Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
January - June 2021. Vol. 15(1): 65–78. DOI: 10.5281/zenodo.4766533
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

History, Evolution and Challenges of Cyber Criminological Scholarship

Philip N. Ndubueze[1]
Federal University Dutse, Jigawa State, Nigeria.

Abstract

The digital revolution has undoubtedly produced new patterns of crime and deviance in contemporary societies and has created new research agenda for the discipline of criminology. The discipline of cyber criminology was founded in 2007 by Indian Criminologist, Professor Karuppannan Jaishankar. Though, still in its infancy; the emerging sub-field is fraught with several challenges. Since, its inception most research efforts on cyber criminology have tended to be cybercrime-biased, thereby neglecting the other two important components of the sub-discipline: cyber deviance and cyberterrorism. This paper discusses the history and evolution of cyber criminology as well as the challenges confronting cyber criminological scholarship. It calls for the restructuring of criminology curriculum at undergraduate and postgraduate levels to include a course on cyber criminology. It also calls for the introduction of Bachelor's degree in cyber criminology programme across universities around the world.

Keywords: Cyber criminology; cybercrime, cyber deviance; cyberterrorism; restructuring; scholarship.

Introduction

Cyber criminology is one of the latest sub-disciplines of Sociology, pioneered by Indian criminologist, Jaishankar (2007) to interrogate issues around the growing wave of deviance, crime and terrorism in the cyberspace and the need to restore social order (P. Ndubueze, 2017b; Philip N Ndubueze, 2016). The discipline of criminology was established in the 1900s, while the first textbook in the field was published in 1920s (Reid, 2017). Conversely, the discipline of cyber criminology which was founded in 2007, had its first textbook titled "Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour" published in 2011 by CRC Press, Bacon Raton (Jaishankar, 2007; Jaishankar, 2011). However, two other cyber criminology textbooks titled: *Cyber Criminology and Technology-Assisted Crime Control* and *Cyber Criminology* were published in 2017 by Ahmadu Bello University Press, Zaria, Nigeria (P. Ndubueze, 2017a) and by Springer Nature Switzerland, AG (Jahankhani, 2018) respectively.

It has been argued that although the breakthrough in cyber technology has facilitated communication and commerce around the world, it has also facilitated a corresponding

[1] Department of Sociology, Federal University Dutse, Nigeria. Email: pnndubueze@gmail.com

increase in crime and criminality in the cyberspace with far-reaching new implications for policing (P. Ndubueze, 2017a). Thus, deployment of effective counter measures against cyber-attacks is presently a struggle for governments around the globe (Diamond & Bachmann, 2016; Kanungo & Chattoraj, 2020). The cyberspace offers new scope to criminologists (Jaishankar, 2007). Called as fifth battle field (cyberspace), it has set a new research agenda for scholars genuinely concerned about the escalating problem of deviant, criminal and terrorist use of the Internet and associated/emerging digital technologies. The discipline of criminology and its newest off-spring cyber criminology belong to the parent discipline of sociology. While criminology is well established as an academic field of study, it is still early days for cyber criminology. Arguably, accepting the fact that the discipline is still in its infancy, not much progress has been made in advancing cyber criminological scholarship around the world.

More specifically, cyber criminological scholarship from the inception of the new discipline has been cybercrime biased. The extant literature of cyber criminology has tended to focus more on the component of cybercrime, thereby neglecting the other two important components (e.g., cyber deviance and cyberterrorism). The emerging issues around the emergence of the internet and digital technology are too numerous and varied to be subsumed under cybercrime. There is therefore the need to bring to the fore the problem of the neglect of cyber deviance and cyberterrorism in many cyber criminological discourses and to underpin the need for the restructuring of cyber criminology curriculum to include them. It is this objective that this paper seeks to achieve.

This paper examines the history and evolution of criminological and cyber criminological scholarships. It underscores the need to restructure the curriculum of cyber criminology to encompass cyber deviance and cyberterrorism, in addition to cybercrime. Challenges of cyber criminological scholarship are also examined and appropriate recommendations made.

The Scope of Cyber Criminology

Before discussing the history and evolution of cyber criminology, it is instructive to first examine the scope of the novel discipline. T. Holt et al. (2015) have categorized the various deviant and criminal activities that are perpetrated in the cyberspace into three: cyber deviance, cybercrime and cyberterrorism. Borrowing from T. Holt et al. (2015) premise, P. Ndubueze (2017a) identifies cyber deviance, cybercrime and cyberterrorism as the traditional concern of the discipline of cyber criminology. He depicted three components as shown in Figure 1:

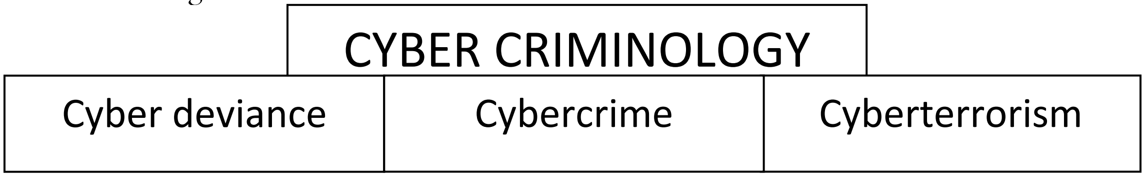

Figure 1: The Scope of Cyber Criminology (P. Ndubueze, 2017a)

