarding, propose

---

[87] The Changing Face of Intelligence: NATO Advanced Research Workshop – Report. (2005). 1st ed. [ebook] Available at: http://www.sant.ox.ac.uk/centres/Nato_conf_report_0106.pdf Accessed 16 Aug. 2014.
[88] FY 2013 Congressional Budget Justification. (2014). 1st ed. [ebook] Available at: http://cryptome.org/2013/08/spy-budget-fy13.pdf Accessed 12 Jun. 2014.
[89] Wikipedia, *UKUSA Agreement*, Wikipedia The Free Encyclopaedia (2014), Available at: http://en.wikipedia.org/wiki/UKUSA_Agreement, accessed 21 June 2014.
[90] AFCEA Intelligence Committee, *The Need To Share: The U.S. Intelligence Community and Law Enforcement*, AFCEA International (April 2007), Available at: http://www.afcea.org/mission/intel/documents/SpringIntel07whitepaper_000.pdf, accessed 15 August 2014

technical solutions as one of the most effective ways to optimize information sharing capabilities in conditions where information sharing is profitable for the parties involved[91].

The introduction of cloud computing networks is an example of intelligence agencies' confidence in the ability of information technology to facilitate intelligence sharing between agencies and to permit analysts to access and rapidly sift through massive volumes of data not explicitly owned or collected by their respective intelligence agencies[92]. The FBI has taken advantage of information technology and set up fusion centers in the US and abroad adding 31 offices to the 44 already in existence in 2001. The UK has followed suit, establishing a Joint Terrorism analysis centre in 2003, and Germany has also mirrored these developments establishing its own Joint Counterterrorism center in 2004 and since 2007 has been operating a joint anti-terror database which pools information from all federal and provincial security agencies in Germany, by utilizing information technology hardware and software to achieve this feat[93]. The Berne club, which is one of the most important examples of intelligence cooperation, is an intelligence sharing forum between the intelligence services of the 28 states of the European Union (EU), Norway and Switzerland. It currently brings together intelligence chiefs of 27 countries, and has utilized information technology to set up its own communications network[94]. Information technology in itself is insufficient to eliminate barriers to information sharing, as these impediments are of political, strategic and bureaucratic making. What information technology has been able to offer, is the availability of interoperable platforms with which intelligence agencies willing to share information can utilize to enhance the effectiveness of information sharing. However as earlier discussed in chapter 4, one must always be aware of the risks and opportunities inherent in the utilization of information technology platforms to facilitate information sharing.

While the underlying motives behind intelligence sharing between intelligence agencies and industry from an intelligence organization's perspective are plausible, the reliance of intelligence agencies on information technology contractors to maintain and upgrade the capabilities of their IT infrastructure, puts intelligence agencies at a vulnerable position. This is because, although intelligence agencies and contractors may have a symbiotic relationship that profits both parties in various respects, the fundamental motivations of a private enterprise and a government agency are not necessarily mutual. One may ask if the emergence of information technology now placed intelligence agencies at a disadvantaged position in their dealings with

---

[91] The White House, (2012). *National Strategy for Information Sharing and Safeguarding*. Washington DC: The White House, p.15.

[92] Kenyon Henry, *Intelligence Agencies Move Towards Single Super-Cloud*, Breaking Defense (17 December 2012), Available at: http://breakingdefense.com/2012/12/intelligence-agencies-move-towards-single-super-cloud/, accessed 10 June 2014.

[93] Mahadevan Prem, *Intelligence Agencies: Adapting To New Threats*, Eidgenossiche Technische Hochschule Zurich Center For Security Studies (October 2010), Available at: http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-82.pdf, accessed 30 July 2014.

[94] Wikipedia, *Club De Berne*, Wikipedia The Free Encyclopaedia (2014), Available at: http://en.wikipedia.org/wiki/Club_de_Berne, accessed 20 August 2014.

private intelligence contractors. Is it possible that along the line, private contractors now wield too much influence on intelligence systems?

