Journal of Forensic Sciences And Criminal Investigation
ISSN: 2476-1311

Juniper Publishers key to the Researchers

Research article
Volume 20 Issue 2 - February 2026
DOI: 10.19080/JFSCI.2026.20.556035

J Forensic Sci & Criminal Inves


# The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes

**EFG Ajayi***

*Freetown University, Freetown, Seirra Leone*

**Submission:** November 06, 2025; **Published:** February 09, 2026

***Corresponding author:** EFG Ajayi, Freetown University 1- 4 Adeyemi Place Goldrich, Freetown, Seirra Leone, Email: ajayi.efg2000@gmail.com

**Abstract**

There is truism in the Latin expression nullum crimen sine lege, to the effect that, it is settled law, globally acknowledged and enacted at many jurisdictions, that no man shall be prosecuted nor punished except there is a codified law, regarding the alleged infraction. This is the real crux of the matter with cybercrime investigation and prosecution. The phenomenal rise in the meritorious use of the internet for electronic commercial transactions and social media engagements as a plus, amongst other uses across the globe, has in the negative also occasioned unprecedented data breaches, the combined effects of which has led to almost insurmountable hurdle in cybercrime investigation, prosecution and low rate of conviction which tasks, this paper shall address. Some of the militating impediments in the path of thorough investigation and diligent prosecution of cybercrimes includes but not limited to inadequate extant laws, obsolete laws which are grossly incapable of keeping phase with recent rapidly emerging technological developments and knowledge deficit. At the international level, inadequate alignment and lack of consensus amongst the different law enforcement agencies more often than not, stultifies investigation and prosecution. Other obstacles are the anonymous nature of the internet and obscurity associated with identity of users, unfettered encryption use, the challenges of digital evidence, the unruly legal horse of jurisdiction leading to disparities and lack of consensus regarding international cooperation in frontally tackling of cybercrimes, the lack of uniform standardization, the twin issues of privacy and data protection, the absence of public-private collaboration, the glaring different levels of technological advancement between developed and developing countries, the lack of adequate training for personnel saddled with investigation and prosecution of cybercrimes, and the dearth of indispensable resources to address cybercrimes. The principal purpose of this paper is to bring to the fore, the obstacles militating against thorough cybercrime investigation and diligent prosecution, with the view to making recommendations that shall make the appropriate authorities across the globe, to address precisely the issues, so as to minimize the consequences of cybercrimes, all over the world.

**Keywords:** Internet technology; cybercrime; Investigation; prosecution; conviction

## Introduction

As the name implies, cyber1-crimes are offences which are committed in the cyberspace and which more often times than not, are invisible to the naked eyes, by so doing, they are diametrically opposed to terrestrial crimes, which are orchestrated and perpetrated on land or other physical bodies like ships and airplanes, and which are almost all of the time, are visible to the eyes [1].

Nowadays, the unprecedent rise in the use of the internet via the instrumentality of the employment of telecommunication tools, has invariably occasioned a paradigm shift in the way business transactions are carried out, not only that but also, how social relationships are sealed via the numerous social media outfits, unfortunately, cyber criminals have capitalized on the availability of the internet to perpetrate several online crimes, which includes but not limited to fraud, theft, and even terrorism [2], an unfortunate development has caused the entire human race humongous financial losses, reputational damages etc. These days, cybercrimes are like household names; they are ubiquitous principally because the modern man is dependent on telecommunication gadgets like smart phones, tablets, laptops and desktops for the purpose of work and communication, this

development makes cybercrimes to be everywhere and embedded in every facet of human life; generally speaking, cybercrimes are commonly called "hacking [3]."

Although cybercrimes may be classified as relatively new, the phenomenon due to havoc wreaked on corporate and individuals has made it to attract and occupy the cynosure of global attention because, no one is immune to cybercrimes; put in another way, all living persons, no matter the standing in the society are vulnerable to cybercrime attacks. For the fact that humanity is in the information age [4], makes cybercrimes vulnerability, almost unavoidable, because in today's world, human life is simply unimaginable without the internet and telecommunications.

This paper adds that the internet advent, elsewhere referred to as the global information super highway, has given impetus to cybercrimes as nearly all of human daily activities, such as, production of goods and services, banking, finance, sales, as well as, purchases of goods, besides countless other transactions are today effected online, and which situation has provided unfettered opportunity and conducive clime, for cybercriminals to perpetrate online crimes, that is to say, the employment of the internet is a launchpad for the committal of serial and unending cybercriminal acts [5].

Computer crime and cybercrime are often used interchangeably, connoting the impression that the two concepts are the same thing, when as a matter of fact, they are only similar but mean different things. The distinction of the two concepts is hereunder provided for the purpose of clarity of expression, and avoidance of doubt. Computer crimes as the name implies, means the criminal acts perpetrated with the use of a computer system or a computer; stated in another way, these are crimes, such as, crimes against the computer hardware and the materials contained in a computer, or those associated in one way or another with the computer, which basically are the software and the data contained in the computer. Relevant examples of computer crimes are fraudulent acts, embezzlement, hacking into a computer, financial scams, etc.

On the other hand, cybercrime is a generic term used for the description of two distinct but closely related criminal acts, namely:

(a) Cyber-dependent and

(b) Cyber-enabled crimes.

Cyber-dependent crimes alternatively known as "pure" cybercrimes mean those offences that could only be perpetrated with the use of computer networks, a computer, or other forms of information and communication technology (ICT). These unlawful acts include but not limited to spreading of viruses, distributed denial of service (DDoS) attacks, hacking, ransomware attacks, malware creation and distribution, as well as, website defacement. Cyber-dependent crimes are thus acts directed against computers, or network resources, these does not rule out secondary outcomes from the cyberattacks. Cyber dependent crimes, as the name implies are invariably dependent on use of technology, ipso facto, they are incapable of existence, without technology [6].

Cyber-enabled criminal offences are the long-established crimes which are well known before the advent of the internet, but the perpetration of these crimes have increased in their severity, reach or intensity through the use of computers, computer networks, or other forms of ICT modes; these includes but not necessarily limited to cyberstalking, identity theft, intellectual property theft, online bullying, online scams, online shoplifting, phishing attacks, sale of counterfeit goods online and online banking and e-commerce frauds, as well as, sexual offences against minors.

On the basis of sovereignty accorded the nation-member states of the world and, of course, jurisdictional liberties, each country enacts its own laws and policies on cybercrimes. In view of this invariable fact, to date, there is no consensus with regards to one acceptable global definition of cybercrimes to adequately encapsulate all the ingredients of this novel variant of crime under discussion. Be that as it may, one outstanding fact beyond debate is that there is a commonality in all the definitional attempts, and that is that reference is made to the Internet. Bearing in mind the foregoing, cybercrime is defined as a crime committed over the Internet, which might include copyright infringement, defamation, fraud, and hacking [7].

Cybercrime also denotes any criminal or other offense facilitated by or involving the use of electronic communications or information systems, including any device, the Internet, or any one or more of them [8]. In the preceding paragraphs above, a definitional attempt for cybercrimes was made to the effect that cybercrimes are those criminal acts perpetrated in cyberspace. A distinction has also been drawn between cybercrimes and computer crimes. At this juncture, the brutal fact must be told to the effect that, cybercrimes are here to stay, that cybercrimes are a noisome pestilence and technological epidemic that the world must learn to live with, and for which managerial skills must be sought as urgently as possible. It is very unfortunate that as solutions are being found to the menacing issue of cybercrimes, so are cybercriminals devising newer and more sophisticated means of carrying out their attacks. By this development, global trade and commerce continue to suffer very huge costs, and the global citizens, directly and otherwise, continue to groan in severe and incurable pains, inflicted by cybercrimes [9].

## Cost of Cybercrimes

At this juncture, it is pertinent to showcase the cost of cybercrimes in order to appreciate the brutal fact that, cybercrimes cost is indeed humongous in terms of financial consequences. Aside from direct financial setbacks occasioned by cybercrimes on businesses across the globe, other unsavoury effects of cybercrimes are reputational damages arising from customer


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

trust erosion, supply chains disruption, intellectual property loss, employment disruptions and job losses, cost of mitigation and repairs to damages of work tools and equipment, insurance premiums, legal fees, fines and penalties levied by authorities worldwide as a result of data breaches.

It has been documented that there are ten ways cybercrime impacts businesses, to wit, direct financial costs, while attacks are getting quicker, the effects are far wider, data theft and privacy breaches, reputational damage, increased security costs, supply chain vulnerabilities, cloud security challenges, regulatory and legal consequences, operational changes and broader business culture shifts [10]. It is in the literature that, from Fortune 500 companies to the small scale enterprises, from agelong manufacturers to cutting-edge technology firms, no business is immune to cybercrime threats, and that, the average cost of a data breach reached USD 4.88 million in 2024, that is, a 20% increase since 2020. According to Cybersecurity Ventures, cybercrime was estimated to cost the entire globe a whopping sum of USD 9.5 trillion in 2024, and further that, if cybercrime were to be measured as a country, same would be the world's third largest economy, after the U.S. and China respectively. This revelation without any iota of doubt shows how mammoth the cybercrimes industry stands. It is expected that global cybercrime damage costs to grow by 15% per year over and reach USD 10.5 trillion by this year, 2025 [11].

