IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. VI (May – Jun. 2015), PP 17-24
www.iosrjournals.org

The Cyberspace: Redefining A New World

U. M. Mbanaso, PhD and E.S. Dandaura, PhD.
Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nasarawa State, Nigeria

Abstract: *The cyberspace driven by information systems and the Internet is transforming our environment in extraordinary ways by enabling economic growth and providing new means by which people connect, interact and collaborate with one another. The continuous evolution of components of information and communications technology (ICT); advances in the underlying digital components (core electronics) and the corresponding reduction in costs suggest that the Internet is increasingly becoming more readily available and accessible worldwide. The outcome is that more and more people around the globe will ultimately rely on the effective functioning of the Internet to survive and prosper. This suggests an unremitting upsurge of the population of cybercitizens globally. Most countries no longer take these emerging trends in the virtual world casually. Aside the evolution of digital economy driven by the extensive use of information space or digital knowledge, most countries are working hard to dominate the information space. As the industrial revolution bifurcated the world, so also is the level of exploitation of the vast opportunities on cyberspace bifurcating nation states. This is simply due to the fact that traditional activities of all sorts are increasingly shifting to this new domain. Certainly, cyberspace has become a new focal point for innovations, enterprises, social networking, criminality and warfare. These factors are reshaping and redefining a new world. Most countries that have recognized cyberspace as the fifth domain, have, equally elevated their perception of the domain as an abstract virtual space to a more concrete space with 'physical boundaries'. This paper explores the different levels at which cyberspace is bringing benefits and risks to mankind, and the factors responsible for the widening gap between 'developed' and 'developing' nations.*

I. Introduction

The emergence of the Internet as well as increasing use of information systems have brought about extraordinary changes to human lives. It is transforming many countries' growth, dismantling barriers to commerce, and allowing people across the globe to communicate, collaborate and exchange ideas regardless of the traditional barriers of class, geographical location and time. This merger of the internet, information systems and people, now popularly known as the cyberspace has created a global virtual realm for competitive advantage. Worldwide, governments, businesses, organizations, and individuals are increasingly adopting cyberspace technologies for improved productivity and profitability. It is indeed altering socio-economic activities, security postures, and creating opportunities for innovations and prosperity. It has also expanded the means to improve general governance and welfare of the people globally. Indeed, cyberspace has ushered in better options for research, development and innovations, which ultimately is leading to exceptional economic growth and prosperity, as well as enabling informed societies worldwide at an amazing speed (WEF, 2014).

The wave of innovations resulting from the convergence of information technology and communications (ICT), as well as the evolving mobility and Social Media landscapes are undoubtedly shaping a new world. Equally, the rapid upturn and sophistication of mobile technologies has resulted in swift change in the manner cyberspace resources are presented and interacted with (UK Cabinet Office, 2011). Conversely, advances in core technologies, which have ushered in reduction in technology costs, is making access to the cyberspace increasingly inexpensive and stress-free worldwide. The consequence is that cyberspace population will continue to surge, making it more attractive to all actors and stakeholders. So, there is a transition from the physical world onto the virtual space underpinned by the evolution of computers, telecommunications, responsiveness of people and rapid advances of auxiliary technologies i.e. core electronics (Australian Government, 2015).

The rising importance of cyberspace to sustain economic growth, delivering of governance to the people, assuring national security and the general prosperity is driving accelerated innovations to the extent that nowadays virtually every traditional activity has its digital equivalent. We can now trade online, pay bills, play games, carryout banking activities, and communicate back and forth with individuals, businesses and governments. More so, people can be educated online, collaborate and share resources, conduct workshops, seminars, and conferences online, indeed one can control remote sites leveraging online infrastructure. Essentially, there is hardly any facet of human endeavour that is not domesticated in the cyberspace domain. Behind these growing activities are innovations propelled by research and development on a variety of scales and scope. Of particular interest, is that cyberspace is a free domain, borderless and in theory governed by virtually no one. But this openness of the cyberspace plus increasingly obsession brings fresh risks also. The sensitive

data, networks and systems that make up the cyberspace infrastructure can be compromised or impaired by criminal minded actors from anywhere and at anytime around the world. Thus, the benefits and risks are reshaping the landscape of cyberspace and the way countries perceive its prominence. In other words, cyberspace has presented a new world stage that promises great benefits to mankind, but at the same time portends danger, conflicts and conspiracy with the quest for superiority and dominance by nations within the information space (Bamford, 2013). The capacity and capability driving innovations, the conflicts and conspiracy are factors defining a new world. Again, as the industrial revolution bifurcated the world, the cyberspace is geared to widen the gap between the 'developed' and 'developing' countries.

What is Cyberspace?