Reliance on the Private Sector

The possession of the most sophisticated and unique technical collection devices is a common characteristic of only the most powerful intelligence agencies in the most technologically advanced States in the world today. Admiral Stansfield Turner acknowledges and expands on the impressive ability of information technology possessed by the United States intelligence community to Survey "almost any point of the earth's surface with some sensor[95]". This indeed places intelligence agencies that possess such technical ability at an advantage in terms of collection ability. However, it is also observable that the most vulnerable states to threats that exploit information technology are the same states that possess such technologies and rely heavily on them. The uncompromised integrity of the information technology infrastructures these service providers utilize are of direct interest to the intelligence agencies they support. Intelligence sharing with industry has become crucial to the performance of intelligence organizations and parallel security capabilities of these supporting contractors are imperative to maintain the integrity of the services these contractors provide. A degree of integration between intelligence organizations and contractors is essential to enable the undisrupted provision of services to intelligence organizations.

As earlier discussed in chapter 4, a considerable amount of intelligence funding is geared towards acquisition of superior information and communications technology, and this increased level of demand has essentially created a market based on the exclusive need of intelligence agencies to possess technological capabilities in excess of the capabilities of intelligence agencies to manufacture them. The influx of information technology into intelligence is at root an irreversible transformation of how agents acquire and use intelligence. The tactics of acquiring, intercepting, disrupting, manipulating and retrieving information from an adversary are dictated at the basic level, by the means (technology) employed in the management of that information. As a result, it is no surprise that intelligence agencies seeking a strategic advantage over adversaries, would need to acquire unique technologies that possess the capability to collect information from an adversary.

This reliance on technology usually results in the acquisition of newer technologies that can penetrate an adversary's information network, or intercept the transmitted information of enemies, in the same vein; intelligence agencies constantly update the defensive capabilities of its information management infrastructure to thwart enemy intrusion. This means that most intelligence agencies are unwilling to buy off-the-shelf information technology hardware and software, but rather prefer custom built and developed products to ensure that information

[95] Shulsky, A. and Schmitt, G. (2002). *Silent warfare*. 1st ed. Washington, D.C.: Brassey's, Inc., p.36.

technology infrastructure in use is impermeable to external exploitation.[96] Intelligence agencies rely on specific communications backbones that they themselves do not have the capability to manage, such as the provision of tailored and secure communications hardware and software. For example, the NSA relies on partnership with AT&T in collecting internet traffic from its Bridgeton facility which plays a role in managing the "common backbone" for all of AT&T's Internet operations[97]. Intelligence agencies have also had to outsource specific tasks that are either too technically complex to undertake on their own, or that would require specific expertise that cannot be replicated effectively within the intelligence community[98].

Details of intelligence spending and sub-contracting are usually classified. However, on investigation of various narratives on the details of sub-contracting by intelligence agencies in the United States, it was uncovered that the Central Intelligence Agency, CIA is involved in funding start-up technological companies which are viewed as potential assets for the agency in the near future. Such as, 3VR which develops analysis software to aid mining of relevant data from huge source information pools, ADAPX involved in the production of collection gadgets exclusively for the CIA, BASIS technology which provides text analytics for various languages and several others[99].

Information technology companies and contractors find themselves in a unique position in the business of intelligence, as they possess proximity to intelligence structure and functions as well as the monopoly of production of intelligence tools. Companies that are involved in the administration of entire telecommunications networks, internet service providers, communications hardware manufacturers, communications software, antivirus manufactures and the like, wield considerable influence on threat perception in cyberspace, and who themselves may have a financial interest in suggesting that threats are sufficiently large, too complicated and immediate and that their products and expertise must be purchased from them without delay[100]. A typical example of this can be seen from, statements made by Eugene Kaspersky, founder of Kaspersky labs "*I'm afraid it will be the end of the world as we know it…I'm scared, believe me*."[101] After Kaspersky lab researchers unearthed Flame (a computer virus which is also referred to as a very

---

[96] Ackerman Spencer, *Snowden Leak Shines Light On US Intelligence Agencies' Use Of Contractors*, The Guardian (10 June 2013), Available at: http://www.theguardian.com/world/2013/jun/10/edward-snowden-booz-allen-hamilton-contractors, accessed 19 June 2014.

[97]Zetter Kim, *Is The NSA Spying On U.S. Internet Traffic?*, Salon (21 June 2006), Available at: http://www.salon.com/2006/06/21/att_nsa/, accessed 4 August 2014.

[98]Rosenbach Eric, *The Role Of Private Corporations In The Intelligence Community*, Belfer Center (July 2009), Available at: http://belfercenter.ksg.harvard.edu/publication/19162/role_of_private_corporations_in_the_intelligence_community.html, accessed 19 June 2014

[99] Hickey Walter, *25 Cutting Edge Firms Funded By The CIA*, Business Insider (11 August 2012), Available at: http://www.businessinsider.com/25-cutting-edge-companies-funded-by-the-central-intelligence-agency-2012-8?op=1, accessed 14 August 2014.

