Cyber Warfare: African Research Must Address Emerging Reality

Uche M. Mbanaso
Director, Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria

Abstract
This thematic report sets out the case for why studies in cyber security and cyber conflict need to be prominent in the African digital transformation research agenda.

Keywords
cyberspace, cyber attacks, cyber conflict, cyber warfare, Africa

DOI: https://doi.org/10.23962/10539/21789

Recommended citation
Mbanaso, U. M. (2016). Cyber warfare: African research must address emerging reality. *The African Journal of Information and Communication (AJIC), 18,* 157-164. https://doi.org/10.23962/10539/21789

Cyberspace is emerging as a new battlefield, as cyber attacks can now complement state conflicts. The recent cyber feud between the US and Russia, in which the former openly accused the latter of deliberate and orchestrated hacking activities to undermine the integrity of the just-concluded US presidential election, did not come as a surprise. As we witness traditional activities increasingly shifting to this new domain, cyberspace is becoming a focal point not only for beneficial innovations, enterprises and social networking, but also a site for criminality and warfare (Ackerman, 2016; Lewis, 2011). These latter features are reshaping and redefining the digital space as an environment not only for progress and prosperity, but also for cyber threats. Meanwhile, many countries, especially in Africa, are embracing emerging trends in cyber space with little insight as to where certain of the trends may lead. The question is: In Africa, how aware are we of cyber conflicts and the possible magnitude of cyber warfare?

Unlike a decade ago, cyber warfare is no longer a strange or mystifying notion. With the emerging reality of nation-state-supported attacks on the digital infrastructure of other nations, the entrenchment of the relatively new phenomenon of cyber warfare in the human lexicon cannot be contested. Like any new concept, there is no agreed definition of cyber warfare (Applegate, 2011). As a basis for this discussion, we define cyber warfare as cyberspace-based conspiracy and conflict, usually including politically-motivated attacks on information systems and networks, targeted at a nation or nations (Betz & Stevens, 2011; Capaccio, 2012). It is a deliberate action by a nation state (or nation states), or by an organised group (or groups), against a state (or states) that is aimed at disrupting or harming critical national infrastructure (CNI) in ways that can bring the infrastructure to a standstill (O'Connell, 2012).

Cyberspace has evolved into a critical domain that countries can no longer take with levity, and that many countries are working hard to control and/or dominate. Besides the threats from financial fraudsters or groups, there are deliberate efforts by nation states to dominate and show supremacy over other states' information spaces, with the potential to negatively impact economic, political or military activities. Cyber warfare from this perspective is, perhaps, an extension of the shared notion of conspiracy and sabotage between and among nations that one finds in conventional battles (Betz & Stevens, 2011).

In cyberspace, which is intrinsically challenged by uncertainties, nation state actors are increasingly dissatisfied with building defensive strategies alone, and are working to build offensive capabilities that can assail their adversaries when desired (Capaccio, 2012, Bamford, 2013). Cyber war is part of an underground and obscure arms race, where nations invest billions of dollars to establish digital armies and stocks of digital weapons – for example malicious software codes that are politically motivated, as exemplified by the Stuxnet worm that disrupted and disabled the centrifugal equipment of an Iranian nuclear facility (Langner, 2013). Exacerbating the potential

dangers of cyber warfare is the fact that no individual, organisation or government can provide an accurate profile of the vulnerability, threat and risk landscapes evolving in, and emanating from, cyberspace (Mbanaso & Dandaura, 2015; Parks & Duggan, 2011).