The term "cyberspace" is yet to have a globally accepted definition though it is sometimes tantamount to the notion of Internet or the view of a digital virtual realm. Several definitions have emerged from notable organisations such as Central Intelligence Agency (CIA), the National Security Agency (NSA), the Russian-American Cyber Security Summit, etc. (East West Institute and Information Security Institute of Moscow State University). According to the U.S. Department of Defence (Department of Defense Dictionary of Military and Associated Terms, 2010), cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". The Russian-American Cyber Security Summit, on the other hand, describe cyberspace as "an electronic medium through which information is created, transmitted, received, stored, processed, and deleted. Both definitions suggest that cyberspace encapsulates the combination of the internet and telecommunications technologies that allow for the recording, storage, retrieval and transmission of information. This view is further supported by Krippendorff (2010) who argues, "cyberspace results from the human collective ability to articulate possibilities in which technological artefacts are designed, used, and conceptualized". Gibson (1984) on the other hand argues that, "cyberspace has an anthropological dimension, an iceberg of social change, approaching a postindustrial culture". This draws our attention to the fact that cyberspace has ushered in new cultural behaviour to human enterprise, which in turn is altering human experience with new perspectives in focus.

Choucri (2013) adopts a more elastic definition of the cyberspace as a borderless domain "created through the interconnection of millions of computers by a global network such as the Internet which is built as a layered construct, where physical elements enable a logical framework of interconnection that permits the processing, manipulation, exploitation, augmentation of information, and the interaction of people and information. The cyberspace is enabled by institutional intermediation and organization, and characterized by decentralization and interplay among these actors, constituencies and interests". Put all together, cyberspace can be summarised as a space characterized by the people, process and technology elements, bounded by logical territories and inhabited by zeroes (00000) and ones (11111).

This paper argues that cyberspace is redefining a new world packed with uncertainties that span negatively and positively into the realm of human enterprise. We frame the defining factors that cut across opportunities and innovations, vulnerabilities, threats and risks, fast evolving cyber conspiracy, conflicts and warfare as they combine to widening the digital divide or virtual inequality between 'developed' and 'developing' countries.

II. Opportunities & Innovations

Perhaps it may be stating the obvious to note here that the global economy nowadays relies greatly on cyberspace infrastructure as most aspects of daily human existence rely on its effective and proper functioning to survive and prosper. Indisputably, the emergence of cyberspace is expanding opportunities in what today is better known as digital revolution underpinning the concept of information economy (UK, HM Government, 2013; Varian, 2015). An economy "in which knowledge is the primary raw material and source of value" (Business Dictionary, 2015), as opposed to other industries, in which tangible materials are the raw inputs. It is open to debate, that the global status today is defined by a country's capability to sustain a maintainable growth in a highly dependent information economy. The implication is that with the rapid-evolving information economy, countries must reprioritise their industrial strategies with emphasis on the dynamics of cyberspace (UK, HM Government, 2013). Interestingly, the industrial market leaders are changing globally, so much so that the digital divide is widening more and more in developing (struggling) nations. It might be astonishing in the decades to come, that countries, industries, enterprises and individuals apparently unknown to the wider economy may spring up surprises. This is likely because digital revolution has witnessed proliferation of inventions and innovations faster in scale and scope, spanning every aspect of human enterprise than any other revolution. It can be argued that the spur of the proliferation of huge enterprise in this domain is driven by the connectivity between people, technology and information – which in other words is that vitality and power of the cyberspace.

These streaming inventions and innovations are driven by the open characteristics of the cyberspace (or simply, the Internet); researchers, innovators and developers do not have to obtain 'approval' from any authority to further their intuitiveness. Once a piece of invention is accepted in the open cyberspace, it fuels and propagates thousands of other innovations worldwide without recourse to anyone except the ethics of referencing the foundational concepts. Again, it can be argued that what has continued to spur these inventions and innovations is the appetite and responsiveness of the people element. This people component is unarguably one of the critical drivers of the soaring surprises on the cyberspace – positive or negative alike. This is bearing in mind the old economic concept of 'demand and supply' philosophy.

The invention of World Wide Web (www) by Sir Bernets Lee in 1989 changed the landscape of the Internet and arguably, is the catalyst of the proliferation of technological advances in the new virtual world – cyberspace. This Web invention, spurred many innovations in business, government and individual enterprises. The Google model is one of the successful critical enterprises that has not only influenced other business models, but has constantly evolved novelty, combining varieties of technologies into a single interface (Entrepreneurial Insights, 2014). Aside the notable e-commerce storefronts, the Web has continued to influence almost every other technological offering in the cyberspace including the Social Media models, e-Learning Models, Webinars, etc. The emerging industrial Internet to a large extent will be influenced by the power of the Web. Already, companies like General Electric (GE) has made serious inroads in manipulating industrial Internet in railroads, pipelines, power grids, subsea wells, etc. (Varian, 1995). Based on the trends, it can be debated that the industrial Internet will fuel advances in machine intelligence whereby machines will have the capability to interact with each other in more interoperable manner.

