

African Renaissance

ISSN: 1744-2532 (Print) ISSN: 2516-5305 (Online)

- Indexed at: EBSCO, ProQuest, J-Gate and Sabinet
- Accredited by IBSS and SCOPUS

Vol. 16, (No. 3), September 2019
pp 65 – 88

Post humanism, Virtual Warfare, and the Defence Preparedness of Nations: A Case for Africa's Readiness

Jegede, Ajibade Ebenezer

*Department of Sociology
College of Business and Social Sciences
Covenant University,
Ota, Ogun State Nigeria
Email: Ajibade.jegede@covenantuniversity.edu.ng*

Okorie Nelson

*Department of Mass Communication
College of Business and Social Sciences
Covenant University,
Ota, Ogun State Nigeria
Email: nelson.okorie@covenantuniversity.edu.ng*

Olusola Oyero

*Department of Mass Communication
College of Business and Social Sciences
Covenant University,
Ota, Ogun State Nigeria
Email: olusola.oyero@covenantuniversity.edu.ng*



Olowolafe, Kemi
Department of Psychology
College of Leadership Development
Covenant University,
Ota, Ogun State Nigeria.

Abstract

Background: The era of posthumanism has signalled a shift in the modal appraisal of global wars with attendant wave of restocking of defence arsenals with high tech virtual compliant weaponry. Despite this development, most nations in Africa are yet to grapple with the fact that the world is in the virtual warfare phase of development, which calls for a change in orientation.

Methods: The study adapted a model developed in Global Defence Perspective (GDP) in lieu of survey data. Here the research assesses the placement of countries along the hierarchy of defence spending for the purpose of analysis.

Results: The authors identified acute corruption, bad leadership, appendages of belligerent nations, policy discontinuity, excessive reliance on mono-economy, declining industrial potentials, infrastructural decay, massive unemployment, weakened economies, and a host of other factors as barriers to defensive investment in Africa.

Conclusions: The discourse appealed to national administrators in Africa to rise up in order to checkmate the probable challenges that are visible through the threat or violence associated with cyber warfare.

Keywords: *Posthuman, Science, Cyberwarfare, Global, Attack, Virtual, Risk*

Introduction and Problem Statement

The mythology relating to the potentials of science taking up the form of human flesh, substituting and performing human roles has been the ambitious project of the techno-scientific community for ages. Science in its highly envisioned stage is akin to transcendentalism of spirito-humanism. This state is currently depicted by the production of human-like computer machines and gadgets which have some level of rationality

or emotional senses (operator-less networking) that are substitutionary of human input or labour and yet ironically viewed as the elongation of man (Mahmud, 2015:9; Fukuyama, 2002:172). It is a disembodied mind encapsulated in machines relatively independent of man yet produced by man. Scientific feat today exists beyond all known comprehension in the technological age with its non-embodied form arriving within the shores of post-humanism in the medical sciences, commerce, and warfare campaigns. Interestingly, it consists of the embedding of combative intelligent forms, bodily encapsulated into computerised artefacts and fashioned with the view of manipulating such configuration for both subtle and revolutionary warfare and with the exclusion of man's bodily inputs.

Computer machine automatically becomes a constructionist body outside the materialist body of man. This stage denotes artificialism, a concerted alteration of reality or formidable improvement that is engaged with the aim of performing optimally and to the disadvantage of other competitors (man as both producer, marketer, and instrument of war) that preceded our scientific existence. The tendency towards artificial life, synthesised intelligence, and telepresence is eroding the barrier between 'natural' and 'human-made' phenomena. It is not at all unfeasible to think of ourselves communicating with a synthetic intelligence on another planet, swapping samples of bio-digital artificial life through interplanetary cyberspace (Pepperell, 2003:161).

This condition presents the increasing alienation of man to his world and is thus further supported by formidable estrangement by reason of mysterious events promoting man's excommunication in the age of virtualism. Weaver (2010:12) describes Posthuman condition in this era as the merging of humans and machines in order to enhance or improve human capabilities. Besides its positive contributions to quality of life, it is equally deemed problematic in all its ramifications. It ushered in a de-emphasis on bodily materiality with unprecedented vulnerabilities in the wake of cashless economy and computer-borne warfare in its varied dimensions. It is grossly admissible of anti-human nature: greed, fraud, destructive practices and it also nurtures the likelihood of a collective or mutual extinction. Just as it promotes virtual-related crimes, it also perfected the art of using the virtual space to intimidate, obliterate and at the extreme, annihilate fellow human being alongside its capability of revolutionizing the theatre of modern conventional wars.

This condition in the context of virtual warfare therefore implies the potentials of either state or non-state actors communicating via or utilizing the internet as a potent force for stealing classified information that is central to the functioning of a sovereign state or corporate entity and the adaptation of such medium towards the delivery of aggression through sending either friendly or unfriendly cues to other nations or other stakeholders within the cyber-distance of their previewed enemies or other areas of intended operations. The endowed capacities of state actors to assess and re-assess the unfolding cyber global events will be determined to a large extent by the nature and magnitude of response enablers. These enablers are not equally distributed among both state and non-state actors. In the age of virtual warfare, the internet represents the extension of natural human capabilities for socio-economic transformation, yet it became the source of enhancing quality delivery of negative advances against partners in the global community, dislodgment of mutual security and the disempowerment of the natural man. Virtual objects now literally appear to rule far above the spontaneity of man in a parallel fetish manner thus corresponding to Marx fetishism of commodity (Chandler, 2013: 519). It is a negation to the intent that virtual warfare obfuscated or obliterated the extant laws of war (Goldsmith, 2013:129).