Cyber deviance: The term cyber deviance is used to refer to online behaviors that may not necessarily be illegal but are clearly contrary to the formal and informal norms or beliefs of the dominant culture (Thomas J Holt et al., 2017; P. Ndubueze, 2017a). In this era of digital revolution, there are several aberrant and morally reprehensible behaviors that occur on the internet, especially on the social media. These acts are normally frowned at by society; even though they do not attract any criminal sanction from the state. Examples may include: social media addiction, sharing of religious posts on a professional WhatsApp group, use of social media language in a formal email communication, use of official airtime for personal calls and so on.

*Cybercrime***:** According to Thomas J Holt et al. (2017) "activities that violate codified legal statuses move from deviance to criminal acts". There is a wide spectrum of online activities that contravene the law in various jurisdictions. Such activates that are prohibited by the state and for which there are prescribed punishments are known as cybercrime. Examples include: online romance scam, online lottery scam, online employment scam, cyberstalking, identity theft, revenge pornography, credit card fraud, sim-card fraud, digital child pornography, phishing, unlawful interceptions, intellectual property theft, and so on.

*Cyberterrorism***:** Terrorism is an age-long global security problem. However, its scope has fundamentally been altered with the emergence of the internet infrastructure and widespread use of digital devices. Cyberterrorism is defined as "the use of digital technology or computer-mediated communications to cause harm and force social change based on ideological or political beliefs" (Thomas J Holt et al., 2017). Today, several terrorists' organizations and their sympathizers use the internet to pursue and promote different kinds of terrorist activities. The internet has become an effective tool for radicalization of recruitment and funding of terrorists faithful in this age of digital revolution. Example of cyber terrorism are online recruitment by terrorist organizations, denial of service attacks by terrorist groups, web defacement by terrorist groups, and so on.

It is important to note that these three components of cyber criminology may overlap and the boundaries may not be so clear-cut as delineated above. Nonetheless, the mapping of these three basic components of cyber criminology is helpful, as it allows scholars and researchers to more systematically study each of the phenomenon. However, it can be attributed that each has certain unique features that makes it clearly distinct. But, cyber criminological thinking and theorizing from inception has been cybercrime biased. There have been relatively few studies interrogating the upsurge of deviance and terrorism in the cyberspace.

Theoretical framework and literature review

Criminological Scholarship and Its Challenges in the Global South

Before looking at the history and evolution of cyber criminological scholarship, it is perhaps instructive to briefly examine the state of criminological scholarship and its challenges in the global south. It is observed that during the late 1800s and early 1900s, criminology had become a distinct area of inquiry. Garofalo, Durkheim and Bonger had stood out among its most distinguished contributors (Arab, 2020; DiCristina, 2016; Husár et al., 2020). It is argued that "classical" criminology is also tied to the Enlightenment of 18th and 19th centuries basically because of its focus on human reason, value, and agency as opposed to the earlier harsh treatment of offenders propelled by arbitrary action and authority of the state (Hunt, 2021). Some pioneering criminological institutes were established in Graz and Rome in 1912, in Vienna in 1922, in Moscow in 1923, in Paris in 1924 and in Prague in 1930 (Kyvsgaard, 2012; Metcalfe et al., 2020).

Expectedly, the discipline of criminology since its establishment has been confronted by several challenges. P.N. Ndubueze (2020) recently identified the lack of methodological rigor, lack of replication of studies, questionable research practices, masculinist and racist bias, quantitative and qualitative divide, and lack of influence over criminal justice policy as some of the challenges of criminological inquiry. But aside the aforementioned challenges, citing many scholars, Carrington et al. (2018) opine that "at present, the production of knowledge in the social sciences, including criminology, is heavily skewed towards a select number of global North countries, and especially English-speaking countries, whose journals, conferences, publishers and universities dominate the intellectual landscape". Carrington et al. (2018)*'s* arguments undoubtedly captures the true state of criminological scholarship in the global south. For example, unlike what is obtained in the global north, there are fewer dedicated criminology text books, journals and conferences in the global south.

Furthermore, some epistemological, methodological and ethical challenges confront criminological scholarship in the global south. For example, it is argued that "there is no global social justice without global cognitive justice…there is no form of knowledge to which we can attribute, in general, an epistemological privilege" (de Sousa Santos as cited in Cunneen (2018)). Cunneen (2018) further pointed out that cognitive justice can only be achieved by understanding and applying different epistemological positions. He warned that failure to do so would by implication re-inscribe the epistemic violence of colonial rule. Drawing from the North/South divide earlier mentioned in this section, he maintained that if Southern criminology does not sufficiently consider epistemologies of the South and their differing ontologies, it runs the risk of re-centering Eurocentric (criminological) knowledge and becoming an exercise in comparative or transitional criminology.