Again, the rapidly advancement of the Internet of Things (IoT), predictably, is poised to change the economic and social landscapes, and it has begun to materialise in earnest. Unsurprisingly, the IoT is likely to reshape the business world with huge benefit to the manufacturing sector, homes, security, transportation, production, etc. even as digital wearable are now common place (Internet of Things Europe, 2015). In other words, the IoT will evolve stronger with accelerated advancement and is geared to transform human lives in an unpredictable manner, meaning that in the cyberspace, imaginations are illimitable and opportunities are inestimable. It is foreseeable though debateable that IoT with increasingly device interoperability will escalate the power of information with better interactions in the cyberspace.

Conversely, another critical invention in the digital revolution is the Cloud Computing. The concept of Cloud Computing has further blurred and dismantled any perceived virtual boundaries in the cyberspace. Simply, cloud computing empowers users in the cyberspace to access and use computing resources on the 'need and demand' basis anywhere, and at any time. Given the growing potentials and benefits, governments, businesses and individuals are beginning to cash into its advantages. Consequently, the increasingly adoption of Cloud Computing, predictably, is significantly going to alter the landscape of computing over the coming decades, with huge impact on governments, markets, economies and societies (WEF, 2014).

Another manifestation of innovation is in the Cybersecurity industry, which inevitably is central to the continuity and safety of the cyberspace. Over the years, criminal minded people for a variety of reasons have challenged the safety and security of the cyberspace. The cybersecurity industry on the other hand has managed to keep pace with growing cyber-threats with huge spending on research and developments. It is debatable that countries that have advanced competitive edge in the cybersecurity industry are most likely to dominate cyberspace in many evolving capacities –information economy, conspiracy, conflicts and warfare. Simply put, the tools that appear to provide genuine security controls may be turned into weapons of destruction in the face of conflicts or warfare, undetectably (Bamford, 2013).

Perhaps, what differentiates countries is that those who have recognised the cyberspace as a new world, have equally instituted a structured, calculated and harmonised national effort that is actionable and measurable. The key driver is deep knowledge (creative awareness) of what the new space has got to offer plus the availability of foundational infrastructure that facilitate research, developments and innovations. In this context, just like in the physical realm; every sector in a nation must have a well-articulated and delineated responsibility, specifically assigned to operate within the cyberspace. More importantly, the success factor will be measured by a country's ability to forge a stronger direction and leadership within the domain. In other words, every sector must have a calculated direction, the leadership and the incentive to compete and grow advantageously.

However, it may be argued that developed countries with longer history of ICTs usage and robust infrastructure ultimately have advantage when it comes to research, development and innovations. Yet, the openness of cyberspace supposedly, mediate this gulf as seen in the experiences of countries like India and other emerging Asian countries. In sum, there are infinite opportunities. However, the issue of which country has an edge is a factor of many variables like the nation's leadership direction, priorities, and the appetite to be in the forefront of information economy (UK Cybersecurity Strategy, 2009).

III. Cyberspace: Vulnerabilities, Threats & Risks

The cyberspace is challenged continually by vulnerabilities, threats and risks that have constantly spurred exploitation, conspiracy and conflicts. The increasing level of inter-dependence between physical and virtual components (technology), people and processes is relentlessly opening up unpredictable vulnerabilities, threats and risks. These span across software (viruses, worms, spyware, root kits, exploit scripts, protocol exploits, etc.), hardware (implantation of Trojans: undesired, malicious, deliberate alterations to electronic circuits) and human factor (insider or outsider threats, also from malicious or inadvertent actions or inaction in planning, design, implementation, deployment and operation). Thus, the notion of people in information systems is fundamental because systems are designed by humans, operated by humans and governed by humans; these key actions are subjective to human imperfection. The human factor, unescapably, cut across the life-cycle of providing and operating information systems infrastructure. For instance, when engineers design a system, it unavoidably often contains hardware flaws, software bugs or programming errors, meaning that since systems are products of human beings, mistakes are unavoidable. The consequence is that human error that is inevitably, persistently, can create security 'holes' that may not be immediately perceived.

