‘Global cybersecurity legislation?’ – factors, perspective and implications

Emmanuel C. Ogu*

Department of Computer Science,
School of Computing and Engineering Sciences,
Babcock University,
Ilishan-Remo, Ogun State, Nigeria
Email: ecoxd1@yahoo.com
*Corresponding author

Chiemela Ogu

Division of Corporate Sustainability Research and Development,
EMINDA Konsults,
Yaba, Lagos, Nigeria
Email: chiemelaogu@gmail.com

Onyekwere U. Oluoha

Computer Science Department,
University of Nigeria,
Nsukka, Nigeria
Email: d_blackdiamond@yahoo.com

Abstract: As at the time of this research, no globally adopted and unified legislation for cybersecurity exists that is currently operational, despite rife global clamours for such a legislative framework. This research paper synthesizes and reviews some of the key imposing factors, putting in perspective the surrounding realities that impede the successful actualisation of such a framework, using the qualitative-exploratory research methodology. Also, presenting the implications of these factors and associated realities for cyber peacekeeping and the struggle for a utopian global information society, and then proposing recommendations pertaining the feasibility and operability of a global cybersecurity legal framework.

Keywords: cybersecurity; cybercrimes; cybersecurity legislation; cyber peacekeeping; cyber policy; cyber law; security policy; security legislation; legislative framework; trans-jurisdictional cyber laws; digital divide.

Reference to this paper should be made as follows: Ogu, E.C., Ogu, C. and Oluoha, O.U. (2020) ‘‘Global cybersecurity legislation?’ – factors, perspective and implications’, *Int. J. Business Continuity and Risk Management*, Vol. 10, No. 1, pp.80–93.

Biographical notes: Emmanuel C. Ogu obtained his BSc in Computer Science (Technology), MSc in Computer Science (Networking and Telecommunications), and PhD in Computer Science with a research focus in Cyber and Network Security, all from the Babcock University, Nigeria. His

research interests cover a broad range of multidisciplinary topics related to contemporary issues and discourses in cybersecurity, security policy and legislation, cyber peacekeeping, and sustainable development. He has authored and co-authored over a dozen peer-reviewed and referred high-quality research articles in the areas of his research interests, which have been published by reputable international journals and indexed in global repositories.

Chiemela Ogu is an Independent Researcher affiliated with the Corporate Sustainability Research and Development (CSRD) Division of EMINDA Konsults – a Nigerian technology innovation and development company. His research areas include computer security, information security, network technology, and cloud computing.

Onyekwere U. Oluoha is an ICT professional with over 14 years of experience in the IT industry. He holds a BSc in Computer Science (Technology) from Babcock University, Nigeria; a MSc in Information Systems Management (ISM) from University of Liverpool, UK; and is currently pursuing a PhD in Computer Science at the University of Nigeria, Nsukka, Nigeria. He possesses a few professional certifications including Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), Cisco Certified Internetworking Expert (CCIE-written), Server and Storage Administration and ITILv3. His research interests include networks and internetworking, network and information security, wireless sensor networks and artificial intelligence.

1 Introduction

Generally, the contexts of ethics and legislation are inextricably related to each other. In lay terms, ethics merely refers to moral standards governing behaviour, actions, and choices; or a discipline that studies the rightness or wrongness of such behaviours, actions and choices. Legislation, on the other hand refers to wider agreed standards and specifications of behaviours, actions and choices that are accepted and adopted by a particular group or region to help inform notions and perspectives of right and wrong, as well as that which is acceptable and unacceptable within jurisdictional contexts; to put it most simply.

The lashing scourge of various nefarious activities perpetrated wilfully in cyberspace by malicious masterminds and even amateur individuals, as well as corporate, state and non-state actors, has inundated many cyber security thought leaders, practitioners and agencies. The concept of cyber proxies and mercenaries as discussed by Maurer (2018) paints a clearer picture of this reality; in which states are able to diffuse power of action to non-state individuals who are aided by the internet to bring about effects across regional and global distances, in what was referred to as the 'diffusion of reach'. In recent times, this reality has resulted in calls and near clamour to begin to forge a path to a globally acceptable legal framework that could enable and facilitate cross-border arrest and effective prosecution of cyber criminals based on universally agreed legislation. More notably amongst those that have at some point lent a voice to sounding this call include the Council of Europe (CoE), the World Summit on the Information Society (WSIS) of the International Telecommunication Union (ITU), and the International Multilateral Partnership Against Cyber Threats (IMPACT) to mention but a charitable few.

In 2001, the first international treaty on cybercrime was enacted. It was sequel to the proceedings and recommendations of the Budapest Convention on Cybercrime. This treaty, amongst other provisions, sought to harmonise national laws (of the various member states) on cybercrimes, improve the investigative techniques that were being adopted for cybercriminal prosecution, and increase international cooperation amongst member nations in the CoE (2015). The Committee of Ministers of the Council of Europe adopted the report of the convention at its 109th session which held on 8 November 2001. The treaty was opened for endorsement in Budapest on 23 November 2001 and it became a law binding (signatory) member nations on the 1st of July 2004 (UNESCO, 2004). This meant that some countries had officially become "red zones" for cybercriminal activities, even though most still remained 'free zones'.