Similarly, Cunneen (2018) explained that indigenous knowledge is local, holistic and oral. They are transmitted through storytelling, rituals, art, dance and ceremonies, and valued knowledge, he further highlighted comes from among other sources, dreams, the ancestors, stories and experience which have depth in relationships to the social and physical environment. He opined that conversely, dominant Western theories of knowledge are based upon notions of objectivity, that see reason as the climax of the hierarchy of knowledge production and that knowledge status is limited to the educated and social elite. He observed that within criminology, there has been very little understanding of the importance and application of indigenous ontologism in the consideration of crime and criminal justice response. Again, he pointed out that indigenous axiology and ethics necessitates a collaborative social science research model. He said that this would entail that research be for the benefit of Indigenous communities and that no research project is worth embarking upon if it does not benefit the community by improving the quality of life for those in the community.

Cunneen (2018) treatise has raised very fundamental questions about the current state of criminological scholarship in the global south. How much have criminologists in countries of the global south been able to domesticate knowledge production in the discipline? Are criminologists in the global south not often 'promoters' of Eurocentric paradigms? How much has our research impacted our communities? Indeed, answers to these critical questions would have huge implications for the future of criminological scholarship in countries of the global south.

Nonetheless, it should be pointed out that the future of criminological scholarship in the global south is not entirely gloomy. In African and Asia for example, the past one decade or so has witnessed an increased interest in criminological and allied scholarship. More and more sociologists are now specializing in criminology and this has served to increase the volume of criminological studies in their universities. Moreover, many universities are realizing the relevance of criminological studies to national security and development and are beginning to mount programs in criminology and related fields. For example, in 2011, Federal University Dutse, Nigeria mounted a Bachelor of Science program in Criminology and Security Studies, perhaps becoming one of the first few conventional universities to do so in the country and in 2018 the University commenced a Master of Science in

Criminology and Security Studies, thereby becoming among the first to do so in the country. These very commendable efforts will promote criminological scholarship and would ultimately pave way for the introduction of a Bachelor of Science program in Cyber Criminology. Already, cyber criminology is one of the taught courses approved for the M.Sc. Criminology and Security Studies at Federal University Dutse, Nigeria. It is expected that sister universities will do likewise in due course.

Results and findings

History and Evolution of Cyber Criminological Scholarship

In the past two decades or so, cyber criminological scholarship has made some remarkable, though skewed progress. Thomas J. Holt and Bossler (2014) appreciated this progress when they posited that:

Over the last 20 years, there has been a substantial increase in the research literature on various forms of cybercrime. These studies have expanded our knowledge of the prevalence of cyber-crime offending and victimization as well as the general influence of technology on various forms of offending behaviors [Emphasis added].

The above quotation seems to suggest that these 20 years of cyber criminological scholarship has been more about cybercrime and less about other variants of offending behaviors online. Since 2007, when cyber criminology was founded by Professor K. Jaishankar, up until the present day, there has been several efforts by cyber criminologists to understand the problem of crime and disorder in the cyberspace. But as mentioned earlier, such efforts have tended to be skewed towards cybercrime. Not so much research has been carried out in the areas of cyber deviance and cyber terrorism. For example, Payne and Hadzhidimova (2020) acknowledge the increase in criminological research on cybercrime over the past twenty years. They argue that since cybercrime [not cyber criminology] is interdisciplinary in nature, cyber criminologists should collaborate with scholars in other disciplines. Bossler and Berenblum (2019) observe that unlike in the past, cybercrime-related presentation in national and international conferences are growing every year,

Cyber criminology has undoubtedly suffered years of neglect by mainstream criminology. For example, until recently, many criminology text books do not include a chapter on cyber criminology or cybercrime. There is a paucity of dedicated textbooks on cyber criminology and very few studies so far have empirically investigated issues surrounding the escalation of deviant and criminal behavior in the cyber space. However, this scenario seems to be changing as there is currently a growing interest in cyber criminological issues across the world, including Nigeria.

According to Diamond and Bachmann (2016) “for the past eight years, the young discipline has grown with the contributions of many experts, including the exceptional efforts of its founder, Jaishankar (2018a) noted that being over ten years old the discipline of cyber criminology has successfully entered the portals of academia by way of courses beginning from minor courses such as those of University of Alabama, Regis University, and Purdue University to the Associate in Arts degree at Arizona Western College, USA. Besides, he noted that many doctoral researchers are focusing on cyber criminology. Today, there is a remarkable increase in the number of undergraduate final year research projects, Master of Science dissertations and Doctor of Philosophy theses that focus on cyber criminological issues. Worthy of note is the immense contribution of cyber criminologists around the world in bringing to fore the discipline of cyber criminology through research articles and book chapters. For example, Jaishankar (2007) brought the new discipline to the fore with his article: "Cyber Criminology: Evolving a Novel Discipline with a New Journal," in the first volume and first issue of the first cyber criminology journal: *International Journal of Cyber Criminology* and ever since published several articles/chapters to review the progress and prospects of the discipline of cyber criminology (Jaishankar, 2010, 2011; Jaishankar, 2018a; Jaishankar & Ngo, 2017). Similarly, a Nigerian cyber criminologist (the author) has also examined the concern, context and future directions of cyber criminology scholarship (Philip N Ndubueze, 2016; P. N. Ndubueze, 2017). An American cyber criminologist (Diamond & Bachmann) has also assessed the obstacles, challenges and prospects of cyber criminology (Diamond & Bachmann, 2016).