Attention on the looming danger of the internet-borne warfare has been drawn in several research findings especially as social relationships are now becoming massively represented in the virtual environment (Jegede, 2016a; Jegede, Adejuwon, Olowookere and Elegbeleye, 2016; Jegede, Ajayi and Allo, 2016). In this unfolding scenario, it is most interesting to know that while most of the advanced capitalist nations are concertedly mass producing, procuring and stockpiling cyber compliant weaponry for the purpose of warding off probable threats of modern virtual warfare, pathetically, the Third World nations in sub-Saharan Africa are pre-tentiously ignoring the realities of this communicable security vulnerabilities looming in the international arena. Can one attribute this to their position in the classificatory schema of the world-ranking economies or racial nomenclature? Irrespective of the reason, it is foolhardy to neglect the looming danger infectible by reason of one's participation in the virtual environment.

The obscure reason for this apathetic development is remotely baffling since the communicable danger inherent in its neglect is quite costly. This danger has futuristic implications; just as the disruptive

nature of cyber-warfare technologies is capable of transferring enormous power to countries that are flexible in commuting their resources into its acquisitions and utilization for both offensive and defensive operations (Hughes, 2009). Virtual warfare is real and its consequences bear enough potency to destabilize both physical, material and human components of any given society. A wake up call at this instance is its urgent recognition and effortfully bracing up to arrest its growing tide globally. In essence, the overall advocacy pursued vigorously in this discourse is both informative and provocative of action from the state of docility especially in the face of daunting challenges promotable by virtual threats. A positive response in this regard is important to allaying the fears of unequal access to the buffers against virtual warfare attacks or onslaughts and the adoption of strategies that are preventive of vulnerabilities such as loss of humanity and other state of affairs most capable of entrenching the subserviency of a region comparatively to the others in the long, non-foreseeable future.

Objectives and Method of Study

The paper utilizes publicly available resources for the analytics of global defence spending. This is extrapolated to establish how spending has increased security or promoted global vulnerabilities. The data was adapted for comparative analysis of intercontinental committal of GDP resources to the procurement of computerized compliant arms and armaments in response to the rising spate of security concerns globally. Nations invest in few instances to tackle intimidating territorial defence spending often brazenly displayed by other nations. It adapted a model developed in Global defence perspective paper (2017) in lieu of survey data. Here the research assesses the placement of countries along the hierarchy of defence spending. Gartner, (2017), earlier disclosed that security risks drive growth in overall security spending. This enabled the reclassification of Sub-Saharan countries along their levels of committal and invariably their responses to the looming threats of cyberwarfare.

Challenges of high modernity: A theoretical discourse on cyberwarfare

The epistemological leaning of discursive cyber conflict and conflagration mostly pervading the global virtual environment lies in risk analysis-

sendemic in the theory of modernity. There is a general agreement that we have been living in a risk society for the past 20 years (Jensen, 2008:757). The theory presents a negative dimension of the constitutive roles of science which is often ignored when the eulogy of scientific breakthroughs is being aired. Several scholars immensely contributed to this school of thought. Although, few of the scholars explored the profundity and nature of change sweeping across all known environments (Anthony Giddens), several others critiqued the risks that are attractable to socio-material relationships in the global world (Beck, 1992, 2005; Ericson and Haggerty, 1997; Jegede, Ajayi and Allo, 2016). The contributions of the former only partially align with the current discourse, but most central is the contribution of the latter scholars. A parallelism of double risks became noticeable either directly or indirectly within the two lines of thought. While one affects the quality of beings, queries their essence and dispossesses them of control over their socio-material world, the other constitutes a threat to mutual responsibility towards collective survival. Giddens for instance observes that the rapidity of change attendant of modernity encompasses virtually the whole of the globe and are not confined to any geographical limited area (Haralambos and Holborn, 2012:). Our world, in his assertion, is a runaway world, profoundly getting out of our control.

Beck in his own contribution posited that staring us in the face is a world of new, incalculable, unpredictable, and catastrophic modernization risks engendering global warming, depletion of the ozone layer, promoting cybercrimes, cyberwarfare, use of chemical weapons and nuclear contamination (Beck, 2004:2). These are products of science and technological manoeuvring often pursued to better the lots of man but in the process, unleash catastrophic impact and thus threaten their collective existence. This critique of science rests solidly on the fundamental sociology of scientific knowledge (Wynne, 1996).

As an offshoot of science, today, the cyber world has produced unparalleled risks that actually threaten our social continuity via the possibilities of cyber-driven vulnerabilities that have culminated into cyber-borne crimes, theft, fraud, and wars which have produced sufficient disillusionment that is spurring our intuitive reflections to continually ask the question of the 'why of science'? It is gradually becoming commonplace to be exposed to the ravenous effects of nuclear threats, lethal chemicals, the proliferation of hi-tech/cyberwarfare machineries and quantitative mass destruction of lives in the global environment.

Two of the features of modernity that produced risks in the cyber world that Giddens indirectly identified are time-space *distanciation* and *disembedding* mechanisms which were materially mitigated by virtual technologies. Just as internet-borne machines and pliable softwares promote de-territorialism, it also dissembled demystifies physical contact. Intrusions into human privacy, organizational secrets and state-classified matters are made easy, handy, and manipulable. Consequently, personal, organizational, and national secrets became exposable, hackable, and usable against the interest of the true owners of the secrets, by predators and virtual belligerents. Thus, making lives riskier than what we are conversant with in the past. The risks that exemplify today's world is transnational in its impact and it features the activism of both state and non-state actors. Apart from the problems that are associated with rivalrous states, (Israel, Iran, Yemen, Syria, Iraq, and Saudi Arabia in the Middle East which is the epicentre of conflict), (South and North Korea, Pakistan, India, China, and Hong Kong in Asia and the Pacific), transnational criminal networks are enjoying a great deal in the unfolding scenario of cyber revolution. Relevant to this discourse is cyber criminality, which is affecting various victims in the cyber community (Jegeede, 2016a).