As at January 23, 2018, of the 196 countries of the world: 50 (≈26%) nations (comprising 46 member nations of the CoE, and 4 non-member nations spanning USA, Asia, and Africa) were signatories to the Budapest Convention on Cybercrime treaty; 56 (≈29%) nations (comprising 43 member nations of the CoE, and 13 non-member nations spanning USA and Asia) had ratified the treaty and its provisions and specifications had entered into force as law within their territories (CoE, 2015). The following are the realities stemming from the implications of these statistics:

a approximately 77% of the world is still relatively 'safe haven' for cybercriminals to perpetrate their malicious activities

b the treaty does not yet bear the force of the law in at least four (8%) of the countries that are signatories to it

c at least 10 (amounting to 5%) countries of the world that are not members of the CoE have ratified the provisions and specifications of the treaty into law, even though they are not signatories to the treaty

d there still exists no acceptable (at least by the democratic standards of a majority) legal framework by which cybercriminals could be globally prosecuted.

Similarly, the WSIS, an offshoot of Resolution 56/183 of the United Nations' General Assembly in endorsing the 2001 proposal of the ITU drawing attention to the need for the summit, was a dual-phased summit sponsored by the United Nations, which took place in Geneva and Tunis in 2003 and 2005 respectively. The summit represented one of the early comprehensive efforts of the United Nations to respond to the evolving realities of an emerging global information society, at a time when the global concerns of sustainable development were mounting. Incidentally, the founding goals of the WSIS were not particularly focused on security; however, with the emergence of the WSIS Declaration of Principles, a call was put out for "strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection", and also actively promoting, developing and implementing a cooperative global culture of cybersecurity in concert with stakeholders and practitioners (WSIS, 2009). Following the resolutions of the WSIS meetings and the 2006 ITU Plenipotentiary Conference, the ITU began to pursue the role of "building confidence and security in the use of ICTs"; this led to the publication and launching of the ITU Global Cybersecurity Agenda (GCA), High-Level Experts Group (HLEG) Global Strategic Report in 2008. The report contained expert recommendations for a global framework for cybersecurity legislation, technical and procedural best practices, responsive organizational structures,

capacity building, and international cooperation towards building confidence and security in an evolving global information society (ITU, 2008).

Further, the ITU was originally was established to standardise and regulate the development of radio communication and information and communication technologies (ICTs) by providing tools and resources that educate and guide member states on issues of legislation, awareness and capacity building, self-assessment, and best practices and approaches to issues of technology and the scourge of cybercrimes, for the purpose of ensuring cybersecurity and cyber peace (Choucri et al., 2014). Comprising 193 countries and almost 800 Sector Members and Associates, the ITU is undoubtedly the foremost agency of the United Nations in matters of technology regulation (UN, 2018; ITU, 2018). Asides the launching of the GCA in response to the mandate to coordinate and implement the resolutions of the WSIS' Action Plan C5, in May 2011, the ITU signed a cooperation agreement and entered into partnership with the IMPACT. This has today resulted in a coalition of at least 150 countries of the world with a fairly unified mission against cyber threats and terrorism, known as the ITU-IMPACT – the world's largest alliance on cybersecurity (ITU, 2012).

IMPACT is a public-private venture that has its headquarters in Malaysia and has been operational since March 2009. It is hoped to become a global forerunner in the fight against cyberterrorism and the protection of critical infrastructures. IMPACT provides tools, mechanisms and resources that help a network of 191 countries to consolidate their efforts at cyber defence through training and skills development, policy and international cooperation, security assurance and research, and an always-online global response centre (Choucri et al., 2014; IMPACT, 2015).

Many other notable international organisations, agencies and alliances have also joined in the debate and clamour for a global legislative framework for collaborative trans-national or trans-continental cybersecurity. Some of these others include: the Organisation for Economic Cooperation and Development (OECD), the International Criminal Police Organization (INTERPOL), the European Police Office (EUROPOL), and the European Network and Information Security Agency (ENISA), amongst others.

While the discourse on the need for a concerted global framework for everything cybersecurity still remains contemporaneous and ongoing for the most part, it may be no gainsaying that its attainment seems yet a long way home. There is yet to exist a universally accepted body of legislation in place – one that is ratified and bears the full force of law in all countries of world, and which could form the basis for effective cross-border arrest and prosecution against cyber-criminal activities. Based on earlier presented statistics, this is likely due, in part, to the fact that many countries yet seem not very motivated in adopting global frameworks to tackle the cybersecurity issues within the contexts of their local jurisdictions, and for plausible reasons that recent existing researches have yet to consolidate.