[100] Richards, J. (2014). *Cyber-war*. 1st ed. Basingstoke [u.a.]: Palgrave Macmillan., p.2.

[101] RT, *'End Of The World As We Know It': Kaspersky Warns Of Cyber-Terror Apocalypse*, RT (6 June 2012), Available at: http://rt.com/news/kaspersky-fears-cyber-pandemic-170/, accessed 11 August 2014.

complex cyber-espionage toolkit). This could be termed exaggeration of the actual threat which the virus actually posed. While individual motives for a deliberate over-estimation or sensationalism of threats are debatable, but one cannot eliminate maximization of profits as a possibility. Other more recognizable private intelligence contractors such as SAIC, BAE Systems, Booz Allen Hamilton, Boeing etc actively conduct their business in various parts of the world while simultaneously providing technical platforms for intelligence agencies who are willing to pay for their services.

> *"The growing nexus of intelligence, defense contracting, and cyber security is massive. New enterprises appear every day in response to perceived threats and manufactured demand[102]".* - **Kevin Gallagher**

Questions of Accountability

These considerations eventually bring to light questions of loyalty and accountability. Where do private contractors loyalties lay? What kind of personnel do they employ? Do personnel of private contracting firms have access to sensitive and even top secret information occasionally? All these are questions which relay the concerns of those that are not quite in full support of the proximal relationship which exists between intelligence communities and industry. They raise questions concerning the effect of these relationships between service providers and intelligence agencies on the accountability of intelligence agencies as well as the contractors they employ.

News narratives and articles following disclosures by whistleblower Edward Snowden, suggest that intelligence service providers such as Stratfor, Amesys, VUPEN, and Archimedes Global have actively sold intelligence surveillance and communications technologies to the highest bidder irrespective of underlying ideologies of the political regimes these technologies are being sold to. Worthy of note are allegations against Amesys which sold intelligence technologies to Libya's Gaddafi while he was still in power[103].

The emergence of information technology and its resultant effect on the conduct of intelligence production has also increased the probability of whistle blowing. The sheer number of intelligence contractors working within the United States intelligence community alone, with top level security clearance is alarming. A security clearance determination document published by the United States government's office of the Director of National intelligence, indicate that a total of 582,524 intelligence contractors' personnel had a confidential/secret level intelligence clearance as at 2012, and 483,263 of these contractors were cleared to view top secret intelligence

---

[102] Gallagher, K. (2014). Private Spies Deserve More Scrutiny. *Huffington Post*. [online] Available at: http://www.huffingtonpost.com/kevin-m-gallagher/private-sector-surveillance_b_5171750.html Accessed 19 Jul. 2014.

[103] Gallagher, K. (2014). Private Spies Deserve More Scrutiny. *Huffington Post*. [online] Available at: http://www.huffingtonpost.com/kevin-m-gallagher/private-sector-surveillance_b_5171750.html Accessed 19 Jul. 2014.

documents, bearing in mind that the US intelligence community is still feeling the effects of leaks from Edward Snowden who was just one of these contractors[104].

Since the relevance of private contractors in intelligence cannot be undermined because of the importance of their technical expertise and efficiency, how does one decipher the motivations of employees of contracting agencies and their level of allegiance to the respective governments in which their employers serve? Can they be held to the same ethical standards and values as their counterparts in public service? Considering the fact that the foremost information technology companies take on a more international business model within which fabrication and extraction subsidiaries established in different nations with varying municipal legal infrastructures all across the globe are necessary. Organizational demands occasionally necessitate mobility of members of staff from one country to another, performing sensitive contractual tasks for different governments. Authors such as James Jasper and Mary Bernstein provide apt insights into the various motives of whistleblowers in the light of technical controversies, but commentaries on motivations of individual whistleblowers and spies who emerge from the private sector, fail to consider these external factors. Such as international demand for, and mobility of technical experts who perform sensitive tasks, and not much attention has been given to these factors which occasionally provide the opportunity adversaries need to gain access to sensitive information.