There is no exploit (or threat) without vulnerability. Threats are continually evolving because of inherent vulnerability that is vary increasingly due to several factors. Simply, vulnerability is the state of visible weakness (exposure of weakness) that can possibly be exploited to carry out attacks or cause harm. Thus, a security breach is as a result of visible weakness found in a system. The unfortunate certainty, however, is that vulnerability in cyberspace infrastructure is likely to be eradicated, no matter the advances in cybersecurity controls. The dialectical relationship between threat, vulnerability and risk is that since, threat results from an exploitation of identified vulnerability in a system, risk is defined by the aftermath of the exploitation of any of such threat into a successful cyber-attack. The fact that criminality in the cyberspace is also creating innovations and opportunities within the cybersecurity industry is another paradox. It has become mice and cat race that no one is really sure who is obviously in the lead. The implication is that cybersecurity service providers are creating business opportunities from vulnerabilities. For instance, the production and sale of malware in one hand, and production and sale of anti-malware in the other hand in the past two decades, arguably, have generated multibillion dollar businesses around the globe (ITU, 2008).

From the foregoing, it is evident that the interplay of cyber opportunities, negative or positive has strong elements of evolving vulnerabilities, threats and risks. What is clear in this context is that countries who aspire competitive lead in the vulnerability landscape and its exploitations can as well take undue advantage of others in the race for digital supremacy. Consequently, it can be argued that vulnerabilities, threats and risks are factors that are equally underpinning the undercurrents of the new world.

IV. Cyber Warfare

Unlike in the last decade, cyber warfare is no longer strange or puzzling. With the emerging reality of state sponsored attacks on the cyber infrastructure of other nations, the entrenchment of the relatively new phenomenon of cyber warfare in human lexicon can hardly be contested. Cyber warfare from this perspective is an extension of the mutual web of conspiracy and sabotage between and among nations in conflict. In a cyberspace which is intrinsically challenged by uncertainties, State actors are unsatisfied with building defensive strategies alone but working effortlessly to build offensive capabilities that can assail their adversaries whenever desirable. Exacerbating this challenge is that no individual, organisation or government can provide an accurate profile of the threats and vulnerabilities evolving and emanating thereof. Consequently, it will appear that the raging war at cyberspace domain will be hard to win due to several factors that are too hard to predict. The factors that interplay and create the vulnerability landscape, which could be exploited by State actors against other States are inherently uncontrollable, arising, as more advancements are made in the technology arena. What has informed State actors is the same long tradition of world's conspiracy and conflicts with taxonomy such as infiltration, sabotage, espionage, war, etc. as majority human activities shift to the new realm. As put by Ranger, (2015) "after years on the defensive, governments are building their own offensive capabilities to deliver attacks… It's all part of a secret, hidden arms race, where countries spend billions of dollars to create new armies and stockpiles of digital weapons." What is key to all these exploits is the capability to latch onto the inherent vulnerabilities within the cyberspace through intensified and structured formal research and development – searching for high profile vulnerabilities, which are hard to discover. That is, the strength of State actors lie in their skills and competence in discovering high-profile zero day vulnerabilities. The US, and other superior cyber-powers have already carved a career in this area with highly-profiled Vulnerability Researchers.

The first attack, allegedly, arose international awareness, was the assault on Estonia, a Baltic State, with estimated population of about 1.3 million (BBC, 2007). Estonia, with claim of being the most internet-savvy State within the European Union, highly-dependent on cyber infrastructure, was seriously hit by sustained coordinated attack against government and critical private institutions' websites causing heavy disruptions. This attack was remarkably an indication of potentially State backed conspiracy that could halt companies or even paralyse a State, as Russian State was suspected to have supported the attack (Ranger, 2015). Another publicly

acknowledged cyberweapon or compromise masterminded by State actors i.e. Stuxnet, yet to be fully understood by military strategists, cyber security experts, and even political decision-makers in most countries, raised world attention (Bamford, 2013). Stuxnet, the cyberweapon that attacked the Iranian nuclear facility at Natanz is now the first acknowledged cyber incident within the scale and scope of cyber warfare. The mastery of the design and how it was able to undermine all security measures by the Iranians even against their computer networks that are isolated from the Internet network by a technology called air-gap continues to baffle cyber experts globally (Langner, 2013). Bamford, (2013), alleged that it was in 2012, anonymous source, revealed to The New York Times that America and Israel were responsible for the security breach in Iranian nuclear facility. The work that cumulated to Iranian attack, apparently, was a long years of US military's effort to develop offensive capabilities that is not only able to defend the US cyberspace but to equally batter its enemies Bamford, (2013). The Stuxnet case, undoubtedly, demonstrated long period of professional and expertise development that attests to the undiscoverable nature of the weapon.