Sinrod and Reilly (2000), decried the implication of this by stating that "these countries [that have failed to adopt a globally unified approach to dealing with cybercrimes], inadvertently or not, present the cyber-criminal with a safe haven to operate." Because cybercriminals can hijack machines from these nations and use them for cybercrimes in other nations across cyberspace, being able to evade proper prosecution in some cases even when they are caught. In fact, as legislation and prosecution became more penal and stringent across various countries of the world, hackers and cybercriminals had to devise other means to carry out their malicious

activities, preserve or increase the force of their attack impact and devastation, neatly cover up their tracks, and further complicate the task of detecting them or their activities on the internet. One of such means which they resorted to was the use of *botnets* (literally, hijacking and taking remote control of other peoples' computers, either to take them out, or to use them to orchestrate cybercrimes against other users and machines). "Never before has it been so easy to commit a crime in one jurisdiction while hiding behind the jurisdiction of another" (Sinrod and Reilly, 2000).

2 Research questions and methodology overview

The pertinent questions therefore remain: "What are the plausible factors and perspectives that continue to pose challenges to the realisation of a global legislative framework for cybersecurity?" and "What are the implications of these factors and perspectives on the actualisation of a safe, secure and utopian global information society?" It is on these questions that subsequent discussions of this research are centred and anchored, in seeking necessary answers.

Being largely a qualitative analysis paper, the qualitative-exploratory methodology is featured, albeit from an analytical and interpretive standpoint; relying on content analysis of relevant and related literature to review the underlying factors that hinder the realisation of a global cybersecurity legislative framework, to put in perspective the emergent realities and their implications for cybersecurity and cyber peacekeeping, and then propose recommendations for more progressive action in this regard. To this end, sources that provide insights and paradigms into the progressive discourse of this research are reviewed, analysed and referred to substantiate discussions and positions at various points of the research.

3 Factors

The incidents that surrounded the ILOVEYOU virus provides perspective to the subsequent discussions, direction, and arguments of this research. On 4 May 2000, the world awoke to a malware that was to win a world record for the most virulent malware of all time two years later. The ILOVEYOU virus originated from a local neighbourhood in Manila, Philippines, and is believed to have been authored by two young Filipino programmers – Francisco Dagamac Jr. and Onel de Guzman. The malware outbreak that was believed to have, at the time, infected about 10% of the global internet-connected computers, caused the global economy damages of up to $8 billion, with an added $15 billion estimated as the cost for removing the malware. All legal charges against the two culprits behind the malware programming were dropped despite the global magnitude of the damage impact and resulting losses from the malware activities due to the absence of effective trans-national legislation upon which basis they could be prosecuted at the time. We discuss the possible factors that could have come to play to here.

3.1 The digital divide

The term 'digital divide' has often been used since the mid to late '90s to reflect/represent a dichotomy or separation between those regions/areas of the world that

have access to modern, cutting edge ICT, resources, equipment and capabilities, and those regions/areas that do not. This definition apparently also incorporates the reality of the brewing new digital divide that is data-induced and fostered by cross-border limitations on data flows by dominating countries of the world due to sovereign economic and trade interests; one that Aaronson and Leblond (2018) recently drew attention to.

The digital divide has brought about mounting new difficulties in setting up globally acceptable cyber-ethical and cybersecurity regulations and legislations to govern the global use and adoption of ICT. Because the reality of the digital divide has often given rise to attempts to categorise countries and regions based on the extent and sophistication of their technological advancements, amongst the challenges that this has brought is the fact that it is difficult to enact legislation that are applicable to the local contexts of various countries across these various categorisations. This factor of the digital divide relates directly to the discourse on global cybersecurity legislation when considered in light of the well-established fact that technological advancement has progressed at a rate that legislation and regulation has not been able to keep up with, thereby resulting in shortcomings that often bring about new challenges (Schia, 2018).

Technology adoption and advancement usually comes with a period of gestation, adaptation and contextualisation, that could be much longer for some than it is for others; and as Moor (1985) posited, technology often brings with it new capabilities that in turn avail new choices for action. Hence, it has been discovered in cases of technology adoption and advancement that often times when it has to do with legislative frameworks for guiding and informing individual decisions on the right use or misuse of such technologies, it is often either that no clearly specified policies currently exist to guide conduct and actions or existing policies seem grossly inadequate. Moor referred to this as a '*policy vacuum*'. In such case, it becomes rather unlikely that such globally adopted legislation would find practical applicability within the contexts of these local situations. In considering a hypothetical example: by the time credit card information theft had become a crime in the developed countries of Western civilisation, some third world developing countries of Africa and Asia had neither known nor seen what an actual credit card looked like in real life; not to talk of how it was to be used. Hence, until recently, it was difficult to even correctly specify or interpret what characterised credit card frauds in most developing countries, talk more of legislating and prosecuting fairly within the contexts of the local jurisdictional justice system. The same can be said of attempted global legislations relating to issues of child pornography, cyber bullying, hacking, and various other issues.