Arguably, the Identification and monitoring of potential whistleblowers and adversaries within a unified governmental structure where employees were held to the same ethical standards, in an environment where leaking of documents was only possible after dissenting employees had gained physical access to documents, was a relatively easier task compared to the identification of whistleblowers and adversaries today, where these adversaries do not necessarily have to be part of the governmental structure, and where access to sensitive documents can be gained from remote sources. As was the case with Hackers known as the "comment Crew" that broke into pentagon defence contractor, QinetiQ's database and are said to have compromised and stolen various secret documents of relevance to UAV functions and software code, from remote locations[105]. Furthermore, the methods and capabilities of whistleblowers as well as the volume of leaks have directly been affected by the technical means with which these whistleblowers carry out their activities. For example, Daniel Ellsberg, who in the absence of modern information technology, leaked 7000 pages of classified documents with the New York Times, and was only able to do so after having physical access to the Pentagon Papers which he made photocopies of, which must have been a physically exhausting and high risk feat at that time. Today, a copy of all those documents could be siphoned from a digital database with a flash drive of just 5Megabytes, measuring 2.5cm by 2cm, in less than 45 seconds. Whistle blowers such as Shawn Carpenter, Edward Snowden and Bradley Manning have all utilized digital media to download and publish

[104] Office of the Director of National Intelligence, (2013). *2012 Report on Security Clearance Determinations*, Available at: www.Fas.org/sgp/othergov/intel/clear-2012.pdf accessed 1 July 2014.
[105]Riley Michael and Elgin Ben, *China's Cyberspies Outwit Model For Bond's Q*, Bloomberg (2 May 2013), Available at: http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html, accessed 19 July 2014.

their leaks.[106] These whistleblowers downloaded many times the volume of data that whistleblowers such as Ellsberg would have been able to accomplish in his era. Whistleblowers also utilize the internet and other technical enablers of information diffusion to publicize leaks and campaign for public approval, while using smart technology to ensure continuous access to the internet and thwart surveillance attempts by intelligence agencies. The relevance of internet privacy and security to the mass public, further exacerbated by sensationalist media narratives which have maintained headlines since whistleblowers such as Julian Assange have achieved prominence in recent years, more attention has been given to these leaks by the mass public and government.

The emergence of information technology and its continuous evolution, has not only increased the importance of information sharing between intelligence and industry, information technology has also provided the infrastructure with which information sharing can be most effectively facilitated. However, vulnerabilities associated with information sharing between intelligence agencies and industry have required intelligence agencies and contracting companies to pursue a uniform baseline standard of protection of information in their possession. The importance of private contractors in intelligence cannot be undermined, as intelligence agencies simply do not have the resources available to manufacture and upgrade cutting edge technology in the capacity that the leading producers of technology can, neither can they identify state of the art technical threats such as viruses, worms etc in the manner that the leading software and anti-virus companies in the world can. However, intelligence agencies must be vigilant and ensure that the perception of inherently technical threats in cyberspace does not put intelligence agencies at risk of having decision making hijacked by those with a deep technical understanding of the threats, and more often than not, have financial interests in exaggerating the perceived threats to promote financial gain from this manufactured demand. The influx of private information technology contractors, has also in many cases granted contractual personnel access to sensitive and top secret information irrespective of the possibility that they may have little or no ideological ties to the government they provide service to, and as traditional vetting processes required for their governmental counterparts may hinder the progress or completion of tasks. Uniform standards of vetting similar to those in the US intelligence authorization act of 2010 for example, must have its jurisdiction extended to apply to its contractors to ensure that personnel in charge of intelligence tasks being sub-contracted are less likely to engage in espionage or whistle blowing, and also to ensure accountability in the event that leaks occur.

Critical analysis of the ability of information technology to enable information sharing, has shown that the utilization of information technology by intelligence agencies to share information in itself cannot guarantee effective sharing of information in an intelligence community, unless socio-political barriers to information sharing have been eliminated independently. Information

[106]Cringely Robert, *Geeks And Leaks: Top 10 Tech Whistleblowers Of All Time*, InfoWorld (20 June 2013), Available at: http://www.infoworld.com/slideshow/106630/geeks-and-leaks-top-10-tech-whistleblowers-of-all-time-220985#slide10, accessed 22 August 2014.

technology can only prove to be an effective enabler of integration in conditions where information sharing is permissible. We have also seen that the utilization of information technology infrastructure to enable information sharing has inadvertently created an opportunity for information technology firms with expertise in the management and upgrading of these sharing platforms, to become relevant in ways that intelligence agencies have become somewhat reliant on them. The resultant relationship between intelligence communities and industry has raised questions of accountability, pertaining to the vulnerabilities and complications that emerge from these relationships and the possible implications for intelligence agencies if these gaps are not sufficiently analyzed and closed.