What may now be considered historic examples of cyber warfare include the assault, allegedly by Russia, on the Baltic state of Estonia in 2007 (BBC, 2007), which disrupted civilian services. The attacks, which disrupted public web resources, including the Estonian Parliament, banks, ministries, newspapers and broadcasters, was allegedly prompted by a feud regarding the relocation of the Bronze Soldier of Tallinn (The Economist, 2010). This attack, which was the first known cyber attack of such magnitude targeted at a nation state, and which used the distributed denial of service (DDoS) method, sparked worldwide concern. The cyber attack on an Iranian nuclear facility in 2010, suspected to have been carried out jointly by the US and Israel (Langner, 2013), and various attacks on US interests, allegedly by China and North Korea (Perlrothoct, 2012), are other prominent examples of cyber attack exploits. (Much earlier in cyber history, many years before the public Internet, there were alleged cyber attacks on the US National Aeronautics and Space Administration (NASA) network, using the WANK worm in 1989, to protest against nuclear programmes (Applegate, 2011)).

The aftermath of the attack on the 2010 Iranian nuclear facility brought a ferocious response from the Iranian state (Perlrothoct, 2012). Iran launched its cyber counter-offensive against Saudi Arabia and Qatar, as well as American networks. Having boasted of possessing a strong cyber army, Iran carried out these attacks on perceived adversaries to buttress a point (Perlrothoct, 2012).

The December 2014 attack on Sony Pictures Entertainment, allegedly committed by North Korea, was of a magnitude capable of provoking a cyber war. The perpetuators of the Sony assault revealed embarrassing documents, whereby sensitive private and personal information of employees of Sony, amongst other critical data, was compromised. The Sony attack raised public uproar in the US, and the US government was clearly perturbed by the incident. North Korea, undoubtedly a strong aggressor in cyberspace, has continued to assemble a sophisticated cyber army for its offensive and defensive strategies (Kwark, 2015). In a similar vein, China has, undeniably, repeatedly invaded US cyberspace, exploiting vulnerabilities in certain military and government information systems and networks (Capaccio, 2012). Experts argue that most of the Chinese attacks are highly customised and specialised, with a high success rate, targeted at vital military installations, mostly vulnerable to industrial espionage (Bowlsbey, 2016; INFOSEC Institute, 2013).

Countries already drawn into cyber conspiracy and conflicts include the US, China, the UK, Israel, North Korea, Iran and Russia, all of whom are making serious coordi-

nated national efforts with respect to defensive and offensive capabilities. There are indications that the US National Security Agency (NSA) conceived the "US Cyber Command" as early as the year 2000, in order to build the US cyber warfare effort (Bamford, 2013). In his account, Bamford states that the US fears that "cyberweapons are as crucial to 21st century warfare as nuclear arms were in the 20th" (Bamford, 2013). Currently, it is estimated that the US Cyber Command force has over 14,000 personnel with over 13 formidable cyber attack formations (Bamford, 2013). Furthermore, the US is one of those countries that has continued to invest in cyber activities, as it is purported that the US sets aside about USD4.7 billion annually for developing cyber warriors, including expertise development via encouragement of doctoral degree studies in the various fields of cyberspace (Bamford, 2013; Miller, 2016). China, meanwhile, is building its cyber warfare paramilitary forces, understood to be especially targeting US expertise and specialisations in communications, electronic warfare and networking (Capaccio, 2012).

According a former UK Defence Secretary, "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" (UK Government, 2013). From the foregoing, the general concern is that the rise in cyber conspiracy and conflicts is capable of provoking a full-scale conventional war or cyber war, or a combination of the two. And there is already evidence that nation states or organised groups can launch digital assaults in the context of political and/or economic disputes. The potential for cyber conflict is no longer uncertain. Rather, the uncertainty is: who will be drawn into the cyber battlefields, and when and how? The cyber conflicts trend is increasing in frequency, scale, sophistication and severity of impact (Ranger, 2015), and the outcomes may be grave.