These developments are very inspiring and commendable as they would further deepen the depth and expand the frontiers of cyber criminological scholarship. It is expected that in the years to come, the discipline of cyber criminology will assume an enviable position in the ranking of academic disciplines around the world. This is because individual internet users, corporate organizations and the government would more than ever before appreciate the need to unravel the "mystery" behind the increased online victimization. They will also see the need to better protect themselves and critical national infrastructure from cyber-attacks.

Challenges of Cyber Criminological Scholarship

Since 2007 when it was formally established with the academically coining of the word "cyber criminology" by the renowned Indian criminologist, Professor Karuppannan Jaishankar; the discipline of cyber criminology has had to contend with several challenges. This was acknowledged by Jaishankar (2018b) when he observed that:

The new breed of criminal activities and offenders in cyber space also present law enforcement officials and prosecutors with issues and challenges in the investigating of cybercrime and prosecuting of cyber criminals. While there exists a sizeable and growing body of literature on cybercrime, there are also research gaps that need to be addressed.

Cyber criminology scholars and researchers have attempted to identify some of the challenges confronting the young discipline. The author has in a previous work highlighted some of these challenges (Philip N Ndubueze, 2016). Some of the challenges are briefly discussed below:

a) **Definitional and Classification Issues:** There is no universally accepted definition of cybercrime; therefore, the term "cybercrime" is used interchangeably with several other terms, such as, computer crime, Internet crime, computer-related crime, online crime, high tech crime, electronic crime, technology crime, and information age crime (Jaishankar, 2018a). Related to the issue of definition is classification. Scholars have also attempted to classify cybercrime differently. For example, Brenner (2001) classified it into four legal-biased categories: i) Prohibited conduct (*actus resus*). ii) Capable mental state (*mens rea*). iii) Attendant circumstances. iv) Forbidden result or harm. Wall (2001) classified cybercrime into four types: cyber trespass, Cyber deception/theft, Cyber pornography/obscenity, and Cyber violence. Wall (as cited in Jaishankar and Ngo (2017)) viewed cybercrime from four perspectives: i) Crimes against machines (especially those that bother on integrity such as harmful trespass. ii) Crimes using machines (such as computer related crimes like acquisition of domain or profile, theft or deception. iii) Crimes in the machine (these are content related crimes such as online obscenity which may involve online sex trade, cybersex and cyber pimping). (iv) Crimes in the machine (content related crimes can also result to violence that may invariably lead to conventional crimes like stalking and personal harassment.

Cybercrime has also been classified based on the role technology play in their commission. Furnell (2002) classified cybercrime into two types: i) Computer-assisted crimes, which use computer to facilitate the act, however the main offence existed before the emergence of computers or can be perpetrated without computers. Examples include fraud, theft, pornography etc. and ii) Computer focused crimes, which include offences that are direct product of computer technology such as hacking, web site defacement and virus/worm attacks. This lack of consensus on definition and classification of cybercrime complicates elementary discourse on cybercrime and sometimes confuse emerging cybercrime researchers.

b) **Reporting and Measurement Issues**: The victim's decision to report crime to law enforcement is a vital step in the criminal justice process (Reyns & Randa, 2017). People do not always report all their crime victimization to the police (Hope, 2013), as crime victims want to be confident that the information they provide to the police will be treated with the highest level of confidentiality. They also want to be assured that their cases will be efficiently and fairly treated and that they will not suffer further victimization by the system (Boateng, 2018).

The study of crime revolves around two most critical issues: crime measurement and instrumentation (Jennings & Reingle, 2014). It has been noted that currently, there is a lack of reliable and valid statistics on the nature, prevalence, trends and impact of cybercrime (Jaishankar & Ngo, 2017). It is noted that even though cybercrime is rapidly increasing, most victims do not report it to the police and that determinants of crime reporting differs between traditional crime and cybercrime; between different variants of cybercrime and between reporting cybercrime to the police and to other organizations (van de Weijer et al., 2019).