Chapter 6- Concluding Remarks

The layman's perception of intelligence agencies, processes and agents in recent years, has been tainted by how intelligence agencies and systems have been portrayed in popular culture and news narratives. The mention of any major intelligence agency such as the MI5, SIS, CIA or FBI invokes images of extremely complicated, technologically savvy, large scale organizations, possessing the resources to 'spy' on every single individual on earth, gathering all kinds of information on persons of interest from major business corporations such as Wal-Mart and Google, and are always at loggerheads with media corporations such as the Guardian or The New-York times concerning one fleeting ethical issue or the other. Recent leaks by whistleblowers have also fuelled the imaginations of many observers and the continuous attempts by intelligence organizations concerned, to minimize the damage these leaks can cause to ongoing intelligence operations have been interpreted by reporters and media sensationalists all over the world as cover-ups. Navigating through this seemingly catastrophic landscape saturated with conspiracy theories and exaggerated news narratives of intelligence operations in popular circulation on one hand, and trying to make sense of the heavily redacted, incomplete and restricted circulation reports from intelligence agencies on the other hand proved to be a difficult endeavor for the author in search of the underlying, relatively inconspicuous causes that have spurred the chain of events which we have witnessed in intelligence systems since the dawn of the century.

At first glance, the most obvious common characteristic which Intelligence systems all over the world seem to share is the appearance of numerous private enterprises providing intelligence and defence contracting functions, as well as cyber security products of all kinds to intelligence organizations. The leading intelligence agencies in the world also appear to have significant links with large scale corporations and information technology firms that either fabricate some of the most sophisticated information technology infrastructure in existence today, or gather largest amounts of data concerning the nature of human interaction, financial transactions or social interests.

During the course of my investigation it became obvious to me that these sorts of relationships between intelligence agencies and private corporations are not accidental, neither are they aesthetic. The relevance of private contract contractors in intelligence systems cannot be undermined because of the importance of their technical expertise to intelligence agencies. Based on my assumptions that surely, these private corporations would not have such intricate ties with intelligence systems unless there was some sort of substantial profit to be made from intelligence contracts, I decided to source for information on the profits these contractors make from intelligence communities. Confirming my assumptions, it was discovered that in the United States alone, a hefty 22.5% of the intelligence budget covers information technology solutions and the United Kingdom's four-year Cyber security program NCSP costs about 650 million Pounds.

One of the key questions that baffled me was why intelligence agencies had to churn out such enormous amounts to contractors in the private sector, instead of investing the funds

elsewhere. Apparently, the administration of intelligence product has become a highly sophisticated agenda, as the incorporation of information technology into the administration of intelligence product, means that intelligence agencies can securely transmit larger amounts of information over vast distances, provided they possess the technology to do so. Considering that the ability of intelligence agencies to be able to transmit intelligence to consumers and directives to operations in the field in real time had not always been a necessity, the obvious question was why such a capability has become so crucial for intelligence agencies to possess.

All the symptoms of intelligence systems that have become so heavily reliant on the private sector to perform intelligence functions had become conspicuous at this point. The bond between intelligence communities and the private sector, had become so tenacious, that even though some intelligence contractors could jeopardize intelligence operations by leaking classified documents, notwithstanding the enormous sums of money that had been invested in private corporations, regardless of consequent ethical issues that may arise as a result of these partnerships, intelligence organizations were still enthusiastic about maintaining these relationships with the private sector, there was a need greater than all the consequences, there was a problem, there was an addiction, and all the indicators pointed out one singular underlying factor, Information Technology.

Changing the focus of my analysis to get a clearer picture of why intelligence systems had become so dependent on information technology to the degree that we can see today, required that I observed how information technology has changed several peripheral considerations that affect intelligence directly and indirectly. Understanding how information technology has altered source information, is one of the most important individual ramifications of information technology's influence on intelligence systems. From that starting point, I was able to identify and understand the underlying causes of the problems which are associated with the direction, collection and analysis functions of intelligence.