Beyond private concerns in the creation of insulators against risks, are the roles of states in their various attempts at stock piling hi-tech cyber compliant weaponry to ward off predatory incursions of both imagined and real enemies. Exploring the risk project of Beck further, the conduct of espionage, hacktivism, and outright stealing of national data is a response toward the uncertainty beclouding the true nature of the enemy's intentions. Information acquired by thievery is inturn used for tactical operations, the demobilization of an opponent's potential, ending in structural and existential annihilation of the vulnerable nation and its citizens. This is promotable of global disorder in the era of virtualism. In the context of all these happenings, the 'look away from danger syndrome' by any nation then becomes psychologically disturbing.

Post Humanism, Virtuality and Changing Trend in Warfare: A Review

There are varied approaches to the impact assessment of Posthumanism across diverse facets of human relationships. Few scholarly works express the fear of man's probable annihilation (Kass, 2001, Fukuyama,

2002 cited Leonie de Jong, 2017) while several others saw Posthumanism as less destructive of man's future (Hayles, 1999; Fernando, 2013). Thweatt-Bates (2012;1) viewed Posthumanism as a way of naming the unknown, possible, (perhaps) future, altered identity of human beings, as we incorporate various technologies into our bodies and selves (cited in Jones and Jones, 2013:41). Posthumanism seems to offer a framework for making sense of our social condition—full of inequality, negativity, and oppression of many sorts—and imagining better futures (Jones and Jones, 2013;42). These attributes of inequality, negativity, and oppression are substantially represented in the virtual world. The concern in this discourse revolves around the impact analysis of virtualism as it affects the essence of man and concomitantly, the assessment of nations' preparedness for a gamut of vulnerabilities that are harvestable in the cyber arena, particularly in the conduct of modern warfare. Reminiscing the age of virtualism, Stock, (2003) conceives of a post-human era as that capable of producing both superhuman and by extension super-powerful nations alongside the inferior people or nations unworthy of reckoning. It is a visible discontinuity of humanity and a transformation occasioning the fusion of a man-machine interface (cyborg) and the production of super intelligence that is enhanced by computer technology (fyborg). It confers undue opportunity on relatively weak nations and equally thrives on the adoption of the economies of scale in the use of tactical fire and civil-military manpower.

In this era of virtual warfare, humanity is ushered into the era of dispossessive control of what becomes of our world. Man now becomes a node in the Posthuman embodiment and his body is no longer part of "the family of man" but of a zoo of post humanities (Harlbastern and Livingston, 1995). Reflecting on the status of man in the virtual age, Braidotti, (2006:1) exclaimed that the era of advanced postmodernity occasioned the destabilization of humanity and this is perfected by technological mediated social relations sporadically taking place in our increasingly globally-connected world and ushering a contradiction on what exactly counts as human when handling cyber-related conflicts and catastrophes. This posthuman condition has significantly affected modern day conduct of warfare ranging from subtle encroachment into national privacy (information warfare) and crescendoing into overt annihilation of one state by another. The centrality of attacks in information warfare consist of seven broad areas: command and control C2W; intelligence-based warfare (IBW); electronic warfare (EW);

psychological warfare (PSYW); hacker warfare (HW); economic information warfare (EIW) and; cyberwarfare (Libicki, 1995). Liles, Dietz, Rogers and Larson, (2012: 170) defines cyberwarfare as “conducting military operations according to information-related principles while disrupting, destroying, and knowing much about an adversary while keeping them from knowing about you.

There is a lot of research on cyber warfare. Few scholars consider it a form of computer network attack (CNA) which occurs in diverse ways such as cyber exploitation that is capable of blocking military communication, malware use for defence secret theft and destruction (Goldsmith, 2013), and others involving the difficulties of detecting attacks. Implicated in this are the cyberwarriors who develop capabilities and undertake cyberattacks in support of a country’s strategic objectives. The activities of cyberwarriors resonates Russia’s statement of defence against accusation of interference in US election. This form of activity carries disruptive potentials that are capable of undermining the civil and military strength of rivals, opposable forces or nations. When activated, secret information is intercepted and penetrated alongside data streaming which is often introduced into defence archives with the view of aiding the conduct of cyber operations with a strategic military outcome (Singer and Friedman, 2014: 127).

The effect of cyberwar is made more real in the context of the colossal damages it potentially unleashes on the information repository of other nations. Akin to this form of war also involves activities that proximately results in death, injury, or significant destruction that are concertedly made achievable by hostile groups or nations through the manipulation of the digital battle space (Theohary and Rollins, 2015: 4). The unravelling scenario in Iraq, Afghanistan, and Syria attested to this state of affair. The material facts and progress report filtering out from thesevarious military campaigns clearly shows that there is a consistent de-emphasis on the use of conventional foot soldiers in the conduct of offensive battles but rather a higher premium is placed on the utilization internet-driven war machines and airpower that are capable of providing optimum results. Pathetically, whether made public or not, the current statistics of human-material destruction today is quite alarming and most especially when compared with the effects of other typologies of warfare that preceded today virtual warfare.

It is instructive to know that the world has gotten to the phase of testing the potency of the state of the art of internet-aided war armaments judging from what occurred in Afghanistan, with the roles of the allied forces and the brutal approach adopted by Russia under the pretence of defending Assad's regime in Syria. The introduction of S300 and S400 air-defence machines completely shows that fewer and fewer number of operational soldiers will be needed in future wars. The ongoing war in the context of Syria far exceeds economic interest but more inclusive of military related interests. The Syria environment automatically becomes test site for sophisticated weapons and determinants of combat efficiency of war machines and airpower. A deviation from what previously existed in the analytics of virtual warfare that is considered in this discourse consist of the probable "discontinuity of humanness" in the conduct of wars. With diverse layering of the digital information environment upon the weapon platform of the military, cyberwarfare opens up extreme annihilating tendencies among warring or combative forces and this is detrimental to human existence. Virtual mode in warfare numbs the conscience (subjective mental state) of man against his fellowmen and thereby functioning unrestrictedly within the ambient of 'no pity' 'absence of feelings' 'exclusion of pain' in the discharge of attacks that are freely dispensed on other individuals or nations alike via the computer terminals (Fukuyama, 2002:166). In virtual war, human-computer interface allows military strategists to interact and get entrenched in computer simulated war environment that is often aided by diverse forms of visual display technology (Rizzo et al, 2011: 176).