This widening of the elements of the digital divide – now including the ability to participate on the cyber warfare battlefield – is yet to be recognised by many developing nations, including many nations in Africa, who are encumbered by pressing domestic problems and socio-economic challenges. These local issues have, unavoidably, distracted attention from the emerging threats of the digital world (Epstein, Nisbet, & Gillespie, 2011; Mbanaso & Dandaura, 2015). With the scale of the events that are unfolding, it is fast becoming a necessity that every nation recognise the criticality of cyberspace as a domain of warfare. This requires African leaders to appreciate the urgent requirement to incorporate this domain into their traditional military operations of land, sea, air and space, making cyber conflict strategy an integral part of overall military strategy, with proportionate investment. Whether African leaders consider cyber warfare or not, the African continent will not be immune to cyber conspiracy and conflicts. And while cyber warfare could potentially become deeply embedded in contemporary military operations, there is at present no international convention on this matter.

The wars that rage in the cyberspace domain are likely to be very difficult to contain, due to several fluid factors. The factors that interplay and create the vulnerability landscape, which could be exploited by any invader against a target, are inherently unpredictable, increasing in severity as advancements are made in the technology arena (Lewis, 2011). A characteristic of cyber warfare is the minimal risk, and relatively low-cost weapons, required by an attacker to inflict significant impact on a target (Applegate, 2011). Another advantageous factor for attackers is the high level of anonymity and deniability afforded by conducting war-like campaigns in cyberspace (Applegate, 2011).

Conventionally, countries build "special forces", usually small formations of highly-skilled specialists who are seen as superior to all other forces. Combatting cyber warfare will need to fall into the category of matters engaged with by such forces, with lessons drawn from traditional special-force experiences. What are the commonalities and similarities between special forces and cyber forces? Several countries have dedicated vulnerability researchers combing cyberspace in an attempt to discover new weaknesses, as advances in technology characteristically breed new vulnerabilities (INFOSEC Institute, 2013; Shen & Nettis, 2016).

Another key point that should be understood in this context is the nature of the conspiracy and conflicts, which is, fundamentally, knowledge-based (Parks & Duggan, 2011; Shen & Nettis, 2016). It is not going to be business as usual, i.e., not a matter of buying tanks and weapons, as was the case in the traditional arms race. What is key, in this context, is the ability to carry out intellectual exploits, the capability to latch onto inherent vulnerabilities within cyberspace, through intensified and structured discovery, i.e., the ability of invaders to identify high-profile vulnerabilities, which even the vendors and manufacturers of technological devices and services find difficult to ascertain. The strength of every invader lies in its skills, expertise and competence in discovering high-profile, zero-day vulnerabilities. What this entails, as a knowledge-based event, is understanding that the threats are not static, but rapidly evolving, which makes reliance on other countries to supply cyber arms and cyber weapons a dangerous game (Capaccio, 2012; Parks & Duggan, 2011).

While some experts have argued that cyber war is unlikely on the scale speculated (Rid, 2011), there are pointers to the contrary. Presently, China and the US are in what can be qualified as conspiracy and cyber conflicts, with Chinese nationals already arrested for committing industrial espionage (Bowlsbey, 2016; INFOSEC Institute, 2013). Russia has been observed using massive cyber offensives to threaten its former allies, especially the Ukraine and Estonia (Applegate, 2011; BBC, 2007). North Korea is constantly using cyber offensives against South Korea (Kwark, 2015; Sang-hun, 2013; Reuters, 2016). To sum up, many of the conspiracies and conflicts seen among nations in the offline realm have shifted to cyberspace. The same sorts of conspirators, alignments and disagreements witnessed offline in past decades appear

to dominate, and even become magnified, in cyberspace.

The common denominator is that open, borderless cyberspace is a level playing ground for those who choose to invest in it. In the near future, nations' successes will be determined by their capacity and capability to maintain competitive advantage in the information space, i.e., cyber power capability. War based on cyber power capability will be difficult for any one side to win decisively except, perhaps, when combined with conventional warfare.