The increase in the volume of data and the predicament of intelligence agencies to cope with newer forms of data was identified to be a direct result of advancements in information technology, and the imperative need for intelligence agencies to consider data management with analysis and analysts to cope with increasing volumes and types of data. The utilization of information technology to aid collection disciplines to simply collect more data was identified as premature response that merely passes on the bulk of the confusion about the dynamics of information flow, from the collectors of intelligence, to the analysts. The inability of analysts to cope effectively with exponentially increased volumes of information, and resultant intelligence failures because of the omission of vital information are all manifestations of the inability of intelligence functions to cope with data.

The chain reaction effect began to be revealed, after the initial effects of information technology on intelligence, had somewhat culminated to an extent where it became imperative that solutions had to be found. Hence, the influx of information technology personnel into intelligence organizations, the reliance on information technology infrastructure to administer intelligence

product and enable intelligence sharing, and the consequent reliance of intelligence systems on the private sector, are all a series of events that are a result of the direct and indirect influence of information technology on intelligence systems.

Bibliography

Ackerman S., *Snowden Leak Shines Light On US Intelligence Agencies' Use Of Contractors*, The Guardian (10 June 2013), Available at: http://www.theguardian.com/world/2013/jun/10/edward-snowden-booz-allen-hamilton-contractors,

AFCEA Intelligence Committee, *The Need To Share: The U.S. Intelligence Community and Law Enforcement*, AFCEA International (April 2007), Available at: http://www.afcea.org/mission/intel/documents/SpringIntel07whitepaper_000.pdf

Arthur C., *Alleged Controllers of 'Mariposa 'Botnet Arrested in Spain*, The Guardian (3 March 2010), Available at: www.Guardian.co.uk/technology/2010/mar/03/mariposa-botnet-spain,

Association of the United States Army, (2014). *The Army in Cyberspace*.

BBC News Europe, *Ukraine Crisis: Transcript of Leaked Nuland-Pyatt Call*, BBC News Europe (7 February 2014), Available at: http://www.bbc.co.uk/news/world-europe-26079957,

Brynjolfsson E., and Mcafee A., *Big Data: The Management Revolution*, Harvard Business School (October 2012), Available at: http://hbr.org/2012/10/big-data-the-management-revolution/ar ,

Center for Intelligence and Security Studies, *Career Outlook*, The University of Mississippi (2014), Available at: http://ciss.olemiss.edu/students/careers/,

CESG, *Certified Professionals*, CESG (2014), Available at: http://www.cesg.gov.uk/awarenesstraining/certified-professionals/Pages/index.aspx,

Copeland J., (2006): *Colossus: The first large scale electronic computer*, Oxford: Oxford University Press, Available at: http://www.colossus-computer.com/colossus1.html#sdfootnote96sym ,

Corera, G. (2014). The World's Most Wanted Cyber-Jihadist. *BBC News*. [online] Available at: http://news.bbc.co.uk/1/hi/world/americas/7191248.stm

Crane, D. (2002). Fourth Dimensional Intelligence-Thoughts on Espionage, Law, and Cyberspace. *Int'l L. Stud. Ser. US Naval War Col.*, 76,

Cringely R., *Geeks and Leaks: Top 10 Tech Whistleblowers of All Time*, and InfoWorld (20 June 2013), Available at: http://www.infoworld.com/slideshow/106630/geeks-and-leaks-top-10-tech-whistleblowers-of-all-time-220985#slide10,

Cukier K., *Data, Data Everywhere*, The Economist (25 February 2010), Available at: http://www.economist.com/node/15557443 ,

Cuthbertson A., *Ukraine Computer Networks Hit by Russian-based Virus*, International Business Times (10 March 2014), Available at: http://www.ibtimes.co.uk/ukraine-computer-networks-hit-by-russian-based-snake-virus-1439592,

Daintith, John, ed. (2009), "IT", A Dictionary of Physics, Oxford University Press

Dawn S. O., 'Red Storm Rising', *Government Computer News*,

Director, Defense Advanced Research Projects Agency

Directorate of Intelligence, *Intelligence Defined*, Federal Bureau of Investigation (2014), Available at: http://www.fbi.gov/about-us/intelligence/defined

Executive Order 12333. (1981, December 4). United States Intelligence Activities, Section 3.4(a). EO provisions found in 46 FR 59941, 3 CFR, 1981 Comp.