Preparedness of Nations towards Virtual Warfare

The preparative assessment of nations toward rebuffing computer technology annihilable threats often aiding modern cyberwarfare is both informative and instructive in order to propel intercontinental action. This is becoming more real as significant part of political and military conflict will take place via the Internet in several years to come and by reason of its ubiquity and non-predictability, the battles fought in the cyberspace can be just as important, if not more potent, than war events taking place on the ground (Geers, 2008; Jegede, 2016b). Majorly, cyberwarfare thrives on varied forms of computer network exploitation (CNE) that are requiring computer network defense (CND) which often

occasions concerted preparedness against virtual attacks (PAVA). The aversion to and systemic preparedness against cyber-attacks in this discourse is in line with the international convention as enshrined in article 51 of U.N. charter (*jus ad bellum*) earlier alluded to by few scholars which views cyber operations as possessing the qualitative capacity of an armed attack directed against any nation (Melzer, 2011:13; Hathaway et al, 2012:27).

Research findings of Dartmouth College on cyberwarfare (2004) identifies three notable areas of preparedness against cyber borne malicious (CBM) and defence vulnerability attacks (DVA). Preparedness measurement indicators (PMI's) in this regard consist of the likelihood of the development of cyber-attack capabilities, increment in foreign military and intelligence agency research and considerable investments in information technology equipment and installations. Investments into these major areas is a function of threat or vulnerability dynamics capable of affecting each region of the world. National investment against cyber-attack capabilities can be measured on the level of, availability and sophistication of war machines, medium and long range missile assets, force and combat readiness of troops cutting across the various arms of Navy, Airforce and the military and rapid response strategies put in place to counter the insurgence of cyber enabled warfare. Investible foreign military and intelligence agency research inputs will cover the following: military IT projects, cyber related equipment acquisition, trained, functional and active warfare units, computer security and specialized trainings existent in the tactical plan manual of nations. The third preparedness measurement indicator consist of information technology investment with inputs in industrial electronics, information technology research and development efforts, network infrastructural development, advanced university engineering curricula, software development, and state-to-state information technology initiatives, technical assistance and training programmes.

The combination and usability of the PMI's will of necessity aids the operationality of counter cyber-warfare strategies and at the same time enables nations to launch attacks on other nations.

In the classification of countries by defence spending, GDP update (2017) classified nations into six categories in relation to their defence prioritization and security posture. These include coalition partners; territorial security seekers; constrained force projector; threat focus self-defenders; global power projectors; and robust self-defenders. The global

power projector includes: US, Russia, China, UK, France the top territorial security seekers identified include countries such as Denmark, Sweden, Latvia, Venezuela and Lithuania. The threat focus self-defender consists of Poland, Qatar, Norway, India. The constrained force projector includes: Turkey, Italy and Ukraine. In the category of robust self-defender include: Saudi-Arabia, Angola, UAE, Morocco, Iran, Pakistan and Syria. Territorial self-defender include: Croatia; Japan and South Korea. Quite early enough, most superpowers had recognized the desirability and the need to convert the potential advantages accessible through the information revolution into warfare capabilities. At the helm of global competitive warfare consist of the US, Russia, China and the 29 NATO members.

Apart from competition and quest for ascendancy among the superpowers, other regional determinants for preparedness rest solely on challenges relating to inducible insecurities that are contiguous to each of the regions. For instance, prior to 1988 and most especially before the commercialization or private uses of digital computers, the U.S. Army had successfully recognized the potentials and adapted the information technology to offensive and defensive operational usage within the information battle space of perceived enemies. Also in the 70's, Russia was attributed to have engaged research into digital revolutionary warfare daubed 'revolution in military affairs' which exposed Russia's military to the use of electronic command and control in all existing military formations (Fitzgerald, 1992). Cyberwarfare was viewed as potent enough to affect both military and civilian population in both positive and negative ways and consequently the realization of this fact calls for changes in military principles, tactics and with enablement of permissible conditions from that of the conventional warfare. The existence and efficient use of PMI's model by Russia was rated as trailing that of the U.S. (Dartmouth, 2004:111).

Reactively during the 1990's, China had efficiently and successfully utilized the PMI's to ward off threats, arrest vulnerabilities that are contactable through malicious compromise of defense secrets and engaged in cyberwarfare strategic attacks as at the latter part of that decade. It concertededly developed cyberwarfare doctrine, conduct basic cyberwarfare training for its officers and conduct cyber warfare exercises (Dartmouth, 2004: 25). As early as 2001, Indian government also eulogised the comparative advantage conferrable through the use of information technology for defense security and cyberwarfare. IT

advantages include the mitigation and reduction of troop's response time to both overt and covert threats, its revolutionary capabilities for strategic planning and as aider of defensive and offensive information warfare. In the same vein, the growth in commerce and economic boom that favoured Asia and the Pacific equally promoted diverse threat among so many gladiators within the region. This has increase the level of preparedness for cyber borne warfare as defence spending soared dramatically. Confronting Asian and Pacific region consists of China's economic domination, North Korea's threats and bragging on the capacity of its nuclear arsenals to destroy other occupiers of the region. The third nature of threat is implicated in the extremism of a brand of Sunni Islam called the Salafiyya.