What may be most disturbing is the inconspicuous nature of nation states' capability, as there is no formal way to assess the true cyber offensive capability of a nation. Unlike the nuclear arms race that can possibly be assessed and constrained, nation states' particular cyber warfare capabilities can lie undetected. Moreover, the absence of international rules of engagement means that any full-scale cyber warfare has no recourse to any international law, even when it can have debilitating effects. While hacking of networks and information systems is an illegal activity, there is no international law addressing the use of cyber power against a state (Applegate, 2011).

Another perspective is that, as alluded to above, the cost of acquiring cyber weapons is relatively cheap, suggesting that poor states can invest little and harvest more, in terms of impact, in the cyber warfare arena. And with the borderless Internet characteristic of anonymity and deniability, nations in conflict can easily draw support from allies, since attribution is difficult.

Accordingly, based on this brief introductory overview, it is my view that studies in cyber security and cyber conflict must henceforth become a significant component of digital transformation research on the African continent.

References

Ackerman, R. K. (2016, April 1). DISA takes proactive approach to cyberthreats. *SIGNAL*. Retrieved from http://www.afcea.org/content/?q=Article-disa-takes-proactive-approach-cyberthreats

Ackerman, R. K. (2016, June 1). The CIA accelerates innovations. *SIGNAL*. Retrieved from http://www.afcea.org/content/?q=Article-cia-accelerates-innovation

Applegate, S. D. (2011). Cybermilitias and political hackers: Use of irregular forces in cyberwarfare. *IEEE Security & Privacy*, *9*(5), 16-22. Available at http://doi.ieeecomputersociety.org/10.1109/MSP.2011.46

Bamford, J. (2013, 12 13). God of war (The secret war). *Wired Magazine USA*. Retrieved from https://www.wired.com/2013/06/general-keith-alexander-cyberwar/all/

BBC. (2007). The cyber raiders hitting Estonia. Retrieved from http://news.bbc.co.uk/2/hi/europe/6665195.stm

Berson, T. A., & Denning, D.E. (2011). Cyberwarfare. *IEEE Security & Privacy*, *9*(5), 13-15. doi: 10.1109/msp.2011.132

Betz, D. J., & Stevens, T. (2011). *Cyberspace and the state: Toward a strategy for cyber-power.* London: The International Institute for Strategic Studies.

Bhatnagar, S., & Goel, A. (2014). Evolution of nanotechnology. *BioEvolution, 1*(3), 76-79. Retrieved from http://www.giapjournals.org/uploads/2/6/6/2/26621256/evolution_of_nanotechnology.pdf

Bowlsbey, B. W. (2016, July 1). Chinese hackers, businesses and government coordinated cyber efforts. *SIGNAL*. Retrieved from http://www.afcea.org/content/?q=Article-chinese-hackers-businesses-and-government-coordinate-cyber-efforts

Capaccio, A. (2012). China most threatening cyberspace force, US panel says. Retrieved from https://www.bloomberg.com/news/articles/2012-11-05/china-most-threatening-cyberspace-force-u-s-panel-says

Collin, B. C. (n.d.). The future of cyberterrorism: Where the physical and virtual worlds converge. *11th Annual International Symposium on Criminal Justice Issues.* Retrieved from http://www.crime-research.org/library/Cyberter.htm

Epstein, D., Nisbet, E. C., & Gillespie, T. (2011). Who's responsible for the digital divide? Public perceptions and policy implications. *The Information Society*, *27*(2), 92-104. Available at http://dx.doi.org/10.1080/01972243.2011.548695

Eubanks, V. E. (2007). Trapped in the digital divide: The distributive paradigm in community informatics. *The Journal of Community Informatics, 3*(2). Retrieved from http://ci-journal.net/index.php/ciej/article/view/293/318

Heickerö, R. (2016). Cyber espionage and illegitimate information retrieval. *International Journal of Cyber Warfare and Terrorism, 6*(1), 13-23. Available at http://www.igi-global.com/article/cyber-espionage-and-illegitimate-information-retrieval/152232