FY 2013 Congressional Budget Justification. (2014). 1st ed. [ebook] Available at: http://cryptome.org/2013/08/spy-budget-fy13.pdf

FY 2013Congressional Budget Justification, National Intelligence Program (February 2012),

Gallagher, K. (2014). Private Spies Deserve More Scrutiny. *Huffington Post*. [online] Available at: http://www.huffingtonpost.com/kevin-m-gallagher/private-sector-surveillance_b_5171750.html

Gutjahr M., *The Intelligence Archipelago*, Joint Military Intelligence College (May 2005), Available at: http://cryptome.org/2014/04/spy-coping.pdf

Hickey W., *25 Cutting Edge Firms Funded By The CIA*, Business Insider (11 August 2012), Available at: http://www.businessinsider.com/25-cutting-edge-companies-funded-by-the-central-intelligence-agency-2012-8?op=1

IBM Global Technology Services, *IBM Security Services 2014 Cyber Security Intelligence*, IBM Global Technology Services (2014), Available at: http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

Information Technology, *Information Technology Strategic Plan*, Federal Bureau of Investigation (2010), Available at: http://www.fbi.gov/about-us/itb/it-strategic-plan-2010-2015

Intelligence.Gov, *We Have Thousands Of Opportunities In All Kinds Of Occupations*, Intelligence.Gov (2014), Available at: http://www.intelligence.gov/careers-in-intelligence/

Joint Intelligence. (2014). 2nd ed. [ebook] Washington DC: Joint Chiefs of Staff. Available at: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

Kenyon H., *Intelligence Agencies Move Towards Single Super-Cloud*, Breaking Defense (17 December 2012), Available at: http://breakingdefense.com/2012/12/intelligence-agencies-move-towards-single-super-cloud/

Lahneman W., *The Future Of Analysis*, Center For International And Security Studies At Maryland (2006) Available at: http://www.cissm.umd.edu/papers/files/future_intel_analysis_final_report1.pdf

Mahadevan P., *Intelligence Agencies: Adapting To New Threats*, Eidgenossiche Technische Hochschule Zurich Center For Security Studies (October 2010), Available at: http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-82.pdf,

Malykhina, E. (2014). What all that NSA intelligence costs. *InformationWeek*. [online] Available at: http://www.informationweek.com/government/cybersecurity/what-all-that-nsa-intelligence-costs/d/d-id/1113132

Matthews W., *Data Surge And Automated Analysis: The Latest ISR Challenge*, Government Business Council (January 2012), Available at: http://www.emc.com/collateral/analyst-reports/the-latest-isr-challenge-insights-gbc.pdf,

Mills C., *How Much Taxpayer's Money is GCHQ Spending Watching Your Cat-Porn Videos?*, Gizmodo (24 June 2013), Available at: http://www.gizmodo.co.uk/2013/06/how-much-does-all-that-spying-cost-gchq/,

Mutegi L., Al *Qaeda Using New Encryption Software To Defy US Intelligence Tracking*, CIO East Africa (22 June 2014), Available at: http://www.cio.co.ke/news/top-stories/al-qaeda-using-new-encryption-software-to-defy-us-intelligence-tracking ,

National Security Agency, *A Reconsideration Of The Role Of SIGINT During The Cuban Missile Crisis, October 1962 (Part 4 Of 4),* National Security Agency (2003), Available at: https://www.nsa.gov/public_info/_files/crypto_almanac_50th/reconsideration_of_the_role_of_sigint_part_4.pdf,

Office of the Director of National Intelligence, (2013). *2012 Report on Security Clearance Determinations*., Available at: www.Fas.org/sgp/othergov/intel/clear-2012.pdf

Pinola M., *Is It Safe To Use An Open Wireless Network?*, About Technology (2014), Available at: http://mobileoffice.about.com/od/wifimobileconnectivity/f/is-it-safe-to-use-an-open-wireless-network.htm,

Richards, J. (2014). *Cyber-war*. 1st ed. Basingstoke [u.a.]: Palgrave Macmillan., p.2.