Exploring the happenings in other continents, one should rarely know that significant countries are not folding their hands watching events unravelling. In the Middle East for example, the rivalry between the Sunni and Shite Muslims remained potent and there is the incremental of cloud of insecurity. At the tail end of Arab spring and concomitantly the insurgence and abating of regional civil wars, there are build-up of hostilities between Saudi Arabia, Iran, Yemen and their allies in their various quest for hegemony over the region. The financing of terrorism in Yemen and the subsequent missile attacks on Saudi-Arabia increases the vitality of threat affecting the Middle East.

Cyber spying grew tremendously in the 21st century. There are diverse means employed by nations to outwit both real and imagined enemies. These several occurrences have not been devoid of allegation and counter allegations emanating from one nation against the other. The American election in 2016 was purportedly manipulated by Russia who was accused of hacking the democrats e-mail account. Also in 2018, Iran accused the West of using lizards for nuclear spying (Firuzabadi, 2018:86). In a counter report, Iran was also accused of backing cyber espionage activism ably conducted by a group code name Charming Kitten targeting US. Officials with a bid of hacking into the mails of those enforcing the sanctions imposed by Donald Trump on Iran's (New York Times, 2018). The veracity or otherwise of all these allegations constitutes a different ballgame entirely but the important point is the fact that docility to the existence of looming threat will doom unprepared nations in a futuristic sense.

In response to the growing cyberwarfare threat, Wales Submit Declaration mandated NATO members to commit 2 percent of their

Gross Domestic Product on defence spending. The declaration represents a wake-up call engendering the realization of and further culminating into a projection or prediction about the future sophistication of cyber driven battles. This singular call explains to a large extent the declaration of a state of emergency requiring the attention of nation state to the daunting challenges of cyberwarfare. Major focus was place on the committal of natural resources for the purpose of defence expenditure and the provision of the state of the art training for military professionals which will in turn enable them respond to the unique challenges of modern cyberwarfare (GDP, 2017).

Unfortunately, there is only few reckoning of any nations in the Sub-Saharan Africa bracing up against the threats of cyberwarfare even until now. This is consistently creating unwarranted psychological noise in the minds of intellectuals and cyber security analysts who are eagerly observing the unfolding scenario of the cyber driven vulnerabilities and its consequences for Africa's development. Efficient acquisition of tactical components that are capable of aiding cyberwarfare execution and defensive operation is abysmally low in Africa and particularly among the countries in the Sub-Saharan region of Africa.

Findings on Comparative Defence Spending affecting Africa

In line with the pursuit of this paper, the comparative analysis of defence spending can best be interrogated from the prioritization accorded defence concerns and the strategies often adopted to ward off threats. The defence compliant indicators in Africa can mainly be assessed by the ubiquity of threats and the dynamics of social occurrences in their various local communities. The explanation on the latter is reserved for the discussion of findings section. Relatively, higher committal of accruals from national income to address the PMI's is significantly correlated with the visible defensive efforts directed at warding off cyber-borne warfare threats. The dynamics of the climatic condition of cyber warfare environment and willingness to invest then becomes, the higher the risks contactable by participation in the cyber arena, the higher the premium placed on the procurement of cyber compliant weaponry and the training made accessible to the combat forces. The table below reveals the combat preparedness of 136 countries collated alongside their defence expenditures. The data presented in the table consist of portion of the national resources committed to the procurement, maintenance

and refurbishment, updating of weaponry and strengthening of indigenous military personnel globally. This data is inclusive of the expenditure on cyber deterrence that is often put in place by diverse nations. It is however instructive to know that the portion of defence budget commuted to warding off of cyber threat is difficult to ascertain due to the lumpsum nature of resources earmarked under of defence spending without itemization of concrete defence focus besides the procurement of weaponry and maintenance of troops welfare.

Country	\$USD	Country	\$USD	Country	\$USD	Country	\$USD
United States	647,000,000,000	Iraq	6,055,000,000	Bangladesh	1,590,000,000	Guatemala	210,000,000
China	151,000,000,000	Chile	5,483,000,000	Jordan	1,500,000,000	Honduras	205,000,000
Saudi Arabia	56,725,000,000	Thailand	5,390,000,000	Sri Lanka	1,500,000,000	Turkmenistan	200,000,000
United Kingdom	50,000,000,000	Kuwait	5,200,000,000	Yemen	1,440,000,000	Cambodia	192,000,000
India	47,000,000,000	Belgium	5,085,000,000	Ireland	1,165,093,600	El Salvador	165,000,000
Russia	47,000,000,000	Ukraine	4,880,000,000	Hungary	1,040,000,000	DRC	162,000,000
Germany	45,200,000,000	Switzerland	4,830,000,000	Slovakia	1,025,000,000	Paraguay	145,000,000
Japan	44,000,000,000	Malaysia	4,700,000,000	Croatia	958,000,000	Panama	145,000,000
France	40,000,000,000	South Africa	4,610,000,000	Serbia	830,000,000	Albania	138,400,000
South Korea	40,000,000,000	Denmark	4,440,000,000	Slovenia	790,000,000	Republic of the Congo	135,300,000
Italy	37,700,000,000	Egypt	4,400,000,000	Bahrain	730,000,000	Ghana	120,000,000
Brazil	29,300,000,000	Argentina	4,330,000,000	Belarus	725,000,000	Namibia	120,000,000