It is perhaps the challenge of poorly defined characteristics of cybercrimes, which Choucri et al. (2014) provided a perspective into, that has birthed the issue of a policy vacuum. Many of the contemporary global definitions for cybercrimes postulated within legal contexts are rather vaguely defined and lacking in specificity. They usually fail to address the specific contextual details that are needed for these to find cross-jurisdictional and global relevance; especially while keeping in perspective the realities posed by the digital divide. This has often left various member jurisdictions to have to craft the specifics of their own legislation, sometimes in line with global definitions. This is because even though these global frameworks and definitions may sometimes have relevance that is not limited by context, often times in trying to interpret their underlying theoretical foundations, especially within local contexts, a lot of domestic jurisdictional

imperatives come into the picture that in the end little to no attention is paid to international considerations (Choucri et al., 2014). As a result, even a cursory analysis often reveals a lot of discrepancies amongst the various local contexts jurisdictional definitions and specifications of cybercrime legislation vis-à-vis the global frameworks. Buchanan (2017) referred to one dimension of this as the 'security dilemma'; a situation in which the anarchic nature of the international system impacts on need for states to prepare capabilities and collect intelligence, in the face of the ever-present risk of misinterpretation and escalation.

3.2 Sovereign political interests

Another factor to be put in perspective is that of sovereign political interests, which can be considered as situations wherein state regulations and legislation shelters, either by means of inaction or legal actions that are not allowed to run their full course, the existence of resident non-state mercenaries and proxies that are empowered by state ideologies and available state infrastructure and resources to orchestrate acts of cybercrimes that benefit the wider state ideological and political frameworks. Maurer (2018), discussed this dilemma across three panels of thought: *delegation*, where "a principal (state) delegates authority to an agent to act on its behalf" in a narrow and unofficial proxy/surrogate relationship; *orchestration*, where following voluntary enlistment states provide intermediary actors "with ideational and material support, and using them to address target actors in pursuit of political goals"; and *sanctioning*, wherein states passively support non-state actors "when it knowingly chooses to tolerate the actor's activities in spite of having the capacity to do otherwise." Smeets (2018), further argued that even though in most cases of politically-motivated and state-inspired cybercriminal activities, state victims of such incidents diplomatically communicate an obligation to respond proportionately; such responses actually go beyond the actual observable activities associated with the cyber incident to the perceived intent of the attacker in sometimes trying to discern destructive motives and whether or not follow-up cyber-attacks are imminent. The resulting inability to gauge the proportionality of attempts to discern perceived attacker intent due to the difficulties associated with trying to accurately interpret such intent typically results in misconceptions that only escalate the situation and breed more anarchy in the long run. This already anarchic situation is further exacerbated by mistrust amongst states who are in a perpetual state of uncertainty about the intentions of other states towards them; and therefore sometimes go to extreme (often illegal, and unethical) measures to probe and spy out such intentions so as to safeguard their vested interests and further establish capabilities to defend themselves in the face of emergent realities (Smeets, 2018).

In what now seems to have become a global struggle for supremacy amongst various national governments, with the USA, China, North Korea, and Russia at the top ranks of this struggle, the popularisation amongst domestic citizens of various government ideologies and propaganda which uphold and sustain the political interests of these governments against their competitors in the global struggle for supremacy has resulted in near subconscious radicalisation of these domestic populations. As a result, in some cases, citizens of such states could find themselves consciously or subconsciously engaging in malicious cyber activities that attempt to foster and advance the political interests and ideologies of their sovereign governments both within and beyond their national borders. In solidarity, these governments could choose to turn a blind eye to

these, sometimes cyber-criminal, activities that benefit their political interests and ideologies; and in some cases attempt to obfuscate evidences and truncate investigations, while also failing to apply existing domestic legislative measures to enforce redress. Some of the more recent and popular examples of these include the recent CNN report by Cohen (2017) that North Korean hackers had infiltrated encrypted government military systems and allegedly stolen over 200 GB of classified collaborative battle information belonging to the American and South-Korean military, including battle plans on how to exterminate the sitting leader of the Democratic People's Republic of Korea (DPRK). Another being the allegations making the rounds about Russia having meddled in the 2016 Presidential election of the USA, with investigations that have now gone on for almost two years with yet inconclusive results.