The unprecedented rise in the use mobile gadgets, Internet of Things (IoT), cloud and remote tools has invariably and permanently led to transformation of how businesses and consumers make use of telecommunication technology and while development has enabled innovation and closer interactions between business partners worldwide on one hand, incidentally, it has on the other hand occasioned dramatic increase in digital attack surface [12]. In a research conducted by over 2,700 risk management professionals from 94 countries and territories, analyzed and published in the 2023 version of the Allianz Risk Barometer [13], revealed that close to half, 45% of experts submitted that cyber incidents remains the most dreaded cause of interruption to businesses, far more than natural disasters, or energy outages [14].

A breakdown of global cybercrime damage predicted by Cybersecurity Ventures in 2024 are USD 9.5 trillion a year, USD 793 billion a month, USD 182.5 billion a week, USD 26 billion a day, USD 1 billion an hour, USD 18 million a minute and USD 302,000 in one second.

## World Cybercrime Index (WCI)

The veil of anonymity surrounding the internet has been pierced to a large extent, after three years of intensive study by international team of researchers, they came up with 'World Cybercrime Index' (WCI), the first of its kind, which exhibits the global key cybercrimes hotspots, and further ranked the cybercriminals act in percentage terms, according to their professionalism and or dexterity in the perpetration of cybercrimes, across the globe. The WCI, shows that only twenty countries host the greatest cybercriminal threat. The list is as follows. Russia 58.39%, Ukraine 36.44%, China 27.86%, USA 25.01%, Nigeria 21.28%, Romania 14.83%, North Korea 10.61%, UK 9.01%, Brazil 8.93%, India 6.13%, Iran 4.78%, Belarus 3.87%, Ghana 3.58%, South Africa 2.58%, Moldova 2.57%, Israel 2.51%, Poland, 2.22%, Germany 2.17%, Netherland 1.92% and Latvia 1.68% [15]. The pioneer researchers of WCI from Oxford University and University of New South Wales Canberra Australia respectively, drummed on the advantage that the WCI would obviate the necessity of focusing time and expending resources on cybercrime countermeasures where the threat of cyber threat are not prevalent beside piercing the veil of anonymity, which had long been associated with the internet and generally help in the crusade against the ever- growing menace of profit-motive, behind cybercrime [16].

## Some countries budgets and financial losses to cybercrimes

That cybercrimes are here with humanity, is not a subject that would naturally generate any controversy, be that as it may, many countries are making efforts to combat this technological disaster, unfortunately the lack of cooperation and concerted efforts by the international community, has thwarted many of the state's efforts and resources. In this section, we discuss briefly how some countries are striving and expending their scarce resources to frontally address cybercrimes, and how the frequency and sophistication of cybercrimes are assuming astronomical proportions.

The United States Federal Trade Commission reported that consumers lost USD 5.9 billion to online fraud in the year 2021 and received 2.8 million reports on the same issue, from consumers. The fraud rate in 2021 rose by over 70%, compared with the previous year. With regards to the magnitude of financial losses incurred by the countries listed, hereunder is the outcome of research. South Korea whereat the cost of cybercrime is USD 72 billion, tops of the list of countries most affected by cybercrime in terms of monetary loss, per the research of Microsoft Korea.

The study indicated that the use of cloud technology and mobile computing makes the country more vulnerable, thereby creating more opportunities for cybercriminals and thus increasing cybersecurity threats in South Korea, as undisputed global leader in electronics and technical advancements. The next in the list of countries that lost money is United States, where the cost of cybercrime is USD 4.1bn. According to the FBI's Internet Crime Report submitted that the US economy lost USD 4.1 billion in 2020 and 791,790 businesses, were affected by online fraud. Germany is the third whereat the amounted expended on cybercrime cost is USD 2,610,520,217, 53% of the sum was spent


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

on security while the remainder, was committed to hardware and software.

Other countries that lost money in USD to cybercrimes are respectively Italy 1,210,000, Canada 685,309,840, Sweden 514,804,728, New Zealand, Australia 456,124,153, Colombia 303,000,000 and Japan 235,833,545. [17]. As propounded elsewhere before now, to the effect that cybercrimes are now part and parcel of humanity, the chances of total elimination of cyber-attacks from man's daily life, appears a chimerical hope, all that can be done is to fashion out well thought out modalities, to minimize the scourge of cybercrimes and one veritable panacea is cyber insurance, for a comprehensive exposition in that regard, please see "The need for the employment of cyber insurance, by global corporate bodies in mitigating the unavoidable risk of cyberattacks [18]."

## Militating factors to investigation and prosecution of cybercrimes

It is a settled matter far beyond debate at law, that thorough investigation, diligent prosecution and tendering incontrovertible evidence are not negotiable in securing the conviction of criminals, unfortunately, because of the intricate nature of cybercrimes, the investigation and prosecution are not as easy [19], as with terrestrial crimes. The impediments which truncate the investigation and prosecution of cybercrimes are hereunder discussed, with the view to making the said obstacles clearly understood.

## The anonymous nature of the Internet and identity hiding by cyber criminals

A discerning mind would wonder why the internet is anonymous and why that development has led to the scourge of cybercrimes being so prevalent nowadays, thereby almost rendering useless, almost all the obvious advantages of the internet and telecommunications. The truth is that, the global information superhighway, that is, the internet, was not intended and designed as anonymous technological instrument, in other words, it is the cybercriminals who exploited the internet's opportunity, for their nefarious activities.

It has been submitted that the core infrastructure of the internet was built for communication as well as data transfer, and not for user identities hiding, in addition, it is on record that today, the world is digitally interconnected, a development which has given a rise to unprecedented online anonymity. Human lives have moved online, from mere shopping, socializing, commercial and financial transactions, as well as, entertainment, concerns about online privacy, data security etc., have escalated.

The germane question being asked remains that, is true anonymity online possible? According to the Pew Research Center, 86% of internet users [20],

have taken several actions to hide their footprints online, via the use of encryption, employment of VPNs or clearing of cookies. It should be reiterated again that the internet, was not designed originally with the intendment of privacy. It is in literature that websites, apps, and many service providers usually collect massive amount of information in the form of data about users, which data are used for advertisement and user experiences, among other purposes [21].

At this point, it is necessary to exhibit the positive side of online anonymity which goes a long way to shielding individuals from online harassment, stalking, and cyberbullying, particularly women and other vulnerable groups who are disproportionately targeted. Anonymity encourages whistleblowers in the reporting of wrongdoing, embezzlement, corruption, and other unlawful activities, without the fear of reprisals or punishment from powerful people, who might be involved in criminal deeds. Online anonymity provides unfettered safety haven for marginalized groups like LGBTQ+ persons, opposition parties with unpopular political differences, and those others facing discrimination, harassment and intimidation, in expressing their divergent views. Online anonymity encourages freedom of expression and speech which are open and frank discussions regarding the expression of controversial or not too popular views, without fear of punishment or reprisal, thus leading to a more diverse, robust and across the board online views. Besides all the foregoing, it fosters dissent views especially under authoritarian and oppressive regimes [22], online anonymity is very fundamental for the citizenry to organize appropriately and voice dissent, against repressive governments and or other powerful entities.

In terms of creative expression, online anonymity undoubtedly empowers writers, artists, and literary and artistic brilliant minds to showcase and share their talents, without fear of unnecessary criticism and or rejection. With respect to data privacy as well as information security, online anonymity not only protect personal information but prevents the unlawful collection, storage and misuse of personal data by unauthorized persons, groups, governments, corporations, and others with malicious intents. It should be added that online anonymity prevents identity theft, that is, the concealment of the true identity of a user online, there is likelihood of reduction in the risk of identity theft, including other online fraudulent practices. Concerning how the internet users can work online and remain anonymous, a comprehensive list of telecommunications tools which includes but not necessarily limited to Advert blockers, DuckDuckGo, Fake emails, File shredder, Incognito mode, Proxy servers, Secure messaging apps, TOR Browser, Virtual machine and VPNs [23], etc. all of which this paper believes were ostensibly designed and manufactured for good use, but which unfortunately have been turned into fraudulent usage by cyber criminals, to perpetrate online crimes.

Cybercriminals are more often than not, almost impossible to track down as result of many factors which includes but not limited to the use of powerful and high-tech telecommunications gadgets, jurisdictional challenges, and the inherent difficulty of evidence gathering and the analysis of digital evidence. Generally,


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

cyber space criminals employ anonymity instruments as exhibited above. It has been posited that cybercriminals use anonymity networks in encrypting online traffic and hide IP address, which is a unique identifier assigned to a computer (or another Internet-connected digital device) by the ISP, when it connects to the Internet [24].

From precedents laid down at many jurisdictions across the globe, it is manifestly clear that online anonymity has been given judicial stamp, on grounds of privacy and the protection of fundamental human rights. In R. v. Spencer [25], a landmark case, the brief facts of which rests on possession of online child phonograph by the Appellant, the Supreme Court of Canada unanimously held without hesitation that, the internet users were entitled to a reasonable expectation of privacy in subscriber information held by ISP and ruled that the request for internet subscribers' information constitute an infringement on the Charter's guarantee, against unreasonable search and seizure.