Riley M., and Elgin B., *China's Cyberspies Outwit Model For Bond's Q*, Bloomberg (2 May 2013), Available at: http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html,

Soderbery R., "How many things are currently connected to the internet to the 'internet of things' (IoT)?" (7 January 2013). Available at: http://forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot,

Rosenbach E., *The Role Of Private Corporations In The Intelligence Community*, Belfer Center (July 2009), Available at: http://belfercenter.ksg.harvard.edu/publication/19162/role_of_private_corporations_in_the_intelligence_community.html

RT, *'End Of The World As We Know It': Kaspersky Warns Of Cyber-Terror Apocalypse*, RT (6 June 2012), Available at: http://rt.com/news/kaspersky-fears-cyber-pandemic-170/

Scott L., and Hughes R, *Intelligence In The Twenty-First Century: Change And Continuity Or Crisis And Transformation?*, Routledge (2009)

Secret Intelligence Service, *SIS Strategy And Values*, Secret Intelligence Service MI6 (2010-2015), Available at: https://www.sis.gov.uk/about-us/sis-strategy-and-values.html,

Shulsky, A. and Schmitt, G. (2002). *Silent warfare*. 1st ed. Washington, D.C.: Brassey's, Inc.

Smith N., *The World Of Signals Intelligence And GCSB In Context*, The National Business Review (2012), Available at: http://www.nbr.co.nz/article/world-signals-intelligence-and-gcsb-context-ns-129503

Solon O., *Cybercriminals Launder Money Using In-Game Currencies*, Wired.co.uk (21 October 2013) , Available at: http://www.wired.co.uk/news/archive/2013-10/21/money-laundering-online

The Bill Tutte Memorial Fund, *How Bill Tutte Won The War*, The Bill Tutte Memorial Fund (2014), Available at: http://billtuttememorial.org.uk/wp-content/uploads/2014/05/How-Bill-Tutte-Won-the-War.pdf

The Changing Face of Intelligence: NATO Advanced Research Workshop – Report. (2005). 1st ed. [ebook] Available at: http://www.sant.ox.ac.uk/centres/Nato_conf_report_0106.pdf

The New Yorker, *Network Insecurity*, The New Yorker (20 May 2013), Available at: http://www.newyorker.com/magazine/2013/05/20/network-insecurity

The UK Cyber Security Strategy. (2014). 1st ed. [ebook] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

The White House, (2012). *National Strategy for Information Sharing and Safeguarding*. Washington DC: The White House, p.15.

Townsend T., Ludwick M., McAllister J., Mellinger A. and Sereno K., *SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project*, Carnegie Mellon University (January 2013), Available at: http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf,

Van Cleave, M. (2005). *The National Counterintelligence Strategy of the United States*. 1st ed. [ebook] Available at: http://fas.org/irp/news/2005/03/ncix030505.pdf

Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.135 Available at: http://dx.doi.org/10.1080/02684527.2012.621604

Weisgerber M., *Brennan: CIA Must Adapt For Future, Digital Threats*, Defence News(11 June 2014), Available at: http://www.defensenews.com/article/20140611/DEFREG02/306110034,

Wikipedia, *Club De Berne*, Wikipedia The Free Encyclopaedia (2014), Available at: http://en.wikipedia.org/wiki/Club_de_Berne,

Wikipedia, *Intelligence Agency*, Wikipedia The Free Encyclopaedia (August 2013), Available at: http://en.wikipedia.org/wiki/Intelligence_agency ,

Wikipedia, *Intelligence Collection Management*, Wikipedia The Free Encyclopaedia (June 2013), Available at: http://en.wikipedia.org/wiki/Intelligence_collection_management#CIA_collection_guidance

Wikipedia, *Intelligence Cycle*, Wikipedia The Free Encyclopaedia (August 2013), Available at: http://en.wikipedia.org/wiki/Intelligence_cycle

Wikipedia, *List of Intelligence Gathering Disciplines*, Wikipedia The Free Encyclopaedia (2014), Available at: http://en.wikipedia.org/wiki/List_of_intelligence_gathering_disciplines,

Wikipedia, *Signals Intelligence In The Cold War*, Wikipedia The Free Encyclopaedia (2014), Available at: http://en.wikipedia.org/wiki/Signals_intelligence_in_the_Cold_War

Wikipedia, *Technology*, Wikipedia The Free Encyclopedia (2014), Available at: http://en.wikipedia.org/wiki/Technology ,

Wikipedia, *UKUSA Agreement*, Wikipedia The Free Encyclopaedia (2014), Available at: http://en.wikipedia.org/wiki/UKUSA_Agreement,

Williams Christopher, *Satellite Phone Encryption Cracked*, The Telegraph (3 February 2012), Available at: www.telegraph.co.uk/technology/news/9058529/satellite-phone-encryption-cracked.html,

Zetter K., *Is The NSA Spying On U.S. Internet Traffic?*, Salon (21 June 2006), Available at: http://www.salon.com/2006/06/21/att_nsa/