3.3 'Ethics of legality' in a tension of autonomies

Scholars of ethics generally study ethical principles from the viewpoints of normative and prescriptive ethics. From the viewpoint of normative ethics, ethical principles are derived from consistent and well-based standards of right and wrong that stipulate and inform human choices, decisions and actions in terms of rights, obligations, benefits of the common good, fairness, as well as other specific virtues. In light of this, ethics would include such standards as relate to reasonable obligations to refrain from rape, stealing, murder, assault, slander, and fraud; standards that also inspire virtues of honesty, compassion, and loyalty; as well as those relating to fundamental human rights (Johnson, 1985; Laudon, 1995). Conversely, from the viewpoint of prescriptive ethics, ethical principles relate to ethical standards that are upheld and enforced amongst persons and groups, which are associated with behaviour, feelings, laws, social habits, norms, and mores that could deviate from some more universal ethical standards, and thus necessitating the need for a body of laws that present a constant review and overview of such standards to ensure that they remain congruent and in line with the progress and continuity of humanity (Sembok, 2003). In more consolidated terms, ethics is grounded in both the notion of responsibility and accountability. This directly translates to the reality that individuals, organisations, and societies, as free moral agents, are responsible for the actions that they take and hence should be held accountable to others for the consequences of their actions; thus accounting for why in contemporary societies, a system of laws clearly define the most significant ethical standards and provide mechanisms for holding people, organisations, and even governments accountable (Laudon, 1995).

Cyberethics (a term that is sometimes used interchangeably with 'internet ethics'), on the other hand, is particularly concerned with ethical issues related to the use of and conduct on the internet (Kavuk et al., 2011) and within cyberspace (Onyancha, 2015). However, cyberethics is believed to now include both internet ethic and computer ethics (Onyancha, 2015); because as Herman (2001) identified, the internet has considerably exacerbated some of the traditional issues in computer ethics. This is because the information and technology revolution has fundamentally changed both the nature and context of human interactions on a global scale (Whyte, 2018); with Frohmann (2008) further adding that "subjectivity is at the heart of information ethics" and the digital revolution, especially when considered in light of the associated 'social cleavages', which cannot be relegated in this discourse (Essien, 2018a) argues.

Froehlich (1992), proposed what has been referred to as the "three facets of most ethical situations", and what Frohmann (2008) referred to as a "triangular model of self, organisation and context (or environment)." This model posits that "there are always three definite elements present in an ethical situation: self, organisation and environment", all posing as agents with an 'autonomous will', and trying to exert their various autonomies on each other, resulting in a tension of autonomies. This convolution of autonomies in tension is aggravated by the fact that legality fails to keep up with the pace of technological innovation and development, especially in light of a global moral culture where individuals increasingly desire to be the sole interpreter of the moral and ethical values that guide their actions. Since ethics is generally based on the notion of right and wrong, in most cases to the layman, whatever act that is not intentionally aimed at causing harm to another is often considered ethical; and there are some polemical arguments that uphold this viewpoint. Christian et al. (2009), gave perspective to this reality in trying to explain a dichotomy between rules, norms and values; positing that

> "Rules are (prescribed) techniques or procedures of action, norms are regularized rules achieved by routinized, repeated, and repeatable action, [while] values are a weighting and an evaluation of rules and/or norms according to moral judgements in terms of good and evil. These three components can be found on the individual and on the social levels of the moral system. Human action is an expression of the practical realization of individual rules, norms, and values."

Hence, in certain cases of action, especially where explicit regulations and legislation are not specified, individuals have often resorted to this basic understanding /principle in choosing their courses of action.

However, sources such as Westby (2013) have identified a discord between ethics and law in what this research refers to as the 'ethics of legality' – a discourse that has made the rounds across various areas of technology research and development, including that of cybersecurity. The core of the discord in the ethics of legality conundrum is based on the fact that *not all harmless actions are legal* especially within the context of ICT; because legality is not administered based on the simple notion of 'harm' or 'no harm'. In an early classic example of this situation: on 3 November 1988, Robert Tappan Morris, a graduate student of Cornell University, was reported to have accidentally released one of the first worms on the internet that featured take-out operations, which later became known as the Morris/internet worm. This worm had the ability to propagate itself on a computer network and infect other systems without any external aid. About 6,200 computers in the US alone were taken out by this worm. The Morris worm worked by exploiting known vulnerabilities in computer networks to install itself onto computers that were connected to the ARPANET at the time, crudely taking them out. Productivity losses valued at between $200 and $53,000 were incurred by the direct effect of the worm's activities. Morris was sentenced in December 1990 to three years of probation, 400 hours of community service, and a fine of $10,050 including the costs of his supervision (Guidoboni and Meltzer, 1991; Lee, 2013). Now, even though Morris' action carried no implicit or explicit intentions to cause harm to third party, the ethics of legality conundrum best explains the reason why it was necessary for him to undergo some form of punishment and restitution for his actions.

Many other cases of cybercriminal activities have equally gone unpunished and unsettled due to these above discussed factors. Some of these have been as a result of the challenges that come with enforcing legislations across the frontiers of the digital divide,

as was the case of the ILOVEYOU malware; some have also been as a result of sovereign political interests, as has been the case in various global cyber-instigated political conflicts; or perhaps another case of the ethics of legality in a tension of autonomies, as was the case of Morris.