In the matter of CDE & FGH v Mirror Group Newspapers and LMN [26], a privacy law English case, involving the misuse of private information and which warranted a claim whereof two claimants petitioned the court for interim injunction, restraining two defendants from making public, to wit, publish private information about the said claimants. An unusual case where the court, not only asserted the anonymity doctrine, but granted same to all the parties and non-parties in the case, as well. From all the foregoing, the point being emphasized is that, globally it is an herculean task to carry out thorough investigation by police and other agencies saddled with that responsibility aimed at tracing and tracking down cybercriminals, in other words, if investigation cannot be successfully carried out, of course, prosecution becomes an insurmountable impossibility, kits, and hacking services with minimal effort, lowering the barriers to entry and enabling even less technically skilled individuals to launch complex attacks.

See generally, Cybercrime When cybercriminals go global, our response must be international. unfortunately, under this scenario, cyber criminals continue to smile their ways to the banks while individuals, organizations and corporates continue to suffer financial setbacks, and associated pains and pangs of cybercrimes. This paper adds that the campaign at various quarters to jettison anonymity while online and mandatory introduction of identification as a perquisite, has been ferociously opposed by human rights activists on the ground of violation of privacy rights [27], with that development, cybercriminals appear to have been offered latitude to continue to operate unhindered, and by so doing, the challenge of anonymity continues to render cybercrimes investigation and prosecution, a de facto impossibility [28].

## Challenges of Digital Evidence

Whilst it is relatively easier to obtain incontrovertible evidence for terrestrial crimes investigations and prosecution, and which said evidence are more often than not, physical and could be obtained at the locus of the crime, digital evidence is much more difficult and could only be obtained online by traces left and which could only be deciphered by experts, besides their volatility. According to Interpol, digital evidence can be volatile, criminals often operate behind layers of anonymity-enhancing technologies, and investigations become entangled in a web of differing legal systems, and political sensitivities.

Digital evidence is indispensable for cybercrime prosecution; however, the very nature of the said digital evidence, presents special challenges. The unique characteristics of digital evidence as far as investigation, prosecution and admissibility before the courts could be summarily described as cross-jurisdictional, dynamic, easily altered, easily duplicated, fragile, voluminous, intangible, latent, that is, could be hidden by way of encryption, have high potential for authenticity purposes, used in supporting criminal investigation, civil suits, regulatory compliance, corporate security and above all, digital evidence is indeed very volatile.

### Voluminous amount of data

The role of digital forensics cannot be over emphasized in nowadays cybercriminal investigations, because they furnish important insights pertaining the criminal activities, nay, they are instrumental to securing the convictions of cybercriminals in courts [29]. But it should be borne in mind that, the fast paced changing nature of digital technology comes with numerous challenges, as well as, gaps in legal frameworks and the arena of digital forensics, in processing of digital evidence [30]. It has been posited that one of the primary challenges in digital forensics, is the huge volume of data, that those charged with investigation must analyze [31]. And further that the amount of data emanating from platforms and modern devices which includes but not limited to social media, smartphones and cloud services, are indeed overwhelming [32]. All the foregoing, result in invariable long delays regarding the analysis of digital evidence, this development impact investigations and more often times than not, result in the loss of crucial and valuable digital evidence [33].

### The use of many devices at different platforms

One other important challenge which serves a stumbling block towards investigations, is the multiplicity of devices and platforms employed, in digital evidence generation. It is important to bear in mind carefully that, these platforms and devices use different storage methods, file formats, and of course, different security protocols. All the afore mentioned differences go a long way to causing insurmountable difficulties for investigators in extracting and analyzing digital evidence, in one standardized format [34].

### Encryption and other security measures

Aside all the challenges enumerated before now, is the ever-increasing use of diverse security measures and encryption tools with the view of protecting digital data [35], this is a legitimate right to which everyone is entitled but cybercriminals have capitalized on same to wreak havoc in the cyberspace. Encryption


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

depending on the power of the tool employed, makes it difficult or total impossibility for cybercrime investigators to access, as well as, analyze digital evidence, most especially if the key or code to the encryption is unavailable [36]. This development it is submitted, has raised queries regarding striking a balance between the investigative needs of cybercrime investigation agencies and inalienable individual rights of privacy, to which all persons are entitled [37].

### Absence of standardization of digital forensics practices and procedures.

The absence of standardisation in the handling of digital forensics practices, as well as, the procedures followed, continue as a mammoth challenge militating against cybercrime investigations across the globe. Apparently, different investigating agencies and digital forensic laboratories employ different techniques, tools and methodologies, a situation which usually produce results which are inconsistent, including human errors in the digital evidence analysis [38]. The cross jurisdictional nature of cybercrime and the peculiar character of digital evidence prompts insurmountable challenges, regarding international cooperation and more often than not, continue to an raise jurisdictional issues, which are very complex indeed. Cybercrimes have no respect for borders, ipso facto, digital evidence are capable of being stored in many jurisdictions [39]. This incontrovertible assertion certainly calls for international cooperation and pragmatic management in order to with certitude, assure that digital evidence is collected, strategically stored and analyzed not only legally, but ethically [40].

### No global uniform rules, for admissibility of digital evidence.

It has been opined that the legal frameworks designed for handling the sensitive issue of digital evidence are just evolving, however, there are seemingly apparent challenges and gaps yet to be surmounted. One outstanding challenge, is the absence of consistent and clear rules for admissibility of digital evidence [41]. It is beyond controversy that evidence rules with respect to cybercrimes were enacted during the analog era, of course the said evidence rules cannot cope with this computer and information age, given the intricacies of digital evidence [42]. Another indisputable challenge remains the need to balance investigative needs of cybercrime investigators, with the privacy rights of citizens [43].

It is well etched in literature, to the effect that the United States Fourth Amendment to the constitution offer protection to citizens from unreasonable searches and seizures, however the courts seized of cybercrime cases, continue to struggle with the application of the privacy right with reference to application to digital evidence [44]. Generally, the coming up of regulations protecting individual data, for example, the European Union General Data Protection Regulation (GDPR), has certainly created obstacles for cybercriminal investigators, who are desirous of accessing and analyzing of digital evidence [45].

### The volatility of digital evidence and issue of preservation

Data preservation is another crucial challenge in the arena of digital forensics, this is not unconnected with the fact that digital evidence is usually volatile and capable of easy modification, alteration and can be deleted, or completely destroyed, willfully or otherwise. In the preservation of digital evidence, the investigators have no choice but employ and use technical means and specialized tools, in making bit-by-bit copies of storage devices or the platforms. This procedure has been described as time-consuming and cumbersome, besides the fact that, evidence may be lost or partially or completely destroyed, before preservation [46].

### Dearth of competent investigative personnel

Human capital is not negotiable in every facet of human life, same is applicable to the crucial issue of digital forensic, a field where there is dearth of experienced and savvy personnel who will not only collect incontrovertible evidence that would nail cybercriminals, but carry out thorough analysis, nay, adequately preserve the collected evidence with the view to tendering them before the courts. Put in other words, the dearth of qualified digital forensic investigators, analysts and examiners presents a humongous challenge to the tracking and conviction of cyberspace criminals. It is in literature that digital forensics, is a highly technical, specialized field, which requires the possession of investigative expertise, technical skills, as well as, a robust legal expertise. Thus, the inadequacy of qualified and experienced digital forensic analysts, ditto the examiners, often leads to avoidable delays during investigations, and which said development, usually compromise the integrity and admissibility of digital evidence, before the courts [47]. This paper adds that, there is poor training and development of investigators, aside the poor terms and conditions in the sense of remuneration, as well as, inadequate security and protection for said investigators, who execute the hazardous job of tracking the cybercriminals.

### Inadequate number of prosecution personnel

It is not a subject for debate that, there are no uniform rules for admissibility of digital evidence, besides that, is the voluminous amount of data to be analyzed, there is the challenge of volatility of digital evidence and issue of preservation, and in addition, is the encryption and other security measures used in the protection of data. All the foregoing factors makes presentation of digital data by lawyers, a very herculean task. In other words, lawyers who are prosecutors must have very sound technical know-how, before diligent prosecution could happen.

The prosecutors of cybercrimes who are savvy, are not many because of the highly specialized technical nature of digital


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

evidence. It is a settled fact that, even if the law enforcement agencies had done a good job in the investigation of cybercrime, at the litigation stage, expertise of prosecution attorneys is still very crucial to secure the conviction of cybercriminals, as it is incumbent on prosecution to proof his case beyond doubts; unfortunately, this is not the case as there is dearth of savvy prosecutors in government justice departments, however, cybercriminals have unfettered access to renown private attorneys who charge very high legal fees, and which is not a problem to the cybercriminals as they could readily afford to pay high professional fees to the best lawyers, who specializes in cybercrime practice; further, anonymity issue of cybercriminals and the nature of evidence which more often than not tenuous, regarding the fact that investigators can only rely on traces and tracks left on computers and the Internet, all the afore stated goes to compounding the case of prosecutors who are not as grounded in handling of cybercrime litigation, compared with their counterparts in private practice; these identified gaps unfortunately are a plus for cybercriminals, who in addition to technicalities in cybercrime cases, have more than enough funds to hire first class attorneys [48]. Thus highly specialized training for legal personnel is not negotiable, so as to enable them handle in a professional manner, the handling of the technical aspects of cybercrime prosecutions.