There is an indication that the American National Security Agency (NSA) conceived "US Cyber Command" as far as the year 2000 to build US cyber warfare effort. According to Bamford, (2013), the US fears that "cyberweapons are as crucial to 21st century warfare as nuclear arms were in the 20th". The US Cyber Command force is over 14, 000 personnel with over 13 formidable cyberattack teams declared Bamford, (2013). The US sets aside $4.7 billion annually for developing cyberwarriors including high-profile expertise development, encouraging many doctoral degree studies in the various field of cyberspace (Bamford, 2013).

Conversely, the aftermath of Stuxnet incident was Iranian ferocious response. It was assumed that Iran hatched its counter on Saudi Aramco, an energy company and RasGas, the Qatari natural gas facility as well as several denial-of-service attack targeted on American interest (Perlrothoct, 2012). The Stuxnet sage also prompted Iran to form its Cyber Command, in attempt to building a tough Cyber force that is capable of inflicting damage to its foes (Langner, 2013).

In a similar development, China, alleged, has continuously invaded US cyberspace, increasingly, exploiting vulnerabilities in some military and government information systems and networks (Capaccio, 2012). Capaccio, (2012), argued that most of the Chinese attacks are highly customised and specialized, with a high success rate targeted to vital military installations vulnerable to industrial espionage. Conversely, China assumed to be a deliberate contender of the US in the cyberspace, is building its cyber warfare paramilitaries, especially understood to be targeting US expertise and specialisations in communications, electronic warfare and networking skills. According to the US- China Economic and Security Review Commission, China's cyber capabilities is a worrying concern to the US, which fears that at any given point, "China's persistence, combined with notable advancements in exploitation activities pose growing challenges to information systems and their users" (Capaccio, 2012).

Similarly, the December, 2014 attack on Sony Pictures Entertainment, alleged committed by North Korea is another level of magnitude of attack that is capable of provoking cyber warfare. The perpetuators of the Sony assault revealed embarrassing documents stolen from their exploits - private and personal sensitive information of employees of Sony amongst other critical data were compromised. The Sony attack raged public uproar in the US and US government was perturbed by the incident. North Korea, undoubtedly, is another strong contender and aggressor in the cyberspace with tracks of several coordinated attacks on South Korean interest. It has continued to assemble sophisticated cyber army for its offensive and defensive strategies. The UK, is not left in the cold, according to its Defence Secretary, Philip Hammond, "we will build in Britain a cyber-strike capability so we can strike back in cyberspace against enemies who attack us, putting cyber alongside land, sea, air and space as a mainstream military activity" (Ranger, 2014).

Debatably, these few examples and many others not highlighted here, are earlier warning that cyber conspiracy and conflicts capable of provoking a full scale conventional war or cyberwar or combination of the two, is no longer uncertain, however, the uncertainty, is when, and those who will be drawn to the cyber-battle fields. We argue that the widening global divide induced by the cyber revolution is yet to be recognised by most of the developing nations encumbered by several domestic problems and cultural issues. These local issues, unavoidably, have continued to influence their poor perception of emerging trends. With the growing scale of conspiracy and conflicts, it is becoming increasingly critical that every nation State must strive to develop the capacity just as in the physical realm, to respond proportionately in the event of cyber conflict. This strengthens our argument, the need that part of the State requirement will be to develop the capability to deter the capacity of other States from conducting attacks against her interests.

V. Widening The Global Divide

Arguably, our dependence on digital infrastructure, instantaneously, is challenging the national and social fabrics, to the extent that sovereignty of many nations is potentially at risk. The emerging virtual inequality between countries in the cyberspace, is influenced by many intriguing factors. It is not only limited by mere accessibility to and use of information and communication technologies (ICTs) or the much touted 'digital

divide'. The mere gap in access to basic telephone and Internet services has significantly reduced and is anticipated to diminish further in the next few decades. For instance, Nigeria, which had same number of internet users (55 million) like the United Kingdom in 2012 witnessed 14% leap from 55milion to 62.4 million internet users by 31st December 2013 (Ifebhor, 2014). This is by far above the UK statistics which showed a marginal increase of two million users in 2013 (from 55 to 57 million). According to Ifebhor (2014), Nigeria has experienced an astronomical 143% growth in internet usage for the past ten years and maintained its lead in the growth of the number of internet users in Africa. With an estimated population of about 177 Million people, Nigeria had a total of 67,319,186 Internet users as at December 31, 2014. This represents 38.0% of the population. It can be debated that this growth is powered by the people element and responsiveness, but the next level- having the cyber power (Betz D. & Stevens T., 2011) requires more resources, understanding and political will to deepen the benefits in respect of evolving creation of wealth through innovations and enterprise (UK, HM Government, 2013).