There are many reasons why cybercrime is under-reported. First, it is a technical type of crime and thus because of its complex nature some victims may not be aware that they have been victimized and even when they are aware, they may not appreciate the potential risk or extent of damage that is associated with such victimization. Second, some victims may not have confidence in the public police service's capacity to handle their complaint and track the offender. Third, some victims especially the corporate category, may likely be scared of the negative publicity that such victimization may cause them if its news eventually goes viral. They may be concerned that they may lose their customers.

c) **Lack of Official Statistics**: The reporting challenge discussed in (b) above has exacerbated the official statistic problem of cybercrime. Because cybercrime is critically under-reported, it is grossly under-represented in official crime statistics. Bossler and Berenblum (2019) argue that the lack of statistics on most variants of cybercrime has been a significant challenge to cybercrime scholars. Unless a critical mass of internet users become more aware of the modus operandi of cyber criminals and the extent to which they can potentially suffer loss as result of cyber-attacks, they would not report cybercrime and official statistics of cybercrime will remain ridiculously low.

d) **Theoretical Issues**: Cybercrime is a complex form of crime. Due to its evolving and technical nature, traditional criminological theories may not sufficiently explain this complex nature of cybercrime. This therefore, necessitates the establishment of cybercrime-oriented theories. Thomas J. Holt and Bossler (2014) noted that cybercrime studies utilize components from traditional criminological theories, especially routine activity theory (RAT), social learning theory (SLT) and general theory of crime (GTC). The first and so far only attempt at developing a cybercrime specific theory was made by Jaishankar in 2008 (see, Jaishankar (2008)).

e) **Suppression by Mainstream Criminology**: Mainstream criminology has dominated criminological scholarship around the globe. This is in spite of the spirited efforts by cyber criminologists to advance the frontiers of the new discipline. Many criminology textbooks do not have dedicated chapters on cyber criminology. A few marginally cover cybercrime issues and often neglect the growing problem of deviance and terrorist use of the Internet architecture (see Philip N Ndubueze (2016)). It was not until 2017 that the first dedicated book on cyber criminology in Nigeria was published (see P. N. Ndubueze (2017)). This suppression is also evidenced in conference themes and sub-themes particularly in African and Nigeria. This is a major challenge as dedicated cyber criminologists as a result of this gap struggle in their bid to frame a cyber-criminological topic that will find expression in the broader theme of such conferences.

f) **Teaching Issues**: According to Jaishankar (2018a) cybercrime is separately taught by cyber security/forensic specialists, cyber lawyers and cyber criminologists. He decried the compartmentalization of the current teaching in cyber criminology and underscore the need for a holistic teaching which is guided by a curriculum that cuts across social science law and technology. Jaishankar's proposal further accentuates the ongoing call for more interdisciplinary collaborations and partnerships in teaching and research. In the digital age, disciplinary boundaries are increasingly becoming fluid. For example, in the Federal University Dutse, Nigeria, some academic staff (including the author) of the Department of Sociology that houses Criminology and Security Studies programs at the undergraduate and postgraduate levels teach courses in the Department of Cyber Security of the university that offers B.Sc. Cyber Security program. Nonetheless, as of date, to the best of the researcher's knowledge, only the Department of Sociology, Federal University Dutse, Nigeria and the National Open University of Nigeria, Abuja offer unit courses in Cyber Criminology. There are currently only 25 universities in Nigeria that offer programs in Criminology and Security Studies (V. Pillah, personal communication, 9th April, 2021). Most of these programs are offered at Bachelor of Science level where cybercrime is taken as a course unit and not cyber criminology.

g) **Skewed Nature of Cyber Criminological Research**: Cyber criminological research is cybercrime heavy. Scholars have tended to focus more on studying cybercrime, thereby neglecting the other two components of cyber criminology: cyber deviance and cyber terrorism. Thomas J. Holt and Bossler (2014) have noted that little research exist on cyber terrorism and online extremism. This is disturbing given that terrorist organizations are increasingly using the Internet to recruit, train and deploy their members. For example, Boko Haram (BH) and the Islamic State of West Africa Province (ISWAP) are increasing using the social media as a propaganda tool in the digital age.

h) **The Global North/South Divide**: The global north/south divide is not only cultural and economical; it is also intellectual. Carrington et al. (2018) argued that "at present, the production of knowledge in social sciences, including criminology, is heavily skewed towards a select number of global North countries, and especially English speaking countries, whose journal, conferences, publications and universities dominate the intellectual landscape". They further noted that this is not just a question of quantities output but also of cultural and intellectual hegemony. In the same vein, Gabbidon and Greene (2001) had earlier found that while early criminology texts contain different citations to African American scholarship, a few of the early texts that did not maintained that trend in the editions that followed. Arguably, this trend has continued for too long and applies to scholarship in the discipline of cyber criminology. For example, while

Jaishankar's Space Transition Theory has received global recognition and despite the fact that it is till date the only cybercrime specific theory, it seems popular in the global south. Routine Activity Theory (RAT) as a theoretical framework has continued to dominate discourses on crime and deviance in the cyberspace among global north scholars. For example, see, Thomas J. Holt and Bossler (2008), Kigerl (2012), Leukfeldt and Yar (2016), Reyns et al. (2016) and so on.