### Necessity for heavy investment in research and development

This paper holds the view that digital forensics is a capital-intensive venture and holds the key to tracking down cybercriminals, unfortunately many governments across the world demonstrate a lack-lustre or outright apathy towards research and development in this critical field, thus adding to the list of challenges militating against investigation and prosecution of cybercriminals. However, there is no doubt that there is need for heavy investment in research and development in the area of digital forensics. For the fact that digital technology is evolving with neck brake rapidity, it is not negotiable that investigators must constantly be trained and developed so as to be at home with new techniques and in order to be savvy in their analysis of digital evidence, put in another way, there is a need for heavy investment in research and development so as to enable investigators, examiners and analysts to be ahead of cyber thieves given the new threats and associated challenges [49].

At this juncture, it is necessary to state that cybercrime and gathering of digital evidence have raised crucial ethical issue and societal questions regarding the balance between individual privacy and security of information, that is to say, the power accorded the law enforcement agencies in their course of investigation on one hand, and the inalienable rights of citizens on the other. It has been opined to the effect that these questions, are interwoven and not easily answered, all said, there is need for continuous engagement and dialogue with all stakeholders across the globe [50].

## The challenge posed by the radical issue of jurisdiction

Aside from insurmountable issue of anonymity discussed before now, one other potent challenge to cybercrime investigation and prosecution, is jurisdiction. When cognizance is taken into account of the time-tested principles of state independence, sovereignty and territorial integrity, each nation-state of the world, have the authority to investigate, prosecute and make laws binding on things and all persons within its geographical entity, called a country [51].

Jurisdiction may be defined as the power of a court or judge to entertain an action, petition or proceedings. See *Alade v Alemuloke* [52]. The issue of jurisdiction is so radical that if forms the basis of any adjudication, stated otherwise, it goes into the roots of any matter before the courts. If a court lacks jurisdiction, it also lacks necessary competence to try the case. A defect in competence is fatal, for the proceedings are null and void ab initio, however well conducted and well decided the case may be [53]. A defect in competence is extrinsic to adjudication. The court must first of all be competent, that is, possess jurisdiction before it can proceed on any adjudication. See Oloba v. Akereja. See also Madukolu & Ors. v. Mkemdilim [54,55].

Given how fundamental the issue of jurisdiction is at law, and bearing in mind its radical nature, it has been asserted to the effect that, there is no technical word in the whole of conflict of laws that is more variously used and abused than jurisdiction. It is a word with too many meanings and all that can be done about it is to ascertain the sense in which it is being used at any given time [56]. A distinction ought to be made between the use of the term jurisdiction in extra-territorial and intra-territorial situations. While intra-territorial competence of a court concerns the authority of a court to hear and determine an issue upon which its decision is sought, the significance of extra-territorial competence of a court comes into focus, when its judgment is sought to be enforced outside the forum.

At this juncture, it is necessary to earmark that jurisdiction has many facets; however, the concern of jurisdiction with respect to investigation and prosecution of cybercrimes basically revolves around two issues, namely, geographical jurisdiction and jurisdiction in personam [57]. Geographical jurisdiction addresses the fundamental issue as to if a court have the power beyond the territory where it is situate, while jurisdiction in personam deals with whether a court is empowered to hear and determine a case, regarding online matters not within its jurisdiction. See *Attaway v. Omega* [58], a case where the transaction regarding the sale of a car was concluded over the internet and whereat, the Indiana Court of Appeals in the USA assumed jurisdiction over a defendant who is out-of-state, the said defendant rescinded payment on the ground that the car was "significantly not as described" but however returned the car, at the buyer's expense.

Given the peculiar nature of cybercrime, it is in a class of its own, it is unique and distinct in character unlike traditional


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

terrestrial crimes, which are committed in a particular locus and whereof, the effect(s) are felt by the victim(s); stated in another way, cybercrimes transcend states and jurisdictions; they are cross border or transitional crimes. Thus, a cybercriminal may sit in the comfort of his home, office, café or wherever he chooses, with a desktop, laptop, tablet or phone connected to the Internet, and carry out his illegal activities that would be felt thousands of kilometers away, from where the act(s) took place [59].

The scenario depicted above, showcasing the pervasiveness of cybercrime has been aptly expressed as "the ubiquity of information in modern communication systems makes it irrelevant as to where perpetrators and victims of crimes are situated in terms of geography. There is no need for the perpetrator or the victim of a crime to move or to meet in person. Unlawful actions such as computer manipulations in one country can have direct, immediate effects in the computer systems of another country [60]."

To sum up jurisdictional challenge to enforcement of cybercrime laws, it means if the hurdle of anonymity is scaled and a cybercriminal is clearly identified but he is situate in another country aside from where the victim is domiciled, the court of the forum cannot effectively try such a criminal as the court lacks jurisdiction geographically, and also in rem [61].

With particular reference to hurdles faced in the investigation and prosecution of cybercrimes worldwide on account on jurisdiction, it has been etched in literature that:

1. Cyber-attackers evade penalty by manipulating cyber data via advanced technologies and adjust data, using advanced technologies which make it difficult to trace or track them down.

2. The investigation and of course prosecution becomes difficult on the grounds that national and international regulations, are weak or not well applied.

3. International cybercrime legislations are inadequate to penalize cybercriminals, not only that but also, they do not lend full support, to the investigation of cybercrimes.

4. On account of territorial integrity and sovereignty of nation-states, it is very challenging to prosecute a cybercriminal who is a citizen of another country. Security authorities may be aware of a cyber-attacker, but the government of the country in question, more often times than not, do not sanction or support prosecution.

5. By the geographical boundaries of a single country or state, the cyberspace is not constrained. Several European countries have severe "Data Privacy Rules" in place, which militates against the investigation of cybercrimes from proceeding [62].

In the attempt to mitigate the hash consequences of diverse jurisdictions on contracting parties, since the principle of territorial integrity of sovereign nations cannot adequately serve the purpose of justice, more importantly, because parties are scattered across the globe, the tools employed in carrying out the transactions are also diverse and domiciled at several places in the world, a number of methods have been adopted globally in litigation resolution by the law courts and which are

1. Minimum contacts test, which arose out of the decision in the case of *International Shoe Co. v. Washington [63],* where the court gave judgment that, a non-resident party can be sued by the plaintiff if they have certain minimum contacts with the state, as long as the litigation is maintained, without jeopardising traditional notions of guaranteeing substantive justice. To invoke the jurisdiction, the defendant's contact with the state must be established. Therefore, the dispute must be borne out of or must be connected to the defendant's forum-related activity, wherein exercise of jurisdiction must be justified.

2. Purposeful availment test, in *Cybersell Inc. v. Cybersell Inc.* The purposeful availment test was explained to the effect that, the non-resident defendant must first do something that invokes the forum's jurisdiction, as well as, the benefits and protections that comes with it. Also, the plaintiff's claim must be based on the defendant's forum-related activity, and finally, jurisdiction must be exercised, in a reasonable manner [64].

3. Sliding scale test: The decision in *Zippo Manufacturing Co. v. Zippo Dot Com. Inc.* gave birth to this test. The are three groups: The first being passive information, which provides viewers with information without allowing them to respond. Second, it is interactive, it enables the defendant to convey with the citizens of the receiving state, and the citizens of the receiving state can respond. Third, it is integral to the perpetrator's corporate; it is used by the defendant to make transactions with the citizens of the forum state and to transmit information from targeted consumers [65].

4. Effects test: In the case of *Calder v. Jones,*76 the Supreme Court founded jurisdiction on the idea that, because the defendant knew his action would harm the plaintiff, he must be believed to have anticipated being dragged into court, where the injury occurred. Because any conduct in cyberspace has consequences in multiple countries, effect cases are particularly important [66,67].

## Apathetic disposition towards the reporting of cybercrimes and data dearth.

One of the fundamental reasons why cybercrimes continue to assume astronomical proportions, is the apathetic disposition of victims towards the reporting of cybercrimes incidents**.** Due to lack of reporting cyber breaches, the cybercriminals continue to smile their ways to the banks, while victims suffer in silence bearing their financial losses and psychological trauma, with philosophical calmness and of course, cybercrimes escalate.

Quite a number of reasons have been adduced as to why victims deliberately chose not to report cyberattacks, and which


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

reasons includes but not limited to the fact that, many victims are not certain about where or who to report cybercrimes, many do not know a particular event in their personal or business life qualifies as a cybercrime, some victims outrightly hold unrepentant view that agencies saddled with cybercrimes, either lacks resources or expertise to successfully tackle cybercrimes, in particular for business outfits, they are usually very worried about negative publicity and reputational damages in the estimation of customers and competition, the emotional distress concomitant with cyber breaches, often makes it unbearable to report same, a large number of victims hold the view that reporting cybercrimes would lead to exposure of their confidential personal information and same may occasion or warrant further privacy breaches, or outright misuse of their private data.