Australia	26,300,000,000	Angola	4,150,000,000	Bulgaria	700,000,000	Chad	120,000,000
Israel	20,000,000,000	Venezuela	4,000,000,000	Cuba	700,000,000	Dominican Republic	110,850,000
Canada	16,000,000,000	Portugal	3,800,000,000	Kenya	595,000,000	Macedonia	108,152,512
UAE	14, 375,000,000	Finland	3,660,000,000	Tunisia	550,000,000	Zimbabwe	95,000,000
Columbia	12,145,000,000	Morocco	3,400,000,000	South Sudan	545,000,000	Mozambique	86,000,000
Spain	11,600,000,000	Vietnam	3,365,000,000	Armenia	512,000,000	Niger	85,000,000
Afghanistan	11,500,000,000	Austria	3,220,000,000	Uruguay	490,000,000	Montenegro	83,000,000
Taiwan	11,725,000,000	Libya	3,000,000,000	Botswana	470,000,000	Gabon	81,520,000
Algeria	10,570,000,000	Philippines	3,000,000,000	Ivory Coast	440,000,000	Mali	76,160,000
Turkey	10,200,000,000	Check Republic	2,596,470,000	Lithuania	430,000,000	Tajikistan	75,000,000
Netherlands	9,840,000,000	Peru	2,560,000,000	Georgia	380,000,000	Uzbekistan	70,000,000
Singapore	9,700,000,000	Sudan	2,470,000,000	Cameroon	370,000,000	Mongolia	70,000,000
Poland	9,360,000,000	Kazakhstan	2,435,000,000	Ethiopia	340,000,000	Suriname	67,410,000
North Korea	7,500,000,000	Equator	2,400,000,000	Estonia	335,000,000	Somalia	58,960,000
Norway	7,000,000,000	Myanmar	2,400,000,000	Bolivia	315,000,000	Madagascar	56,000,000
Pakistan	7,000,000,000	Nigeria	2,330,000,000	Latvia	280,000,000	Nicaragua	44,200,000
Mexico	7,000,000,000	Romania	2,190,000,000	Uganda	280,000,000	Mauritania	39,140,500
Indonesia	6,900,000,000	Qatar	1,930,000,000	Bosnia and Herzegovina	250,000,000	Laos	18,500,000
Oman	6,715,000,000	Syria	1,872,000,000	Zambia	245,000,000	Central African Republic	18,500,000

Greece	6,540,000,000	New Zealand	1,870,000,000	Kyrgyzstan	240,000,000	Sierra Leone	13,040,000
Iran	6,300,000,000	Lebanon	1,735,000,000	Tanzania	220,000,000	Liberia	10,000,000
Sweden	6,215,000,000	Azerbaijan	1,600,000,000	Nepal	210,000,000	Bhutan	10,000,000

<https://www.globalfirepower.com/defense-spending-budget.asp>
2018

At the top of the list comprises of the six super powers US, China, UK, Russia, Germany and France. Conventionally, the superpowers were known for competitive rivalries and unrelentless quest to outwit each other. Seeking global relevance and domination have been at the centre of defence spending for most advanced economies and this is mostly done to attract followership of other less advanced nations in a bid to make them ready markets for manufactured weapons and war technologies. The top 10 only featured the dominant actor (oil rich Saudi Arabia) from the Middle East. The appearance of Saudi Arabia alongside known great nations in modern warfare can be explained by the ever growing threats persistently directed at ousting the nation from her exalted position as the leading Islamic nation having the custodian of the globally acclaimed Islamic culture ably promoted by the orthodoxy of ancient Islamic religion. The positioning of Saudi Arabia among the warfare giant nations is also connected with the ever growing threats of Iran and some few dissident Islamic countries in the Middle East.

Paradoxically, none of the African countries featured among the first twenty nations in relation to defence spending. Only four were found in the category of one to fifty, twelve in the category of fifty-one to hundred and fifteen nations were found among one hundred and one to one thirty-six category. The first four African countries in the first twenty of defence spenders consist of two Islamic countries, Algeria, (23) and Egypt (45) both having direct exposure to the threats or potential onslaught of the terror group and the vulnerability to the activities of the ISIS. The other two, South Africa (43) and Angola (47) can be classified as moderate spenders. The growth in military committals of South African may be closely linked with the gains of the apartheid in which social militarization for the purpose of political freedom exerted more influence on political leaders in their various decisions on warfare armament spending even after the concession of autonomy. Angola has

hitherto been the stronghold of Jonas Sarrvimbi with protracted civil war which ended after the latter's assassination. The protracted civil war may be regarded as the catalyst for further expansion in military expenditures even after the cessation of hostilities. Next to those earlier explained involves those in the category of fifty-one to hundred consist of Morocco (51), Libya (54), Sudan (58), Nigeria (62), Tunisia (84), and South Sudan (85) both of who are known to be notorious nations with the ubiquity of religious fundamentalism, terror and ISIS activism. Morocco has a contiguous boundary with the European nations that are widely adjudged to be powered by modern state of the art weaponry. First, strategic and deliberate investment into the procurements of compliant weaponry is closely tied to warding off of vulnerabilities possible by the perceived superior powers of European nations. This might not also be unconnected to the perception of the custodian of Islamic culture in several nations in this class consistently rebuffing the Western culture as antithetical to their religio-social culture. Second revolves around the attempts at checkmating the growing insurgencies possible by radical Islamic terrorism.

Also, Libya's notoriety in state sponsorship of terror and lately of protracted inter-tribal wars ravaging the country may likely account for the depth of the committals of natural resources to the procurements of weapons. The continued war after the demise of Libya's maximum ruler Mohammar Gadhafi explains in part the positioning of this country as a robust spender on war equipments. Sudan remained under the watch list of the global community as one of the genocidal nations with a series of unabated civil wars and wanton wastages of human lives. The fear of sudden reappraisal for non-committal to and absence of respect for human rights along high profiles of state-sponsored killings may also likely explain the magnitude of interest of Sudan on defence spending. Nigeria's sixty-second position among world buyers of weapons can conveniently be linked to the fear of the growing web of influence of Boko Haram and of late the dastard incursions of Shiite Islamic terror groups especially along the Northern part of the country. The insurgence of the Fulani herdsmen and the engagement in a killing spree across the northern part of the country with later expansion to the Western and Southern parts could also explain the growing interest of Nigeria's government in defence spending.