4 Perspective and implications

Indeed, the internet and cyberspace have become a global phenomenon, creating a virtual society that unites us all, and the responsibility of securing this society must remain a shared and collaborative responsibility; because, as history has already taught us, a threat to cybersecurity that is left to fester unchecked in any corner of cyberspace remains a latent threat to the entire expanse of cyberspace. Hence, the call for the establishment of global cybersecurity legislative frameworks is not one that can be considered to be misplaced; because the safety and security of the cyberspace of the future would continue to look less promising in the absence of such, and with possible retributive consequences lurking in the shadows. But then again, the current top-down approach has failed in consistently yielding effective results in the task of this shared responsibility.

This is because, as has been earlier discussed, contexts play a cardinal role in the design of ethical principles and legislation. Phenomena such as business practice, industry, extent of adoption and use, geographic location, relationship, place, space, agreement, culture and religion, as well as existing regulatory frameworks, all help to define contexts (Baldini et al., 2018). As the capabilities of technology continue to open up new possibilities and choices for action, some of the existing policy definitions and specifications for cybercrimes often quickly become obsolete as the problem of contexts assume a more complex nature due to the fact that contexts can switch very dynamically (between home, office, religious grounds, cross-border interactions, etc.). A central task of computer ethics, therefore, is to determine what should be done in such cases of the policy vacuum which Moor (1985) identified; that is, how to formulate/decisively choose policies to inform and guide right actions in these grey areas. However, one difficulty which was also identified is that along with a policy vacuum there is often a conceptual vacuum. That is, although a problem in computer ethics may seem clear initially, a little reflection might reveal a conceptual muddle, which in part relates to the fact that the theoretical foundations of existing (global/jurisdictional) policies are often difficult to understand and correctly adapt to changing contexts. What is therefore needed in such cases is an in-depth analysis that provides a coherent conceptual framework within which to formulate policies for guiding action (Moor, 1985).

It would likely continue to be a problem to establish effective cybersecurity legislation across the frontiers and boundaries of the digital divide, especially in light of the principle of moral impartiality, posited in Rehg (2015, p.3) as adapted from Habermas's principle of universalisation; stating that "a moral norm (policy, rule) is valid just in case the *foreseeable consequences and side-effects of its general observance for the interests and value-orientations of each individual could be jointly accepted by all those affected without coercion*." In other words, it is only on the basis of prior knowledge of the multifaceted consequences and side-effects of observing a policy/rule with respect to the interests and values of individuals who willingly choose to be jointly bound by such policy/rule that it actually becomes valid. This would likely remain

difficult to achieve until the gaps created by the digital divide are effectively bridged. Whyte (2018), brought in an associated panel to this reality by drawing attention to the fact that when it comes to the issues to cybersecurity, the traditional obstacles to the construction and definition of new knowledge becomes even more pronounced as attempts now have to be made to tangibly link "technological empirical foundations with socio-physical outcomes."

Furthermore, as the contemporary issues of global cyber peacekeeping begin to take centre stage in civic debates and discourses, the concern of global cybersecurity legislations are expected to emerge repeatedly, time and again, to guide, inform and help to enforce the right use of cyberspace resources and capabilities. The following recommendations are offered.

5 Recommendations

Indeed, as sources such as Garg (2018) have rightly opined, if the digital future and global information society that we all envisage would come to fruition, then "harmonization of data privacy and security compliance requirements, expectations, policies, regulations, and laws across every region and border is absolutely necessary." However, as has already been established, it would remain difficult to immediately arrive at a globally acceptable cybersecurity legislative framework due to a convoluted mix of imposing factors of a polysomic nature, which have been discussed in this research. A soft landing out of this quagmire would be to begin with the establishment of consensuses on issues and concerns of cybersecurity amongst states and regions that roughly fall on the same sides of the digital divide, and gradually begin to work a way up towards a global consensus. This is in line with the call by Essien (2018b) for a new set of rhetoric and metaphors for conceptualising, describing, understanding, valuing and managing the issues posed by the digital divide.

Indeed, several attempts to categorise countries based on their levels of technological advancement and development have been embarked on in the past. Some of these existing categorisations have been on the basis of the number of technology users/subscribers, extent and capability of national technology infrastructure, commitment to certain global technological specifications/regulations, and effectiveness of technology policy and regulatory measures, to mention a few; and it has often been noticed that certain states/regions could fall within similar categories in such attempts. Hence, regardless of the yardsticks or metrics for such categorisations, it may be possible and actually much easier to reach a consensus regarding what characteristics would define a particular technological abuse or misuse as a cybercrime within certain of such technological development categories/regions, and what investigative and evidence-gathering measures would be best suited for their local technological contexts; especially since the organisation of contemporary political alliances such as the United Nations, Economic Community of West African States, European Union, NATO and the likes typically lump member states together within a structure that does not make it easy for those states with fairly similar technological strengths and rates of development to achieve a cohesion that could enable them reach a consensus on issues of legislation that could have a wider acceptability within the context of their technological capabilities and development. This is a proposition that is in a sense similar to the 'multilateral' model of global internet governance adopted by China, in which stakeholders try to unify their

various contexts towards global governance, but in line with existing higher-level global specifications and requirements (Lewis, 2017).