Unfortunately, as plausible as the rationale in above the paragraph might be, reporting of cybercrime is the first and foremost step in the waging of determined war against the cybercrime menace, thus, the lack of reporting, constitutes a huge challenge in the investigation and prosecution of cybercrimes, simply because, what is reported, is what could only be investigated and prosecuted.

Per the USA FBI's Internet Crime Complaint Center (IC3) 2024. Internet Crime Report combines information from 859,532 complaints of suspected internet crimes and details reported losses exceeding USD 16 billion, a 33% increase in losses from 2023. The said 2024 report, added that the most complaints emanated from people over 60 years suffered the most losses at nearly USD 5 billion, and submitted the greatest number of complaints.

According to FBI Director, Kash Patel "reporting is one of the first and most important steps in fighting crime so law enforcement can use this information to combat a variety of frauds and scams," he said FBI is only as successful as the reports it receives; that's why it's imperative that the public immediately report suspected cyber-enabled criminal activity to the FBI [68]."

In another survey of Internet users ranging between ages of 20 and 70 years, it was found that, though there exists a very high level of poor and negative attitude to cybercrime victimization reporting, but the reality cannot exclusively be blamed on the police, other predictors, like public awareness level of cybercrime in general, and particularly relating cybercrime laws, reporting channels, implications for reporting or not reporting, and criminal justice operations, need to be factored for effective cybercrime policing in Nigeria [69].

The lack of adequate and effective reporting of cybercrimes incidences to the concerned authorities across the globe, in effect, has militated against bringing to global attention and appreciation of the extent of the cybercrimes menace; closely related to reluctance to disclosure of cybercrimes is the lack of cooperation on the part of the victims, other stake holders and witnesses with police or other agencies saddled with investigation and prosecution of cybercriminals, it is immaterial whether private, corporate or institutional entities are the victims.

Several reasons have been advanced for reluctance to report cybercrimes, and these includes but not limited to costs arising from follow up of cybercrimes, which more often than not, far outweigh the benefit derivable thereof, the damage to the reputation and goodwill of victims especially corporates which are going concerns, of course, the protracted investigation and prosecution which are generally considered as effort and time wasting exercises, more importantly, the difficulty of diligent investigation which is usually scuttled when a particular cybercrime investigation and prosecution traverses many jurisdictions, thereby bringing to the fore issues in approach to cybercrimes.

Lack of effective reporting of cybercrime events and dearth of data go pari passu, the rationale being that, it is when cybercrimes are reported that data about same can be collated, analysed and published. The dearth of reliable data and information generally about cybercrimes has created lack of awareness; the said development has shrouded the extent of the problem to which mankind is presently faced with. This paper is of the view that the awareness and appreciation of any problem in human endeavors, is the beginning of any problem solving; as things stands today, only a fragment of the elite are aware of the impact of cybercrimes on the society [70].

## Absence of standardised international protocols for cyber security.

As at the time of writing this paper, there is no one universal law or regulation governing the cyberspace activities, this obvious lacuna, poses a virulent challenge to the digital ecosystem and serves as a severe inhibition to cybercrimes investigation and prosecution. It has been submitted that the adoption of the United Nations Charter predates the cyberspace emergence, thus the creation of inherent challenges applying legal provisions, based on traditional notions of state sovereignty and physical control to a space largely dominated by private institutions, and transnational going concerns [71].

Stated in another way, the extant statutes enacted before now, cannot cope with the rapidly evolving paradigm shift occasioned in the field of technology, hence this paper assets that the law and its enforcement mechanisms, are behind emerging technologies, such as, 5G, advanced materials, AI, biotechnology, blockchain, cloud computing, edge computing, Internet of Things, quantum computing, robotics, virtual and augmented reality, etc. he challenges concomitant with lack of standardization of international protocols for cyber security as etched in different literatures, and same could be summed up to the effect that, critical infrastructure risk has increased, thereby making it easy targets


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

for cybercriminals to wreak havoc, a situation which ultimately disorganises essential services, which are indispensable to humanity, there is haphazard responses to cyber events, a development which leads sovereign nation-states ascribing different interpretations to what a cyberattack is, and of course avoidable jurisdictional disputes, there are various compliance requirements which cross-boarder going concerns have to abide with, including standards, this raises the bar of compliance costs, which corporates must cough out, further, information sharing regarding threat intelligence and joint response to cyber threats has become herculean, and there is little or no accountability because cross boarder cybercrimes more often than not escape punishment, as a result of the inherent difficulty of the establishment of the appropriate jurisdiction, and the application of well settled legal frameworks, across jurisdictions [72].

## The challenge of inadequate and or non-existent uniform extradition treaties

Extradition has been defined as the formal process, whereby a State requests from the requested State, the return of a person accused or convicted of a crime, to stand trial or serve a sentence in the requesting State. Further, the concept is said to have 8 principles, namely double (dual) criminality, the rule of specialty, the non-extradition of nationals, risk of persecution in the requesting State, the political offense exception, risk of unfair trial in the requesting State, double jeopardy (*ne bis in idem*) and the non-discrimination clause.

This paper asserts that once a cyberspace accused person is not within the jurisdiction where the effect of his offence is felt, the investigation and prosecution of such offence(s) automatically becomes a herculean challenge, because of territorial limitations accorded to all sovereign nation-states. It has been submitted that generally, most extradition agreements to date, are bilateral in nature, but increasingly multilateral agreements are signed and implemented either at the regional level or at the international level, the Organized Crime Convention represents a typical example, and that multilateral conventions have the advantage of providing common definitions for offences and procedures for States, which usually have different legal traditions and procedures [73]. Cybercrimes, being transnational crimes traversing over two or more states, usually face almost insurmountable hurdle of extraditing a suspect domiciled in another country, on the ground of sovereignty of nation-states, to which each country in the world, have absolute and total control in which it exercises geographical jurisdiction over persons, all moveable and immovables.

As at the time of putting this paper together, there is no one single international instrument governing or regulating extradition that is of enforceable character, against erring nation state. What we have in existence are bilateral, multilateral or regional extradition agreements, even at that, these instruments have no coercive attribute, *ipso facto*, nations of the world often act with impunity by flagrantly choosing which rule or law to obey, as far as extradition of suspected criminals is concerned. Besides the afore-stated hurdle against the investigation and prosecution of global cybercrimes, a good number of nation-states do not subscribe to the idea of their nationals being tried for offences committed outside their shores, such countries prefer to conduct the trial of their own citizens and in their own very jurisdiction. For example, the Extradition Law of the People's Republic of China (PRC Presidential Order No. 42 of 2000) [74], Article 3 states that "The People's Republic of China cooperates with foreign states in extradition on the basis of equality and reciprocity." But in same breath also, the said Article 3 declared that "No cooperation in extradition may impair the sovereignty, security or public interests of the People's Republic of China." As a matter of reality, China does not extradite her nationals.

Other countries with extradition clauses are Brazil, Austria, France, Japan, The Czech Republic, and Germany [75-80]. At this juncture, a discerning mind would wonder why some nation states would desire to preside or exercise jurisdiction over offences committed by their citizens elsewhere. This development certainly cast aspersion on the credibility of justice to be handed down by courts seized of such trials, and of course same constitute a very heavy hurdle to investigation and prosecution of cybercrimes, globally.

Of the eight principles of extradition, perhaps the most debatable one is, double (or dual) criminality, premised on the fact that the alleged offence for which extradition is sought, must constitute a criminal offence, in both the requesting and requested State [81]. It should be carefully borne in mind that, slight differences in the cybercrime laws of the concerned two or more countries, could militate against extradition of the suspect. Cybercrimes cases involving extradition are always complicated far more than imagined, for instance, the popular "Love Bug" virus case, the facts of which were that in May 2000, a computer virus named the "love bug," emerged and spread rapidly around the globe, it infected not less than 270,000 computers and forced the shutdown of computers at large corporations like USA Ford Motor, Dow Chemical, and the UK House of Lords. The computer security experts eventually traced the virus to the Philippines, the combined team of investigators from Philippines and the USA went into tracking down the person(s) who manufactured the said virus and escalated it. They were frustrated in their efforts by the Philippines' lack of computer crime laws. The "love bug" destroyed files and impeded e-mail traffic in more than twenty countries. It was estimated that the virus caused USD 10 billion in damages. The unfortunate episode prompted the Philippines, to enact a cybercrime law. The "love bug" of course, accentuates the dual criminality case [82].