Tunisia's position in the hierarchy of defence spending also depicted the threat level existent in her local environment. The nation serves as a

recruitment ground for ISIS fighters and she is also prone to terror onslaughts occurring from the displacement of the group from the Middle East. South Sudan placement side-by-side with Tunisia can be linked to the uncontrollable rivalries among the local gladiators in the newly referendum-created nation. The rise and fall of local leaders promotes significant bracing up against negative surprises. Twenty two African nations trailing the afore-discussed six terror-ridden nations can be adjudged to be relatively peaceful: Botswana (88), Cameroon (92), Ethiopia (93), Uganda (97), Zambia (99), Tanzania (101), Ghana (113), Namibia (114), Zimbabwe (118), Mozambique (119), Niger (120), Gabon (122), Mali (122), Madagascar (129), Mauritania (131) Central African Republic (133) with few countries such as Ivory Coast (89), Republic of Congo (112), Chad (115), Somalia (128), Sierra Leone (134), and Liberia (135) having the history of civil wars, Jihadism and internal insurgencies which promoted wanton destruction of lives and properties in the past besides the ongoing turbulence in Somalia.

Discussion of Findings

The discussion under this section will attempt the explanation of the rationale behind the underfunding of defence arsenals to the capabilities of most countries in Sub-Saharan Africa. Holding the context of persistent slow economic growth nurtured by geo-political turmoil, financial market fragility, and sustained high-debt levels (Schwab, 2016:3), reference is made in this section to social occurrences inhibiting the committal of national resources towards warding off cyber-borne threats in Africa. These inhibitors include: acute corruption, bad leadership, appendages of belligerent nations, policy discontinuity, excessive reliance on mono-economy, declining industrial potentials, infrastructural decay, massive unemployment, weakened economies, and a host of other clogs. There is a significant relationship between the existence of corruption and the dearth of insurable materials and infrastructure. Sobjak (2018), reiterates that real and perceived corruption risks discourage mutual benefits accruable through investment in projects of collective concern. Chunks of the capital required for national development have leaked out through the conduits of misappropriation, money laundering, and outright stealing or looting of treasuries. The existence of corruption is closely tied to bad leadership. Ebegebulem (2012:221), attributed Africa's underdevelopment in all ramifications to

bad leadership. Corruption is promoted by the erosion of civic virtues, positioning of corrupt elites in governance, latter's capability to block pragmatic anti-corruption policies. There is a visible absence of purposeful leadership that could act as an architect and engineer of progressive change and development; thus, in a way promoting the deprivation of the continent of the possession of the potentials of measuring at par with futuristic articulate nations.

Conclusion and Recommendations

In the era of Posthumanism, the spate and enormity of threats that are linkable to the de-emphasis on the use of man as a major component in the execution of modern warfare is gaining momentum among highly industrialized and terror-prone states for three important reasons. They are the availability of the alternative that is located in the potentiality of virtual machines consistently providing substitutionary roles for the promotion of computer-borne offensive and defensive operations;; and the ease at which defence secrets can be stolen, traded, and utilized against the true owners of such defence secrets. This collectively became an impetus pushing both state and non-state actors toward jettisoning the massive use of man's input in cyberwarfare.

Regrettably, there exists a skewed effect affecting accessibility to, the utilization of, and the currying of advantages that are endemic in the modern arena of cyberwarfare environment in exclusion of Sub-Saharan Africa due to corruption, bad leadership, deteriorating economies, and other negative cues earlier enunciated above. Consequently, it is strongly advocated that political administrators in Africa engage a pragmatic appraisal of the unfolding development with the view of positioning their nations to stand shoulder to shoulder with other nations with cyberwarfare compliant potentials. This can be attained by investing qualitative resources in the procurement, maintenance, and serviceability of weaponry and the training of service personnel in the utilization of such state-of-the-art arms and armament.

References

- Beck, U. (1992, 2005), *Risk society: Towards a new modernity*. New York: Sage.
- Beck, U. (2004), Risk, uncertainty and government. In Pat O'Malley (Ed.) *Risk, Uncertainty and Government. Great Britain: Glass House Press*, Pp. 1-28.
- Braidotti, R. (2006). Post human, all too human: towards a new process ontology. *Theory, Culture & Society*, Vol. 23 (7-8), Pp. 197-208.
- Chandler, D. (2013). The world of attachment? The Post-humanist challenge to freedom and necessity. *Millennium: Journal of International Studies* 41(3) 516 –534
- Clynes, M. and Kline, N. (1960) 'Cyborgs and Space' in C. Gray, H. Figueroa-Sarriera, and S. Mentor (1995) *The Cyborg Handbook*, New York: Routledge, 29-33. Cornell
- Dion, E. (2004) "The e-Forces: The evolution of battle-groupings in the face of 21st century challenges," *Canadian Army Journal*, p. 3, October 29-30.
- Ebegbulem, J. C. (2012). Corruption and leadership crisis in Africa: Nigeria in focus. *International Journal of Business and Social Sciences*, Vol. 3, No. 11, June.
- Ericson, R. and Haggerty, K. (1997), *Policing the risk society*. Toronto: University of Toronto Press.
- Ferrando, F. (2013). "Posthumanism, Transhumanism, Antihumanism, Metahumanism, and New Materialisms: Differences and Relations." *Existenz* 28, 2: p. 26-32.
- Firuzabadi, H. (2018). "Iran accuses west of using lizards for nuclear spying", *Times of Israel*, 13th February, P. 86.
- Fitzgerald, M. C. (1992). "Russia's new military doctrine," *RUSI Journal*, October, 458
- Fukuyama, F. (2002). *Our Posthuman Future: Consequences of the Biotechnology Revolution*.
- Gartner, Inc. (NYSE:IT) (2017). *Gartner Forecasts Worldwide Security Spending Will Reach \$96 Billion in 2018, Up 8 Percent from 2017*. Egham, UK. <https://www.gartner.com/newsroom/id/3836563>
- Geers, K. (2008). *Cyberspace and the changing nature of warfare*. SC Magazine, 27 August