Though the gap in accessibility to the Internet and, particularly, access to broadband is diminishing, the elements of capacity and capability that is revolutionizing opportunities on the cyberspace is widening significantly. The perception of countries and regions, especially how individuals, businesses, economies and societies are able to take advantage of new evolving ICT platform is redefining a new world order. The blurring line between those who create, provide, export and equally consume, and those who import and consume, is astonishingly glaring in this highly disputed domain. The important structural differences between cyber-developing countries and those countries who are struggling to get grip with cyber reality are beginning to emerge as to how cyberspace is perceived. Most tagged countries under the notion of 'developing or third world countries' are without clear direction in terms of strategic realities of the new virtual world. An argument can be put forward as to what is responsible for modern world inequality that the digital revolution is also creating (Acemoglu & Robinson, 2012).

Targowski (1996) opines that "Industrial Revolution proudly changed the rural character of the economics of Europe and United States", it can be argued that the open cyberspace share equally the same characteristics but this time at much more global magnitude. He argues that the Industrial Revolution brought drastic change in the world economies for three main factors: "a thriving commercial class, growing markets, and increasing population"; similar factors are also driving the digital or information revolution powered by the cyberspace. The same reason the world saw a clear demarcation, of which the aftermath is the notion of 'developed and developing' countries, is about to repeat itself, especially in the African continent where good political leadership is still a huge challenge.

Perhaps the 'ignorance hypothesis', which claims that poor countries are poor because their leaderships unwittingly implement extractive economic policies, as argued by Acemoglu & Robinson (2012), may not apply fully in this context. The paradox here is that cyberspace is 'open' as opposed to the industrial revolution that evolved in utmost secrecy. Thus the ignorance theory contrasts the case of better-informed society that is core to cyberspace influence. The institutional differences and constraints manifest significantly in the leadership style of 'poor' nations, which invariably can explain the emerging digital inequality. Asides the potent infinite opportunities and benefits oscillating to the advantage of developed economies, leaderships of emerging economies lag behind in forging strategic directions that can engender positive changes in their countries. The political structure and democratic institutions are extractive to the extent that the morale and sensitivity required to create a just and sustainable society is absent in most of the 'emerging' or 'under developing' cyber-world. According to Acemoglu & Robinson (2012), "intimately linked to technology are the education, skills, competences, and know-how of the people acquired in formal school". This perhaps explains the sustained efforts by most cyber-savvy world in addressing the cybersecurity skill gaps (Bamford, 2013) (UK Cabinet Office, National security and intelligence, 2013). In a deliberate effort to maximize the gains of the cyberspace, most cyber-savvy States have enacted multifarious legislations and established several new structures to facilitate and oversee the evolvement of cyberspace and its governance.

For instance, the UK has Office of Cyber Security and Information Assurance (OCSIA) created to "provide strategic leadership across government for cyber security issues" (UK Cabinet Office, The UK Cyber Security Strategy, 2011). OCSIA constantly reviews cyberspace issues to advance UK cyberspace interests. The UK in this regard has quite significant number of legislation and initiatives cutting across spectrum of cyberspace domain. In contrast, a country like Nigeria has just signed into law, the Cybercrime bill 2015, on May 2015 as the only substantive legislation on cyberspace. The Cybersecurity or Cybercrime bill drafted in 2011 was toasted in the National Assembly for some years, which supports our earlier assertion on political immaturity. Equally, although, Nigeria has developed and launched National Cybersecurity Strategy and Policy, there is no clear direction on how the Strategy can be implemented and monitored, which in our opinion, may make the document unproductive. Perhaps, the way to argue these political and structural differences in developing countries is lack of foresight on the part of political leaders, who shy away from the power of knowledge to put national priorities in proper perspective. In Nigeria, the Office of the National Security Adviser (ONSA), that currently handles

cybersecurity issues, arguably, has made some effort in championing the cause of cybersecurity. However, statutorily, ONSA does not have the current skill-sets and expertise, to proportionately advance the cause of cyberspace in Nigeria. The reality is that ONSA is inadequately staffed and lacks in-house expertise to provide the level of leadership direction on cyberspace domain. Invariably, what should be ideal, is for ONSA to remain the focal point, provide oversight functions but then empower relevant elements of government, and the private sectors to take active engagement on the cyberspace. In peculiarity, the US and UK, notably, have full-fledged dedicated institutions with relevant expertise and professionals in charge of cyberspace realm, augmented by efforts of security and intelligence community. Besides, these countries have identified the huge cyber skills dearth, despite their long history of usage of ICT, and currently, addressing the same through deliberate, formal and structured education. This is not the case in Nigeria encumbered with political senility and status quo syndrome i.e. expertise and specialisations are implausible sort after. The general notion is 'having something is better than having none'; in essence, 'we make do with what we have', irrespective of the knowledge gap in the specific area space. Conversely, the improvised professionals or self-made cybersecurity practitioners attempting to engage themselves in the affairs of cybersecurity will obviously results to wrong diagnoses followed by wrong prescriptions. This can be likened to taking a Navy Captain to a fighter jet, he can seat comfortably on the cockpit, ramble the engine, but cannot fly, though he is seen to be doing something. The fact is that cyberspace is highly technical, to the extent that foundational knowledge about the nuances of it, is required to correctly provide the kind of leadership direction that will yield tangible results. The right captains must be put in place to critically drive the affairs of this new domain. Moreover, the advancement of the cyberspace requires greater input from the academia through formal research and development, which is grossly absent in most of these developing States. Again, in Nigeria, there are no indications of any known Research Institutes or Centre of Excellence emerging in the nearest future, which supposedly, should be the hallmark of active engagement on the cyberspace.