Another vital extradition principle is "*aut dedere aut judicare*," [83], an international treaty expressed in Latin which means, state parties are under obligation to "either extradite or prosecute," the accused person domiciled in their territory. Put in another way,


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

nation-states across the globe are obliged to either extradite the accused person to the requesting state, or alternatively prosecute the said accused person, at their jurisdiction. This paper notes that the principal object of "*aut dedere aut judicare*," is to ensure that accused person(s) would not escape justice by taking refuge in another country, aside from where they committed the crime. It has been objectively asserted that, extradition, a process long rooted in principles of reciprocity and sovereignty, was not *ab initio* formulated for modern space offences like cybercrimes, which cross territorial bounds. Besides this, the absence of worldwide definitions of cyber offences, the divergent procedural safeguards, and of course, the inconsistent respect for human rights norms, have furthered the obstruction of cooperative enforcement [84]. See the illuminating case of how extradition could be truncated in the matter of *Lauri Love v. USA* [85] where the Court quashed the extradition of the Appellant to the US to face charges of hacking USA governmental bodies and intelligence agencies, as it would be "oppressive" for him to undergo trial in the USA, but not in the UK on the grounds of his multiple medical condition, to wit, suffering from Asperger Syndrome (AS), eczema and depression. From the decision of the foregoing case, it is manifestly clear that even if extradition is clearly justified, same could be nullified on account of jeopardy to the health and well being of the accused person(s).

## The need for individual privacy and data protection

In the current digital age, there is no controversy that law enforcement agencies need data for investigation and crime prevention, particularly with the view to identifying potential threats, conducting investigation for the crimes, as well as, the gathering of digital evidence with the view to diligent prosecution.

Besides the foregoing, for safety of members of the public, law enforcement agencies need access to data with the hope to preventing possible terrorist attacks on one hand, and providing adequate responses to emergencies on the other, thereby guaranteeing public safety. Be that as it may, mind bearing technological advancements, the law agencies are employing advanced technologies, such as, surveillance systems and AI, thereof having access to huge amounts of data. The fore going development has naturally raised data protection and privacy issues, because of gathered data by law agencies, runs misuse risk, and may erode public trust.

One insurmountable hurdle to cybercrime investigations and prosecution remains the unwavering respect for human liberty of privacy and data protection because, cybercrime investigation more often than not, involve getting access to and analysis of huge amounts of data, a development which raises privacy concerns. In other words, there is invariable need to strike a balance between law enforcement needs, as well as, the protection of human liberty, particularly, individual privacy, this development presents a key challenge in today's digital age, alternatively referred to as, the information age [86]. It has been forcefully argued that to strike a balance between compelling security need and individual privacy, is very crucial for creating and maintaining a safer internet, while at the same time, upholding the tenets of human rights [87].

This paper is unflagging in its conviction to the effect that, allowing law enforcement agencies to have unfettered and sweeping access to data and personal information is antithetical to the inalienable fundamental rights of citizens. To stem the tide of data intrusion, good screening tools have been suggested and which said tools, are designed to identify automatically only the pertinent information, thereby leading to reduction of extensive searches [88]. Simply put, modern and good screening tools helps in speeding up investigations, as well as, ensuring that personal data, actually remains private, by so doing, a balance would be struck between sound law enforcement, and the deserved respect for individual privacy.

To maintain a healthy equilibrium between individual liberty of privacy and data protection as well as, attend to the needs of law enforcement agencies in carrying out their onerous tasks for public safety in this cybercrime filled digital era, a number of suggestions has been put forward, to wit, that law enforcement agencies should be transparent and accountable regarding their act of data collection modalities, including the technologies employed. Aside from the above, it has in no uncertain terms been advocated, that there is need for the establishment of crystal-clear guidelines regarding the collection of data, storage, access, and retention by law enforcement agencies. It has also been canvassed that there should be collection of only necessary data, for specific investigations which would go a long way, to obviating broad scope data collection.

The last but not the least, is the call for independent oversight bodies to monitor and regulate law enforcement activities, particularly with respect to strict compliance with data protection rules and regulations [89]. All over the world, when the issue of privacy and data protection comes up for discuss, the European Union stands out as a trail blazer, via the instrumentality of the enacted General Data Protection Regulation (GDPR) [90].

## Rapid phase of technological advancement.

It is a well settled matter far beyond debate, that technology is always ahead of the law, this is because, a particular technology would first have to be invented and be in use or operation, before the law regulating same, is enacted. In other words, the rapid phase of technological advancement connotes that legal frameworks and the law enforcement mechanisms may not adequately address the quick phase of technology. Typical examples of emerging technologies are blockchain and artificial intelligence (AI), which are not effectively catered for, by extant laws.

It has been documented that the fast-phased technological innovation, the universal and ever- increasing accessibility of information communication technologies ICTs, in addition to high- speed Internet and mobile devices with Internet connectivity, have occasioned irreversible transformation of


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

societies, across the globe. There is no controversy that, advances in ICTs have the propensity of facilitating criminal communication and collaboration, when of course law enforcement agencies may apparently lack the knowhow and financial resources, and indispensable legal apparatus to investigate digital crime. Cultural variations and differences in the existing legal systems, could invariably further complicate effective prevention, investigation and prosecution of cybercrimes [91]. The advent of rapid technological breakthroughs has been described as a double-edged sword in the arena of cybercrime investigation, and prosecution. On one hand, new technologies make available high powered and precision tools for law enforcement agencies in carrying out their onerous duties, but the said new technologies, also present new opportunities and means for cybercriminals to carry out their nefarious activities, and obviate tracking [92].

In the light of the above unfortunate development, there is no other alternative than embark on relentless crafting of new legal frameworks, effective investigation modalities and high precision forensic tools, so as to frontally address global cybercrime, as the new laws and regulations strive to do battle with cybercrime and jurisdictional disparities in the face new technologies.One of the veritable setbacks for rapid phase of technological advancement as far as cybercrimes investigation and prosecution are concerned, is in area of internet user anonymity and power laden evasion tools [93], such as, proxy servers and VPNs which makes cybercriminals untraceable, it goes without saying of course that, if cybercriminals cannot be traced, the chances of investigation and prosecution become, a nullity.

At this juncture, having before now discussed the intricacies concomitant with digital evidence collection and storage, the absence standardised protocols or universal rule for digital evidence handling, truncates admissibility of the said evidence in court [94], this development of course produces wrong judgements which goes a long way, to eroding the trust and confidence of the litigants and the general public, in justice and the rule of law. Besides the foregoing, is the unassailable fact that cybercrime investigations are indeed capital intensive, and they are complex [95], in addition to high level manpower requirements, which are not readily available, most especially when complex cases traversing several jurisdictions comes up for hearing and determination. Above all, nowadays, high tech cyberattack techniques are employed, such as, AI used in automating attacks [96], which makes the attacks to strike targets with precision, not only that but also, makes detection of cybercriminals orchestrating the cyberattacks, harder to trace or track down.

## Lack of public-private sectors collaboration and global cooperation

The absence of effective partnership between private and public sectors, as well as, the lack- luster cooperative efforts at a worldwide level, has done incalculable damages to sound cybercrime investigation and prosecution. One of the insurmountable hurdles against thorough investigation and diligent prosecution of cybercrimes is the seamless and geographic spread of the internet, this development enables malicious actors, otherwise known as cybercriminals to operate from several jurisdictions, thereby constituting a challenge for law enforcement agencies, to trace and track them down [97]. The lack of cooperation between public and private sectors, technology outfits cybersecurity experts and companies, goes a long way to fueling the apprehension of malicious actors, and of course their investigation and prosecution.

Another fundamental factor militating against global investigation and prosecution of cybercrimes is the widespread employment of anonymity equipment [98], such as, Tor network, proxy servers and VPNs, these tools hide not only the identities of malicious cyberspace actors, but also their locations which of course makes the cybercriminals, untraceable across the globe. Of course, when identity and location of cybercriminals are unknown and there is absence of global collaboration and cooperation to frontally tackle the menace, at private- public intergovernmental level, cybercrimes would naturally continue to escalate beyond imaginable proportions. Cybercrimes being a global issue, demands that acquired information must be shared between affected the parties in order to join hands and frontally defend and attack the common enemy, unfortunately, one other critical issue which has aided the thriving of cyberattacks is lack of information sharing between private and public agencies.

It has been posited that the tripartite concepts of digitalization, smart technologies and globalisation have in no uncertain measure, skyrocketed the proclivity and gravity of cybercrime [99], notwithstanding this incontrovertible fact, information sharing is still at its lowest ebb, a development attributable to lack of trust between the parties, different perceptions regarding the nomenclature, extent and severity of the challenges, and reputational damages which cyber breaches may occasion, on the part of private entities, etc.

The thought-provoking question has been posed to the effect that "what happens if the threat data is not shared? The answer has been provided that knowledge gap widens when information is shared without government input and evaluation. Incidentally, with the multitude of threats emerging daily, public and private sector organisations cannot afford to defend them separately [100].

The barriers to achievement laden PPPs and other forms of multistakeholder collaboration has been identified as the lack of trust amongst partners, the rule of law which is weak, conflicting regulatory and legislative frameworks, inadequate resources which includes but not limited to technology, technical expertise, funding, legal and dearth of personnel, as well as, lack of alignment, coordination, and motivation amongst partners. Approaches deemed effective for public-private collaboration on cybercrime


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

has been suggested, to wit, building trust and supporting demand-and need-driven initiatives should be prioritized. The said methodology should incorporate human rights standards and safeguards, as well as, seek regional synergies. Partnerships premised on voluntary cooperation and adaptive models that reflect the dynamic nature of cybercrime is recommended. The approaches should incorporate flexible strategies which would enable ongoing assessment, and the updating of processes necessary, for continuous improvement.