i) **Dearth of Dedicated Research Centres**: There are not enough cyber criminological research centers across the world but especially in the global south. The notable ones are: Oxford Internet Institute Oxford, Franser Simon Cybercrime Centre, Canada, Austrian etc. Establishment of more of such centers will certainly enhance both the scope, quality, volume, dissemination and impact of cyber criminological studies across the globe.

j) **Paucity of Dedicated Journals:** Again, only few dedicated cyber criminological journals currently exist. Top among them being the one floated by the founding father of cyber criminology himself: International Journal of Cyber Criminology, which marked its one-decade anniversary only in 2017. Others are: Journal of Cyber Security, published by the Oxford University Press. An early cyber criminologist, Michael Bachmann of Texas Christian University, United States made efforts in 2014 to publish one, titled: *Journal of Technology and Crime*, but that did not quite pay off as the journal was shut down a few years later due to some operational challenges.

Discussion

Restructuring Cyber Criminology Scholarship

Cyber criminology has a three-fold scholarship focus: cyber deviance, cybercrime and cyberterrorism. Fundamentally, discourses on the deviance and criminal use of the Internet and associated technologies revolve around these three sometimes overlapping themes: cyber deviance, cybercrime and cyberterrorism. However, cyber criminological researchers and texts have form the outset being cybercrime biased. For example, while there are a few published dedicated cyber criminology texts around the world such as Jaishankar (2018b), Jaishankar (2011) and P. Ndubueze (2017a); there are many published cybercrime texts such as Gillespie (2015), Graham and Smith (2019), Thomas J. Holt (2016), Thomas J. Holt and Bossler (2016), Johnson (2016), Marcum (2015), Loader and Thomas (2013), Yar and Steinmetz (2019), Wall (2001). Again, there are fewer studies that have investigated non-criminal online deviant behavior and terrorist use of the internet when compared to those that have examined the various forms criminal behavior online.

Scholars and researchers have tended to focus more on the cybercrime component of cyber criminology thereby relegating the other two critical components (cyber deviance and cyberterrorism) to the background. Obviously, unpacking these three important components of cyber criminology will allow scholars to more rigorously investigate them. Furthermore, restructuring of cyber criminological scholarship would entail making frantic efforts to address the challenges confronting the discipline, which are discussed in the preceding section of this article. While, these challenges cannot be tackled overnight, genuine concern about them, backed by practical steps in resolving them would positively impact on the tenor of cyber criminological scholarship.

Finally, and more specifically, restructuring would entail taking practical steps to indigenize the scope, content and impact of cyber criminological researchers by countries where the program is offered around the world. Cyber criminological researches should be largely be locally inspired and focused. Above all. Cyber criminological research should speak to the practical needs of the program host countries by proffering possible practical solutions to the escalating problems that linger in the cyberspace and how they unsettle their citizens.

Conclusion

Cyber criminology, though still at its infancy and confronted with a myriad of challenges, has indeed made some giant strides in the fourteen years of its existence. This paper examines state of criminology and its challenges in the global south; the history and evolution as well as challenges of cyber criminology scholarship. It noted that whereas the discipline of cyber criminology comprises of three components: cyber deviance, cybercrime and cyber terrorism; the cybercrime component is emphasized at the detriment of the cyber deviance and cyber terrorism components. The paper calls for the restructuring of the focus of cyber criminology scholarship to include these relegated but equally important components and the domestication of cyber criminological research endeavor by scholars across the globe but particularly by those of the global south. The paper also called for criminologists interested in interrogating the escalating problems of deviance, crime and terrorism in the cyberspace to join the advocacy for the introduction of cyber criminology program at bachelor's level across conventional universities around the globe.

Given the emerging nature of deviance, crime and terrorism in the cyberspace, it is safe to posit that cyber criminological scholarship has a huge scope and prospect. What is required is the restructuring or re-engineering of its scope to engender a more aggressive and focused approach in the quest to interrogate the emerging dynamics of crime and disorder in the cyberspace. The following policy recommendations are considered potentially useful for restructuring cyber criminological scholarship:

1. Universities may consider developing a Benchmark for Minimum Academic Standards (BMAS) for the introduction of a Bachelor of Science program in Cyber Criminology. The program may be housed in Sociology or Criminology departments. This will provide the opportunity for scholars and students to more methodologically investigate issues surrounding cyberspace deviance, crime and terrorism. It will also help to train a more "cyber-oriented" and "internet-aware "manpower for law enforcement and security services. It will no doubt enhance both teaching and research in cyber criminology. Existing criminology, criminal justice and security studies or related program around the world may begin to contemplate the introduction of a Bachelor of Science program in Cyber Criminology in their respective universities.
2. There is need for cyber criminologists to restructure their research focus to include the other two critical components of cyber criminology: cyber deviance and cyber terrorism. This will ensure that cyber criminological scholarship is not skewed towards cybercrime. More so, their research outputs should be tailored to address the real cyber-associated problems of the global south countries.
3. There is need for governments and Universities across the globe to establish more Cyber Security Research Centers. This will serve as a hot-bed for the incubation and dissemination of contemporary researches on the triple-problem of deviance, crime and terrorism in the cyberspace. Such centers will encourage interdisciplinary researches on cyber criminology and cyber security.
4. Cyber criminologists across the globe should make efforts to domesticate the content and impact of their research. They should seek for avenues to properly disseminate their research outputs to not only the academic community but to policy makers and private organizations.