Unlike the US, the UK and most of the other cyber-developing nations, who have deliberately commissioned research efforts in the many areas of cyberspace, of which, the outcome is driving innovations and inventions on the cyberspace. These challenges are perhaps not peculiar to Nigeria alone but indeed present in different dimensions in most developing countries. Undisputedly, several factors are responsible for the widening digital gap, however the most devastating is absence of informed leadership in these developing countries, which can create requisite economic institutions and structures capable of creating the necessary incentives that can bolster the desired developments. Incidentally, similar factors also that barred the developing countries from benefitting from the industrial revolution, is again playing out. Therefore, it appears history is repeating itself again with only few countries able to effectively leapfrog the gap.

VI. Conclusion

So far this paper has argued that the merger of computer technology, virtual reality, networks, telecommunications, and people element has created a new world, which need as much attention by governments as they do their territorial spaces. According to Benedikt (1991), the cyber world "is indifferent to physical constraints, a world without a place which is in constant state of change". This new world or the era of cyberspace is being redefined by convergence of factors that are shaping its operations and activities but creating a centre stage for the definition of the new 'world power', economically, and enabling transnational State dominance. Consequently, the way countries perceive the virtual world influences their actions and strategic interests. Also significant is the understanding that as much as this 'new cyber world' is rapidly changing the world in many positive ways, part of the vitality of its evolvement is the perils that come with its revolution and how it is constantly influencing innovations and enterprise. The surge in migration of every traditional activities into this sphere, and the increasingly over-dependence by human beings on its proper functioning is making the cyberspace a new centre stage for international conspiracy and conflicts. Opportunities are infinite; nations are creating enterprises and wealth, striving to dominate the digital space in all facets of life similar to the physical world stage. Possibly cyber conflicts within the scale of war have be predicted. Illegal cyberweapons are now sold like physical arms in many underground online markets. However, the most disturbing is the fact that there is no international body responsible for oversight and regulation of the excessiveness of evolving cyberweapons trade. The growing large consumers of cyberweapons, now free for all, for those willing to pay huge sum of money is informing another global concerns.

Cyberspace is redefining a new world characterised by the ability of a State to compete advantageously with reasonable capacity and capability to excel in it. Countries are striving to have strong productive capacities in cyber products and services, especially in cybersecurity, which is a vital component in both defence and offensive strategies. The real front-runners are still the developed nations, and the differentiator in this case remains the informed leadership issue. Our conclusion is that leaders of developed nations have identified the criticality of the new world and are in the forefront of its advancement in all directions. These leaders have gained insight of the nuances of cyberspace and are convinced, so they have taken proactive steps to protect the

open cyberspace, defend it and bourgeon on it equally as they have with the physical world. For instance, the US, Britain, European countries, Russian, China, etc. through executive orders have extensive in-road and significant influence already on the cyberspace. They have shown leadership on the cyberspace by their actions – multiple strategies and initiatives in different facet of cyberspace domain that is setting the altitude for public and private sectors evolvement. In contrast, absence of political maturity, vague understanding of the new domain, and crowded domestic issues are responsible for slow adoption of strategies to harness the immense potentials of the cyberspace by developing nations. Sadly, as industrial revolution demarcated the world, so is the cyberspace fast bifurcating our global space.