- Global Defence Perspective (GDP) (2017). Updating the map of defence prioritization and posture in a challenging World. www.pwc.com accessed on 14th September 2018.
- Goldsmith, J. (2013). How cyber changes the laws of war. *The European Journal of International Law* Vol. 24 no. 1, p. 129-138.
- Government of India (2001). “Challenges to the Management of National Security” Report of the Group of Ministers on National Security, February 2001.
- Gray, C. (2002). *Cyborg Citizen: Politics in the Posthuman Age*, New York: Routledge
- Harlbastern, J., and Livingston, I. (1995). “Introduction: posthuman bodies”, *Posthuman Bodies*. Indiana University Press, P.1-19.
- Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., and Spiegel, J. (2012). *The Law of Cyber-Attacks*. California Law Review?
- Hayles, K. (1999) *How we Became Posthuman*. The University of Chicago Press,---. 2011 “Wrestling with Transhumanism.” [Metanexus.net](http://www.metanexus.net), 1 September, <http://www.metanexus.net/essay/h-wrestling-transhumanism>. Accessed 21 April 2017.
- Hughes, R. (2009). Towards a Global Regime for Cyber Warfare. In Christian Czosseck, Kenneth Geers (Eds.) *The Virtual Battlefield: Perspectives on Cyber Warfare*, Vol. 3, Pp. 106-117.
- Jegede, A. E. (2016a) Modern Technology, Global Risk and the Challenges of Crime in the Era of Late Modernity. In Nelson Okorie, Babatunde Raphael Ojebuyi and AbiodunSalawu (Eds.) *Impact of the Media on African Socio-Economic Development*. IGI Books Publication, Pp. 18-32
- Jegede, A. E., (2016b) Cyber Space and Crime Engineering: A Sociological Review. *International Journal of Forensic Science*, Vol. 1, Issue 1, Pp. 1-12.
- Jegede, A. E., Adejuwon, G. A., Olowookere, E. I. and Elegbeleye, A. O. (2016) Ecological Approach to Nigerian Youths Cyber-Fraud Participation. *Social Sciences*,
- Jegede, A. E., Ajayi, M.P. and Allo, T. (2016) Risk and Investment Decision Making in the Technological Age: A Dialysis of Cyber Fraud Complication in Nigeria. *International Journal of Cyber Criminology*. Vol. 10, Issue 1, Pg. 62-78.

- Jensen, M. (2008). Pesticides in risk society: The view from everyday life. *Current Sociology*, Vol. 56, No. 5, September, Pp. 757-778.
- Jones, H. and Jones, N. (2017). Race as Technology: From Posthuman Cyborg to Human Industry. *Ilha do Desterro* v. 70, n°2, p. 039-051, Florianópolis, mai/ago, Pp. 39-51.
- Kass, L. (2017). "Preventing a Brave New World." *The New Republic Online*, 21 June 2001,
- Leonie de Jong / s0730769 (2017). *Posthuman Anxiety: The Fear of the Loss of Humanity*,
- Libicki, M. (1995) 'What is information warfare?' ACIS Paper 3: August 1995; National Defense University Press. <http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html>
- Liles, S., Dietz, J. E., Rogers, M. and Larson, D. (2012). *Applying Traditional Military Principles to Cyber Warfare*. Tallinn: NATO, CCD COE Publications.
- Machlis, B. (2018). Arms Race is on. *The Times of Israel*, 21st March.
- Mahmud, A. (2015). Post/ human beings & techno-salvation: Exploring artificial intelligence in selected science fictions. *Socrates*, Vol. 3, No. 2, p. 9-29.
- Melzer, N. (2011). *Cyberwar and International Law*. UNIDIR Resources: Ideas for Peace and Security.
- New York Times, (2018). AP Exclusive: Iran Hackers Hunt Nuke Workers, US Officials. Dec. 13.
- Pepperell, R. (2003). *The Posthuman Condition: Consciousness beyond the brain*. Great Britain, Intellect Books.
- Picador.
- Research Master Thesis Literary Studies, Faculty of Humanities Leiden University.
- Rizzo, A., Parsons, T. D., Belinda, L., Kenny, P., Buckwalter, J. G., Rothbaum, B., Difede, J., Frazier, J., Newman, B., William, J/ and Reger, G. (2011). "Virtual reality goes to war: A brief review of the future of military behavioural healthcare", *Journal of Clinical Psychology Medical Settings*, 18, 176-187.
- Schwab, K. (2016). *The Global Competitiveness Report 2016–2017*. Geneva: World Economic Forum.
- Singer, P. W. and Friedman, A. (2014). *Cyber Security and Cyberwar: What Everyone Needs to Know*. Madison Ave., New York: Oxford University Press.

- Sobjak, A. (2018). Corruption risks in infrastructural investments in Sub-Saharan Africa. OECD Global Anti-Corruption & Integrity Forum, February.
- The Times of Israel (2018), US indicts 2 Iranians accused of spying, surveillance of Israeli, Jewish targets. September 25.
- Theohary, C. A. and Rollins, J. W. (2015). Cyberwarfare and Cyber Terrorism: In Brief. USA: CRS Report
- Thweatt-Bates, J. (2012). Cyborg Selves: A Theological Anthropology of the Posthuman. Burlington, VT: Ashgate.
- Weaver, J. A. (2010), Educating the Posthuman: Biosciences, Fiction and Curriculum Studies. Rotterdam, Netherlands: Sense Publishers.
- web.stanford.edu/~mvr2j/sfsu09/extra/Kass3.pdf. Accessed 05 Jan. 2017 cited in
- Wynne, B. (1996). 'May the sheep safely graze? A reflexive view of the expert-lay knowledge divide'. In S. Lash, B. Szerszynski and B. Wynne (eds.) Risk Environment and Modernity: Towards New Ecology. London: Sage, Pp. 44-83.