INFOSEC Institute. (2013). China vs US, cyber superpowers compared. Retrieved from http://resources.infosecinstitute.com/china-vs-us-cyber-superpowers-compared/#gref

Kwark, J. S. (2015, March 17). North Korea blamed for nuclear-power plant hack. *The Wall Street Journal*. Available at http://www.wsj.com/articles/north-korea-blamed-for-nuclear-power-plant-hack-1426589324

Langner, R. (2013). *The Stuxnet's Secret Twin.* Retrieved from http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/

Lewis, J. A. (2011, March). Cyberwar thresholds and effects. *IEEE Security & Privacy*, *9*(5), 23-29. Doi: 10.1109/MSP.2011.25

Liehr, M., Coolbaugh, D., Bowers, J. E., Alferness, R., Watts, M., Kimerling, L., & Koch, T. L. (2016). AIM photonics: What merging photonics with nano-electronics will do. *IEEE Optical Interconnects Conference*. doi: 10.1109/OIC.2016.7482991

Mbanaso, U., & Dandaura, E. S. (2015). The cyberspace: Redefining a new world. *IOSR Journal of Computer Engineering*, *17*(3), 17-24. doi: 10.9790/0661-17361724

Miller, J. A. (2016, April 1). Disruptive by design: Breaking down the federal cyber budget. *SIGNAL*. Retrieved from http://www.afcea.org/content/?q=Article-disruptive-design-breaking-down-federal-cyber-budget

O'Connell, M. E. (2012). Cyber security without cyber war. *Conflict & Security Law*, *17*(2), 187-209. doi: 10.1093/jcsl/krs017

Parks, R. C., & Duggan, P. (2011, October). Principles of cyberwarfare. *IEEE Security & Privacy*, *9*(5), 30-35. doi: 10.1109/MSP.2011.138

Paul, B., & Chakrabarty, K. (2009). Advances in nanoelectronics circuits and systems {Editorial]. *IET Computers & Digital Techniques*, *3*(6), 551-552. doi: 10.1049/iet-

cdt.2009.9040
Perlrothoct, N. (2012). In cyberattack on Saudi firm, U.S. sees Iran firing back. *The New York Times*. Retrieved from http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=1&_r=2&
Ranger, S. (2015). *Inside the secret digital arms race: Facing the threat of a global cyberwar.* Retrieved from http://www.techrepublic.com/article/inside-the-secret-digital-arms-race
Reuters. (2016, June 13). *North Korea mounts long-running hack of South Korea computers.* Retrieved from http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE
Rid, T. (2011, October 10). *Cyber war might never happen.* Retrieved from http://www.kcl.ac.uk/newsevents/news/newsrecords/2011/10October/Cyber-war-might-never-happen.aspx
Rid, T. (2012). Cyber war will not take place. *The Journal of Strategic Studies*, *35*(1), 5-32. http://dx.doi.org/10.1080/01402390.2011.608939
Riggins, F. J., & Dewan, S. (2005). The digital divide: Current and future research directions. *Journal of the Association for Information Systems*, *6*(12). Available at http://aisel.aisnet.org/jais/vol6/iss12/13/
Sang-hun, C. (2013, March 20). Computer networks in South Korea are paralyzed in cyberattacks. *The New York Times.* Retrieved from http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html
Shen, F., & Nettis, M. (2016, April 1). Military, government focus on statewide cyber education. *SIGNAL*. Retrieved from http://www.afcea.org/content/?q=Article-military-government-focus-statewide-cyber-education
Targowski A. (1996). The evolution of cyberspace. *Information Technology Management and Organizational Innovations, Proceedings of the 7th Information Resources Management Association International Conference*. IDEA Group Publishing (pp. 333-338).
The Economist. (2010). War in the fifth domain: Are the mouse and keyboard the new weapons of conflict? Retrieved from http://www.economist.com/node/16478792
HM Government. (2013, June). *Information economy strategy*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206944/13-901-information-economy-strategy.pdf