Ultimately, however, we must all get to agree that the phenomenon of cyberspace is one that is truly complex, and which would continue to remain difficult to regulate, and that discussions relating to cyberethics are yet likely to remain polarised into the near future; especially because cyberspace and the internet are still considerably at their gestational stages of existence. But then, by starting small to arrive at these agreements, commendable strides can be made towards progress. While the call for a global legislative framework for cybersecurity may be one that would remain a subject of polemical discussion for a long time to come, we can begin to adopt a more bottom-up approach to pursuing this vision as against the current top-down approaches. Let individual countries and jurisdictions begin to establish and strengthen the effectiveness of their domestic cybersecurity legislations; and then when groups of these countries come together, a start off point for discussions would be on the basis of inherent similarities in their existing individual legislations. Thus, we can begin to gradually build up towards a more globally acceptable framework; as against the reverse being the case, where such agreements are made at the global levels of discussion and handed down to the lower level member states for implementation, which may eventually come off to them as parochial and non-circumspective in perspective.

6 Conclusions and future research

The calls for Global Cybersecurity Legislation is one that is likely to remain of a contentious nature even into the near foreseeable future. This paper has been able to review and analyse complex and co-occurring polysomic factors, as well as provide perspective and discuss implications of the associated realities that impede the success of these calls. Recommendations have been given to help to gradually beat a progressive path towards the realisation of a global cybersecurity legislative framework, and these are hoped to engender constructive debate and progressive discussions amongst stakeholders, academics and researchers, practitioners, jurors, legislators and policy makers towards this goal.

References

Aaronson, S.A. and Leblond, P. (2018) 'Another digital divide: the rise of data realms and its implications for the WTO', *Journal of International Economic Law*, Vol. 21, No. 2, pp.245–272, DOI: 10.1093/jiel/jgy019.

Baldini, G., Botterman, M., Neisse, R. and Tallacchini, M. (2018) 'Ethical design in the internet of things', *Science and Engineering Ethics*, June, Vol. 24, No. 3, pp.905–925, DOI: 10.1007/s11948-016-9754-5.

Buchanan, B. (2017) *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*, Oxford University Press, Oxford, DOI: 10.1093/acprof:oso/9780190665012.001.0001.

Choucri, N., Madnick, S. and Ferwerda, J. (2014) 'Institutions for cyber security: international responses and global imperatives', *Information Technology for Development*, Vol. 20, No. 2, pp.96–121, DOI: 10.1080/02681102.2013.836699.

Christian, F., Robert, B. and Celina, R. (2009) 'Cyberethics and co-operation in the information society', *Science and Engineering Ethics*, Vol. 15, No. 4, pp.447–466, DOI: 10.1007/s11948-009-9138-1.

Cohen, Z. (2017) *North Korean Hackers Stole US-South Korea War Plans, Official Says*, CNN, 11 October [online] https://edition.cnn.com/2017/10/10/politics/north-korea-hackers-us-south-korea-war-plan/index.html (accessed 17 February 2018).

Council of Europe (CoE) (2015) *Convention on Cybercrime – CETS No. 185*, The Council of Europe's Official Treaty Office, 24 April [online] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (accessed 18 April 2019).

Essien, E.D. (2018a) 'Ethical dilemma of the digital divide in the threshold of social inequalities in Africa', in *Ethics and Decision-Making for Sustainable Business Practices*, pp.73–89, IGI Global, DOI: 10.4018/978-1-5225-3773-1.ch005.

Essien, E.D. (2018b) 'Ethical implications of the digital divide and social exclusion: imperative for cyber-security culture in Africa', *International Journal of Innovation in the Digital Economy*, Vol. 9, No. 1, pp.14–25, DOI: 10.4018/IJIDE.2018010102.

Froehlich, T.J. (1992) 'Ethical considerations of information professionals', in Williams, M.E. (Ed.): *Annual Review of Information Science and Technology (ARIST)*, Vol. 27, pp.291–324 [online] https://eric.ed.gov/?id=EJ481924 (accessed 18 April 2019).

Frohmann, B. (2008) 'Subjectivity and information ethics 1', *Journal of the American Society for Information Science and Technology*, Vol. 59, No. 2, pp.267–277, DOI: 10.1002/asi.20742.

Garg, R. (2018) *Open Data Privacy and Security Policy Issues and its Influence on Embracing the Internet of Things*, First Monday [online] http://www.firstmonday.dk/ojs/index.php/fm/article/view/8166/7211 (accessed 9 September 2018).

Guidoboni, T.A. and Meltzer, E.R. (1991) *United States v. Morris, 928 F. 2d 504*, US Court of Appeals, United States Department of Justice, Washington, DC [online] http://scholar.google.com/scholar_case?case=551386241451639668 (accessed 26 April 2015).