References

[1]. UK Cabinet Office, (2011), The UK Cyber Security Strategy, [online], Available from:www.cabinetoffice.gov.uk, [Accessed:25/03/2014]

[2]. UK Cabinet Office, National security and intelligence (2013). Progress against the Objectives of the National Cyber Security Strategy. [online] Available from: https://www.gov.uk/government/publications/national-cyber-security-strategy-2-years-on. [Accessed:15/06/2014]

[3]. Steve Ranger, (2015), inside the secret digital arms race: Facing the threat of a global cyberwar. [online] Available from: http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/. [Accessed:25/04/2015]

[4]. BBC, (2007), The cyber raiders hitting Estonia, [online] Available from: http://news.bbc.co.uk/2/hi/europe/6665195.stm. [Accessed: 25/04/2015]

[5]. James Bamford (2013), God of War (The Secret War), Wired USA

[6]. Raph Langner, (2013), The Stuxnet's Secret Twin, Available from: http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/, Accessed: 23rd September, 2014

[7]. Nicole Perlrothoct, (2012), In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back, Available from:http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=1&_r=2&, Accessed: 25th April, 2015

[8]. Anthony Capaccio, (2012), China Most Threatening Cyberspace Force, Available from: http://www.bloomberg.com/news/articles/2012-11-05/china-most-threatening-cyberspace-force-u-s-panel-says, [Accessed: 25/04/2015]

[9]. World Economic Forum (WEF), 2014, The Global Information Technology Report 2014

[10]. Internet of Things Europe (2015) Internet of Things Connected Objects [Online] Available from: http://www.internet-of-things.eu/ [Accessed: 25/04/2015]

[11]. Australian Government, (2015) Future Cyber Security Landscape: A Perspective on the Future, Available from: http://www.dsto.defence.gov.au

[12]. Uk HM Government, (2013), Information Economy Strategy: Industrial Strategy: government and industry in partnership Available from: www.gov.uk/bis

[13]. ITU (2009) Understanding Cybercrime: A Guide For Developing Countries, 1211 Geneva 20 Switzerland

[14]. Liviu Arsene, China's Cyber Militia Threatens US Cyberspace [Online] Available from: http://www.hotforsecurity.com/blog/chinas-cyber-militia-threatens-us-cyberspace-4313.html, [Accessed: 09/03/2015]

[15]. Business Dictionary, (2015), Available from: http://www.businessdictionary.com/definition/information-economy.html, [Accessed: 25/03/ 2015]

[16]. ITU, (2008), ITU Study on the Financial Aspects of Network Security: Malware and Spam

[17]. Department of Defense Dictionary of Military and Associated Terms, joint publication 1-02 ed. (2010), page 83, by Office of the Joint Chiefs of Staff, accessed June 4, 2012, last modified March 15, 2012, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[18]. East West Institute and Information Security Institute of Moscow State University, The Russia - U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, ed. Karl F. Rauscher and Valery Yaschenko, Issue 1

[19]. Klaus Krippendorff (2010) The Growth of Cyberspace and the Rise of a Design Culture, workshop on Social Theory and Social Computing at the University of Hawaii, Honolulu, Hi

[20]. Nazli Choucri, (2013) Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences, World Social Science Forum (WSSF) 2013 Montreal, Canada

[21]. UNCTAD (United Nations Conference on trade and development), 2013, The Cloud Economy and Developing Countries, Information Economy Report 2013

[22]. INFOSEC Institute, (2013), China vs US, cyber superpowers compared, Available from: http://resources.infosecinstitute.com/china-vs-us-cyber-superpowers-compared/ Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao (2011),The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

[23]. Steve Ranger, (2014), Inside the secret digital arms race: Facing the threat of a global cyberwar [online] Available from: http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/. [Accessed:25/04/2015]

[24]. kennedy Ifebhor, (2014) Nigeria Overtakes UK in Internet Access –digitXplus Report [online] Available from: http://nigeriacommunicationsweek.com.ng/telecom/nigeria-overtakes-uk-in-internet-access-digitxplus-report. [Accessed: 23/02/2015]

[25]. VARIAN H.R. (2015) The Information Economy: How much will two bits be worth in the digital marketplace? [Online] Available from: http://people.ischool.berkeley.edu/~hal/pages/sciam.html [Accessed:23/02/2015]

[26]. Entrepreneurial Insights (2014) Google's business model [Online] Available from:http://www.entrepreneurial-insights.com/google-business-model/ [Accessed:23/04/2015]

[27]. Business Model Innovation Matters (2015) Understanding Google Business Model[Online] Available from: http://bmimatters.com/2012/03/29/understanding-google-business-model/ [Accessed:05/05/2015]

[28]. ACEMOGLU D. & ROBINSON J. A. (2012) Why Nations Fail: The Origin of Power, Prosperity, and Poverty, Crown Business, New York

[29]. BETZ, D & STEVENS T (2011) Cyberspace and the state: towards a strategy for cyber power. Abington: Routledge

[30]. Benedikt M. (1991) Cyberspace: First Steps , MIT Press, 1991

[31]. Targowski A. (1996) The Evolution of Cyberspace, IRMA International Conference, IT Management and Organizational Innovations, 1996, pp333-338.