Further, literature has it that establishing PPPs on cybercrime calls for due diligence which involves a systematic needs assessment, evaluation of existing initiatives, and review of legislative and regulatory frameworks. The suggestion Iay emphasise on upholding human rights standards and ensuring data protection, including privacy. Major steps include implementing capacity-building programmes, developing robust information-sharing mechanisms, and engaging in consultative policy development. Finally, all stakeholders embarking on a PPP are strongly advised to perform risk assessments being part of due diligence, so to ensure that the establishment of the PPP, is feasible.

The benefits attributable to cybersecurity information sharing has been catalogued to the effect that, cooperation and coordination in that regard, helps to strengthen cyberattack mitigation and response capabilities, it enhances collective knowledge and effective collaborations, encourages better understanding of threats and future risks, gives fillip for identification of incentives for likely future attacks, increases the propensity of detecting attacks, reduces cybersecurity investments, and analyse future investment strategies [101].

## Conclusions

In the light of all that has been submitted in sections 1 to 12 above, this paper with humility hereby concludes as follows that: In the introductory section of this writeup, attempt was made to explain the concept of cybercrime, ditto was the definitional challenge where no globally accepted definition is acknowledged, but a common theme runs through all the definitions to the effect that, cybercrimes are perpetrated via the internet. A clear distinction was also elaborated upon regarding the differences between cybercrimes and computer crimes. This paper submits unequivocally that cybercrimes are mere outgrows of technological advanced development in the communication sector. Put in other words, cybercrimes are unintended consequences of high-tech innovation because, the progenitors of the internet never contemplated the adverse employment of the internet, it is therefore unfortunate that cybercriminals capitalized on the vulnerability of the internet invention, for their egocentric purposes of making illicit profit, revenge, competitive advantage and other malicious acts.

Further, this literature holds unflaggingly the position that, cybercrimes are now part and parcel of human life, they are here to stay, just like the medical scientists and doctors advised the world regarding Covid-19, in other words, cybercrime, the noisome pestilence and technological epidemic is one adverse phenomenal ailment, which the world must learn to live with, via the instrumentality of devising appropriate strategies, to cope with the scourge. With regards to cybercrimes cost, this is very huge and amazing. The financial implications are the one most talked and researched about, other costs include but not restricted to reputational damages rooted in customer trust erosion, supply chains disruption, intellectual property loss, employment disruptions and job losses, mitigation cost and repairs to damages of work tools and equipment, insurance premiums, legal fees, fines and penalties levied by authorities worldwide, of course, there is massive psychological trauma on victims, all arising from data breaches. It is on record that no business is immune to cybercrime threats, further that, cost estimate for the scourge of cybercrimes is a staggering sum of USD 9.5 trillion for the year 2024, in addition, the startling revelation is that, if cybercrime were to be valued as a country, same would be the world's third largest economy, following USA. and China. Cyber incidents remain the most dreaded cause of interruption to businesses, superseding natural disasters, and energy outages.

A new research outcome has been added to the beneath the surface study of cybercrimes and named the World Cybercrime Index (WCI), a pioneer work, which pierced the veil of anonymity surrounding the use of the internet, and exhibits the global key cybercrimes hotspots, and further ranked the cybercriminals act in percentage terms, according to their professionalism and or dexterity in the perpetration of cybercrimes, across the globe. The WCI, shows that only twenty countries host the greatest cybercriminal threats with Russia on top with 58.39% and Latvia the last, at 1.68%. The most beneficial purpose of the WCI is that it would obviate making going concerns spend less efforts and expenses, where cyber threats are not prevalent, aside from removing the blanket of anonymity, synonymous with the internet.

No controversy is raised whenever cybercrimes are said to occasion financial losses, this is the gospel truth, thus in an attempt to mitigate cybercrimes losses, a good number of countries make provision for budgets, in preparation for any eventualities of cyberattacks, elsewhere in this paper, referred to as technological epidemic. Research earlier cited stated that South Korea loss to cybercrime is USD 72 Billion and tops the list of countries most affected by cybercrime, followed by United States with a loss of USD. bn and 791,790 businesses were affected by online fraud.

As highlighted before now that, cybercrimes have become part of human life, the best that could be done is to devise strategies that would go long ways to minimizing the adverse effects of cyberattacks and one of the ways, is via the instrumentality of


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

cyber insurance. At this juncture, it is necessary to dwell on the factors militating against thorough investigation and diligent prosecution of cybercrimes. One of the fundamental setbacks is the obscurity otherwise referred to as the anonymous nature of the Internet, with the concomitant identity hiding by cyber criminals and other people for good purposes, such as, forestalling online harassment, stalking, and cyberbullying, particularly women, and for whistleblowers in the reporting of wrongdoing, embezzlement, corruption, and other unlawful activities, without the fear of reprisals or punishment from powerful people, who might be involved in criminal deeds.

Online anonymity offers safety haven for marginalized groups, opposition parties, those facing persecution, discrimination, harassment and intimidation, in expressing their divergent views via the use of anonymizing advert blockers, fake emails, incognito mode, proxy servers, TOR Browser, virtual machine and VPNs. From all indications, online anonymity has been accorded judicial accent, a development premised on fundamental human rights with its variants of privacy and data protection doctrines. Be that as it may, it should be borne in mind that the judicial nod while assuring citizens of their fundamental human rights, has inadvertently created avenue for cybercrimes to continue thriving. Summarily put, the judicial endorsement of online anonymity creates a stumbling block on the part of investigation and prosecution of cybercriminals, ipso facto, conviction of cyber offenders, remains a chimerical hope.

This paper inter alia, adds in this concluding session that, the challenges posed by the very nature of digital evidence which constitute a serious impediment to thorough investigation and diligent prosecution of cybercrimes, because of the inherent difficulty of gathering them online, aside the associated volatility compared with terrestrial crimes, which are easily accessible and gathered, at the scene of the crime.

Besides anonymity, the difficulty of gathering and volatility, is another challenge of digital evidence becoming entangled in a web of differing legal systems and political sensitivities, given the cross jurisdictional nature of cybercrimes in addition to being dynamic, easily altered, easily duplicated, fragile, voluminous, intangible and capable of encryption. At this juncture, it is pertinent to add that one other challenge of digital evidence remains the voluminous amount of data that investigators must gather together, preserve and analyze critically to unravel cybercrimes.

Another stumbling block closely related to huge volume of data for analysis, is the employment of many devices which includes laptops, desktops, tablets and smart phones used at different platforms which are either personal, organizational or the almost countless number of social media platforms in digital evidence generation, nay, these platforms and devices use different storage methods, file formats, and of course different security protocols, thereby compounding the investigation and prosecution processes. It should be borne in mind that aside from anonymity tools, the proliferation of encryption devices and other unfettered security measures, designed to protect digital data, makes it impossible to access protected data, this has constituted immeasurable hurdle to cybercrime investigation and prosecution. The absence or lack of standardization of digital forensics practices and procedures, whereof different investigating agencies and digital forensic laboratories, situate in different countries employ different techniques, tools and methodologies, thereof producing inconsistent results besides unavoidable human errors, certainly poses a militating challenge to investigation and prosecution of cybercrimes.

The fact that there are no uniform rules for admissibility of digital evidence, continue to cause impediment to cybercrime investigation and prosecution, particularly for conviction of cyber offenders. It is well settled that the extant evidential rules were enacted during the analogue era and cannot possibly address the current era of computer and information age, in other words, evidential rules for admissibility of digital evidence, are just evolving. Existing sound literature on computer and information technology with certitude, posit that digital evidence is volatile and that the issue of preservation or storage, is intricate. These two attributes of digital evidence are onerous challenges to cybercrime investigation and prosecution. Competent personnel are indispensable in all facets of life, for they are the coordinators that harnesses all factors of production to achieve organizational goals. The dearth of competent and experienced investigative and prosecution personnel in the arena of cybercrimes, thwarts the conviction of cyber actors. Digital forensic is a very high technical human endeavor which can only be handled by experts, unfortunately, the dearth of qualified digital forensic investigators, analysts and examiners, presents a humongous challenge to the tracking and conviction of cyberspace criminals. As if the foregoing were not enough, there is poor training and development of investigators, prosecutors and examiners, aside from the despicable terms and conditions regarding remuneration, ditto, inadequate security and protection for all the personnel, in this sensitive area of our digital life.

Given the fact that there are no uniform rules for admissibility of digital evidence, the voluminous amount of data to be analyzed, the challenge of volatility of digital evidence and issue of preservation, and in addition, is the encryption and other security measures used in the protection of data. All the foregoing factors makes presentation of digital data by lawyers, a very herculean task. In other words, lawyers who are prosecutors must have a sound technical know-how before diligent prosecution could happen. Unfortunately, there is dearth of competent prosecution personnel in government justice departments, but, cybercriminals with huge but illicit wealth, could hire the best of attorneys, whose fees are very high indeed.