Herman, T. (2001) 'The state of computer ethics as a philosophical field of inquiry: some contemporary perspectives, future projections, and current resources', *Ethics and Information Technology*, Vol. 3, No. 2, pp.97–108, DOI: 10.1023/A:1011889808481.

IMPACT (2015) *International Multilateral Partnership against Cyber Threats*, IMPACT Alliance [online] http://www.impact-alliance.org/home/index.html (accessed 1 September 2018).

International Telecommunication Union (ITU) (2008) *Global Strategic Report*, Cybersecurity Gateway [online] http://www.cybersecurity-gateway.org/pdf/global_strategic_report.pdf (accessed 31 August 2018).

International Telecommunication Union (ITU) (2012) *ITU-D ICT Applications and Cybersecurity Division Publications*, ITU International, 29 March [online] http://www.itu.int/ITU-D/cyb/publications/ (accessed 1 September 2018).

International Telecommunication Union (ITU) (2018) *About International Telecommunication Union (ITU)*, ITU International [online] https://www.itu.int/en/about/Pages/default.aspx (accessed 1 September 2018).

Johnson, D.G. (1985) *Computer Ethics*, Prentice-Hall Publishers, New Jersey, NJ, USA.

Kavuk, M., Keser, H. and Teker, N. (2011) 'Reviewing unethical behaviors of primary education students' internet usage', *Procedia-Social and Behavioral Sciences*, Vol. 28, pp.1043–1052.

Laudon, K.C. (1995) 'Ethical concepts and information technology', *Communications of the ACM*, December, Vol. 38, No. 12, pp.33–39, DOI: 10.1145/219663.219677.

Lee, T.B. (2013) *How A Grad Student Trying to Build the First Botnet Brought the Internet to its Knees*, The Washington Post, Washington.

Lewis, D. (2017) *China's Global Internet Ambitions: Finding Roots in ASEAN*, Institute of Chinese Studies (ICS), Delhi, India [online] http://www.icsin.org/uploads/2017/08/03/5daba78af515cb7bc67e43ae7c1d4ba1.pdf (accessed 1 September 2018).

Maurer, T. (2018) *Cyber Mercenaries*, Cambridge University Press, Cambridge.

Moor, J.H. (1985) 'What is computer ethics?', *Metaphilosophy*, October, Vol. 16, No. 4, pp.266–275 [online] https://www.jstor.org/stable/24436819 (accessed 18 April 2019).

Onyancha, O.B. (2015) 'An informetrics view of the relationship between internet ethics, computer ethics and cyberethics', *Library Hi Tech*, Vol. 33, No. 3, pp.387–408.

Rehg, W. (2015) 'Discourse ethics for computer ethics: a heuristic for engaged dialogical reflection', *Ethics and Information Technology*, Vol. 17, No. 1, pp.27–39, DOI: 10.1007/s10676-014-9359-0.

Schia, N.N. (2018) 'The cyber frontier and digital pitfalls in the Global South', *Third World Quarterly*, pp.821–837, DOI: 10.1080/01436597.2017.1408403.

Sembok, T.M. (2003) 'Ethics of information communication technology (ICT)', *Proceedings of the Regional Meeting on Ethics of Science and Technology*, UNESCO: Regional Unit for Social & Human Sciences in Asia and the Pacific (RUSHSAP), Bangkok, November, pp.239–325.

Sinrod, E.J. and Reilly, W.P. (2000) 'Cyber-crimes: a practical approach to the application of federal computer crime laws', *Santa Clara Computer & High Tech. LJ*, Vol. 16, p.177.

Smeets, M. (2018) 'Integrating offensive cyber capabilities: meaning, dilemmas, and assessment', *Defence Studies*, pp.1–16, DOI: 10.1080/14702436.2018.1508349.

UN (2018) *Agencies of the UN: ITU*, United Nations Agencies [online] https://www.un.cv/agency-itu.php (accessed 1 September 2018).

UNESCO (2004) *The COE International Convention On Cybercrime Before Its Entry Into Force*, United Nations Educational, Scientific and Cultural Organization (UNESCO), January–March, 24 April [online] http://portal.unesco.org/culture/en/files/19556/11515912361coe_e.pdf/coe_e.pdf (accessed 2 January 2018).

Westby, J.R. (2013) *Legal Guide to Botnet Research*, American Bar Association (ABA) Publishing, Illinois.

Whyte, C. (2018) 'Crossing the digital divide: monism, dualism and the reason collective action is critical for cyber theory production', *Politics and Governance*, 11 June, Vol. 6, No. 2, pp.73–82, DOI: 10.17645/pag.v6i2.1338.

World Summit on the Information Society (WSIS) (2009) *WSIS Action Line C5*, Cybersecurity Gateway [online] http://www.cybersecurity-gateway.org/wsis.html (accessed 31 August 2018).