5. Cyber criminologists should encourage their colleagues in allied disciplines to join the crusade for a safe and secure cyberspace. They should be encouraged to research in any aspect of the emerging forms of deviance, crime and terrorism in the cyberspace and be willing to share their findings and recommendations with the academic community, bureaucrats and industrial players.

References

Arab, M. S. (2020). Global Surge in Cybercrimes-Indian Response and Empirical Evidence on Need for a Robust Crime Prevention System. *International Journal of Cyber Criminology, 14*(2), 497-507. http://dx.doi.org/10.5281/zenodo.4772797

Boateng, F. D. (2018). Crime Reporting Behavior: Do Attitudes Toward the Police Matter? *Journal of Interpersonal Violence, 33*(18), 2891-2916. https://doi.org/10.1177/0886260516632356

Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice, 42*(5), 495-499. https://doi.org/10.1080/0735648X.2019.1692426

Brenner, S. W. (2001). Cybercrime investigation and prosecution: the role of penal and procedural law. *eLaw Journal: Murdoch University Electronic Journal of Law, 8*(2), 1-38. https://www.researchgate.net/publication/240610895

Carrington, K., Hogg, R., Scott, J., & Sozzo, M. (2018). Criminology, southern theory and cognitive justice. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave handbook of criminology and the global south* (pp. 3-17). Springer. https://doi.org/10.1007/978-3-319-65021-0_1

Cunneen, C. (2018). Indigenous Challenges for Southern Criminology. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South* (pp. 19-41). Springer International Publishing. https://doi.org/10.1007/978-3-319-65021-0_2

Diamond, B., & Bachmann, M. (2016). Assessment of Cyber Criminology: Obstacles, Challenges, and Promising Paths of the New Science of Cyber Crime. In K. Jaishankar (Ed.), *Interpersonal Criminology* (pp. 279-288). Routledge. https://doi.org/10.1201/9781315368528

DiCristina, B. (2016). Criminology and the "essence" of crime: The views of Garofalo, Durkheim, and Bonger. *International Criminal Justice Review, 26*(4), 297-315. https://doi.org/10.1177%2F1057567716660359

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. Addison-Wesley London. http://informationr.net/ir/reviews/revs053.html

Gabbidon, S. L., & Greene, H. T. (2001). The presence of African American scholarship in early American criminology texts (1918–1960). *Journal of Criminal Justice Education, 12*(2), 301-310. https://doi.org/10.1080/10511250100086131

Gillespie, A. A. (2015). *Cybercrime: Key issues and debates*. Routledge. https://doi.org/10.4324/9781315884202

Graham, R. S., & Smith, S. K. (2019). *Cybercrime and digital deviance*. Routledge. https://doi.org/10.4324/9781351238090

Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge. https://doi.org/10.4324/9781315777870

Holt, T. J. (2016). *Crime online : correlates, causes, and context*. Durham: Carolina Academic Press. http://www.worldcat.org/oclc/953108852

Holt, T. J., & Bossler, A. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses.* London: Routledge, Taylor and Francis Group. https://digitalcommons.georgiasouthern.edu/crimjust-criminology-facbookshelf/32/

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25. https://doi.org/10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40. https://doi.org/10.1080/01639625.2013.822209

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: An introduction*. Routledge. https://doi.org/10.4324/9781315296975

Hope, T. (2013). What do crime statistics tell us? In *Criminology* (3 ed.). Oxford University Press. https://doi.org/10.1093/he/9780199691296.003.0003

Hunt, L. W. (2021). Hobbesian causation and personal identity in the history of criminology. *Intellectual History Review, 31*(2), 247-266. https://doi.org/10.1080/17496977.2020.1738761

Husár, M., Jaššo, M., & Dillinger, T. (2020). Centrope as a laboratory of cross-border cooperation–lessons from 17 years of the Centrope region (2003-2019). *socialspacejournal.eu, 20*(2), 163-183. http://socialspacejournal.eu/Social%20Space%20Journal%2022020(20).pdf#page=163

Jahankhani, H. (2018). *Cyber criminology*. Springer. https://doi.org/10.1007/978-3-319-97181-0

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International journal of cyber criminology, 1*(1), 1-6. http://cybercrimejournal.sascv.org/editorial.htm

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283-301). Pearson. https://www.researchgate.net/publication/321716315

Jaishankar, K. (2010). The Future of Cyber Criminology: Challenges and Opportunities1. *International Journal of Cyber Criminology, 4*(1&2), 26-31. https://cybercrimejournal.sascv.org/editorialijccjandec2010.htm

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior.* Taylor & Francis. https://books.google.com.pk/books?id=cWOQWx4QPFYC

Jaishankar, K. (2018a). Cyber criminology as an academic discipline: History, contribution and impact. *International Journal of Cyber Criminology, 12*(1), 1-8. https://doi.org/10.5281/zenodo.1467308

Jaishankar, K. (2018b). *Cyber Criminology: Evolution, Contribution and Impact.* UGC-MHRD Criminology Module. http://dx.doi.org/10.13140/RG.2.2.25117.00488

Jaishankar, K., & Ngo, F. T. (2017). Commemorating a decade in existence of the international journal of cyber criminology: a research agenda to advance the scholarship on cyber crime. *International Journal of Cyber Criminology, 11*(1), 1-9. https://doi.org/10.5281/zenodo.495762

Jennings, W. G., & Reingle, J. M. (2014). *Criminological and Criminal Justice Research Methods.* Wolters Kluwer Law & Business. https://books.google.com.pk/books?id=od0uDwAAQBAJ

Johnson, M. (2016). *Cyber crime, security and digital intelligence*. Routledge. https://doi.org/10.4324/9781315575667

Kanungo, E., & Chattoraj, P. (2020). Award of Compensation as a Mode of Victim Restoration: A Comparative Analysis of Laws in India, New Zealand and Germany. *International Journal of Criminal Justice Sciences, 15*(2), 325-342. http://dx.doi.org/10.5281/zenodo.4743317

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social science computer review, 30*(4), 470-486. https://doi.org/10.1177%2F0894439311422689

Kyvsgaard, B. (2012). Criminology Past and Present: Worries and Achievements. Speech at the 50 Years Jubilee Seminar of the Scandinavian Research Council for Criminology. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 13*(sup1), 4-11. https://doi.org/10.1080/14043858.2012.738630

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Loader, B. D., & Thomas, D. (2013). *Cybercrime: Security and Surveillance in the Information Age*. Taylor & Francis. https://books.google.com.pk/books?id=MtP1AhhZcfAC

Marcum, C. D. (2015). *Cyber Crime*. Wolters Kluwer. https://books.google.com.pk/books?id=mrvfDgAAQBAJ

Metcalfe, A., Soboroff, S., & Kelley, C. P. (2020). Social and Leadership Processes within the Kurdish Women's Freedom Movement. *Res Militaris, 10*(2), 1-19. https://resmilitaris.net/index.php/2020/06/01/id1032029/

Ndubueze, P. (2017a). Cyber Criminology: Contexts, Concerns and Directions. In P. N. Ndubueze (Ed.), *Cyber Criminology and Technology-Assisted Crime Control: A Reader* (pp. 1-28). Ahmadu Bello University Press. https://www.researchgate.net/publication/326658340

Ndubueze, P. (2017b). Policing cybercrime through a third party approach: An empirical evidence from Nigeria. *Unilag Sociological Review (USR), XIII*, 48-77. https://www.researchgate.net/publication/348661866

Ndubueze, P. N. (2016). Cyber criminology and the quest for social order in Nigerian Cyberspace. *The Nigerian Journal of Sociology and Anthropology, 14*(1), 32-48. http://www.nasajournal.com.ng/journal_articles/vol_14/issue_1/paper_3.pdf

Ndubueze, P. N. (2017). Cyber terrorism and national security in digital Nigeria. In P. Adejoh & W. Adisa (Eds.), *Terrorism & Counter Terrorism War in Nigeria. Essays in Honour of Lieutenant General Tukur Yusuf Buratai* (pp. 325-347). University of Lagos Press & Bookshop.

Ndubueze, P. N. (2020). Contemporary issues in criminology and criminal Justice. In P. N. Ndubueze, N. P. Oli, & B. N. Nwokeoma (Eds.), *Contemporary Issues in Criminology and Criminal Justice: A Fesyschrift in Honour of Professor E.U.M. Igbo at 70* (pp. 1-19). University of Nigeria Press.

Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology, 14*(1), 81-105. https://doi.org/10.5281/zenodo.3741131

Reid, S. T. (2017). *Crime and Criminology*. Wolters Kluwer. https://books.google.com.pk/books?id=8ptjEAAAQBAJ

Reyns, B. W., Henson, B., & Fisher, B. S. (2016). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice, 32*(2), 148-168. https://doi.org/10.1177%2F1043986215621378

Reyns, B. W., & Randa, R. (2017). Victim reporting behaviors following identity theft victimization: Results from the national crime victimization survey. *Crime & Delinquency, 63*(7), 814-838. https://doi.org/10.1177%2F0011128715620428

van de Weijer, S. G., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology, 16*(4), 486-508. https://doi.org/10.1177%2F1477370818773610

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 1-17). New York: Routledge. https://www.routledge.com/Crime-and-the-Internet/Wall/p/book/9780415244299

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society*. SAGE Publications. https://books.google.com.pk/books?id=gpuHDwAAQBAJ