It is not a debatable issue that, digital forensics is highly technical and very capital-intensive, added to these unassailable


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

facts, is that digital technology is evolving at a neck braking speed, however, cybercriminals could conveniently afford whatever latest tool or technology, in furtherance of their nefarious acts, it is sad to note that governments across the globe, exhibit a lackadaisical attitude, towards heavy investment in research and development pertaining ICT infrastructures. Undoubtedly, this situation has added another challenge militating against investigation and prosecution of cybercriminals. All said, there is the need for heavy investment in research and development in the area of digital forensics, so as to stem the tide of cybercrimes.

## Recommendations

It is widely acknowledged that cybercrimes is a pervasive technological scourge, having adverse effects on all people of the world, be it individual, business, corporate, organizations, agencies, governments and international bodies. Be that as it may, this paper holds the position that no matter how severe a challenge or problem is, there must be solution(s), it is in view of the foregoing believe, that the following far reaching recommendations are proffered, to minimize the adverse consequences of cybercrimes investigation and prosecution, across the globe. As elsewhere pointed out before now, that *nullum crimen sine lege,* meaning that no man shall be prosecuted nor punished except there is a codified law regarding the alleged infraction, however it is unfortunate to note many countries to date have no governing law or regulation regarding cybercrimes [102], also, some nation-states have laws which are either moribund and therefore not effective, perhaps because of their enactment during the analogue era. In the light of this legal lacuna, the first and foremost recommendation this paper projects, is that all sovereign nations should as a matter of urgency, update their legislations by adapting the laws to be in consonance with today's rapidly changing phase of cyber threats, and evolution of various gadgets and tools, which are making cybercrime investigation and prosecution, almost impossible. It is highly recommended that the model treaty, the Budapest Convention and the recently enacted United Nations Convention against Cybercrimes should be used.

The proposed enactments, must for the purpose of effectively addressing the stumbling blocks in the path of cybercrimes investigation and prosecution, make available legal powers for digital evidence collection, as well as frontally address emerging and advanced technological issues, such as, the misuse of AI, cloud hacking, and fraud pertaining to cryptocurrency. In addition, emerging technologies, such as, expansion of 5G, advanced robotics, cybersecurity AI, machine learning, augmented reality, blockchain, edge computing, extended reality, generative AI, internet of things, nano-technology, neuromorphic computing, quantum computing, synthetic media, virtual reality, voice-activated technology, etc., must be taken into cognizance in the proposed enactments, such that, the laws shall address the technologies as they are emerging, not that after their full emergency and operations, shall the law start catching up with the said emerging technologies, most importantly is the necessity to specifically focus on cybercrimes particularly challenges pertaining to jurisdiction, cybercrimes being cross-jurisdictional unlawful act. It is equally highly strongly recommended that, cybercrimes should be explicitly defined and other key concepts associated with it, because the concept to date, is not defined in most legislations bearing in mind that a clear-cut definition of a concept gives insights regarding the meaning and purpose of that concept.

While the foregoing recommendations are directed at sovereign nations to update their cybercrime legislations, this paper hereby calls for the establishment of "Global Digital Forensic Center" as a subsidiary or agency of the United Nations, like UNICITRAL, UNDOC etc. There is no argument that cybercrime is a global issue, ipso facto, a global approach is expedient to frontally tackle that menace, to wit, cybercrime with its so much pervasive global threat to individuals, corporates and governments. The recommended Global Digital Forensic Center (GDFC) should be staffed with well-trained forensics laboratory experts with robust legal knowledge, particularly digital evidence gathering, analysis and preservation, who would only attend to issues of digital evidence beyond the level of nation-state forensic experts. The center shall be training resource center for national investigators and prosecutors, whereat they shall be kitted with digital scientific evidence and sound legal knowledge. In order to ensure optimal rendering of effective services that would put activities of cybercriminals in check, the proposed center must be equipped with state-of-the-art technology including needed software with inbuilt precision and mechanical accuracy for forensic evidence collection, preservation, accurate analysis, be all that as it may for investigators, it is equally not negotiable that prosecutors for the purpose of securing conviction of cybercriminals, are well grounded in the art, science and legal gymnastics of thorough knowledge of online investigative technics, tracing digital footprints and of course, the presentation of incontrovertible evidence laden with technicalities in very simple, clear and easily digestible manner before the courts, seized of high-profile cybercrime cases.

Closely related to the setting up of Global Digital Forensic Center is the recommendation that each sovereign nation should set up National Digital Forensic Center which shall be the hub of digital forensic experts comprising investigators, analysts, cybersecurity and prosecutors. All the human and inanimate requirements, such as, hard and software advocated at the global level should be replicated at the national level and with constant training and development of the personnel, so as not only stay abreast of trends in cybercrime issues but be far ahead of plots by cyber actors in their ruinous activities.

Given the scary submission to the effect that, if cybercrime were to be measured as a GDP of a country, it would be the third largest economy after US and China [103], and further


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

that, it is indisputable that, cybercrimes traverses across many jurisdictions and countries thereby wreaking havoc and leaving sorrow in its trail, it is on those grounds that this article forcefully recommends that a special court should be established as Cybercrime International Court (CIC) to specifically address cases of cross country cyberattacks, with a sum more than USD 5 million, in the alternative, a special unit named International Cybercrime Unit (ICU) should be set up, under International Criminal Court (ICC), to preside over cases of cyber infractions as earlier stated. The implementation of this recommendation shall with certitude, send the appropriate signals to cyber actors that, it is not going to be business, as usual.

Section 5.2.4 of this paper deals with absence of standardization of digital forensics practices and procedures, to surmount this hurdle regarding digital forensics standardization, this research's recommendation is that ISO/IEC 17025 accreditation, should be adopted. The certification by the joint cooperation of International Standard Organization (ISO) and International Electrotechnical Commission (IEC) confers reliability, validity, and reproducibility of forensic evidence, thereby making the evidence without any iota of doubt, admissible not only in the courts of law, but acceptable to members of the public [104].

Section 5.2.5 of this research addresses the challenge of no uniform rules for admissibility of digital evidence. The fact needs no over flogging to the effect that, where no uniform rules for admissibility of digital evidence exists, same definitely occasion legal chaos where worthy evidence are rejected and inadmissible evidence are admissible. To scale the afore stated hurdle, nation-states are strongly advised to amend their extant law of evidence, which probably came into force before the widespread use of computers and ICT, to make strong provisions for electronic architectures, records and admissibility of digital evidence. In addition, stake holders are advised to use uniform protocols, by following established, standardised format for digital evidence deciphering, gathering, acquiring, storage and analysis. Technically and meticulously maintain custody chain, regarding audit logs of every transaction and interaction with the digital evidence, detailing whose custody was it, why, for what reason(s) and for how long, who handled it, when, and for what purpose. The foregoing recommendations shall without doubt improve the credibility and admissibility of digital evidence.

To ensure data integrity, the use of hashing, that is, a means of keeping sensitive data and information, such as, messages, passwords and documents, secure, is encouraged by employing cryptographic hash functions, such as, SHA-256, that creates a special fingerprint of the digital evidence, which ensures that evidence has not been interfered with. Another potent recommendation for admissibility of evidence is the employment of tamper-evident storage, which utilizes preservation storage solutions, as well as, file management systems, which detect or outrightly prevent unauthorized alteration(s), to the stored evidence.

Above all, this research recommends the preservation of digital evidence with layers of security measures, including the use of not only physical but digital isolation of devices, including the diligent management of all encrypted files [105].

Section 5.2.6 of this research discussed the challenges associated with volatility of digital evidence and the crucial issue of preservation of the said novel brand of evidence, this study unequivocally recommends that the collection should be by experts only, and placed on very high priority because of their innate nature of volatility, further, forensic images should be created making exact bit-for-bit copy of the original evidence's storage device, to preserve the data's integrity. All acts done during collection and preservation processes, such as, the time, dates, methods, locations, processes and personnel involved must be meticulously recorded. Use of hashing, that is, a means of keeping sensitive data and information, such as, messages, passwords and documents, very secure, is recommended, and so is chain of custody of the evidence, with the view to knowing who was in possession and the rationale for same. Above all, the evidence must be well secured in controlled environment, in order to avoid unauthorized access, damage, alteration etc. For the storage, it is important that new or clean media must be made use of in order to obviate contamination. Most important of all, is the need to collaborate with only experts, who are specialists in handling the intricacies associated with digital forensic evidence, particularly the preservation and analysis, all of which enhances the credibility of the garnered evidence [106].

Under sections 5.2.7 and 5.2.8 of this paper, the dearth of competent investigative personnel and inadequate number of human capitals for prosecution of cybercriminals were amply discussed, as factors militating against thorough investigation and diligent prosecution of cybercrimes. These challenges, as fundamental as they stand, are not insurmountable. On that note, to overcome the lapses of personnel in this arena of cybercrimes investigation and prosecution, a serial well-planned programs of training and development is the recommendation proffered by this paper because, it is well settled that the importance of training and development cannot be over emphasized, given the myriads of advantages conferred on the employee and the organizations that sponsor the projects, in summary, training and development brings about employees higher skills and enhancement of knowledge, increased productivity, effectiveness and efficiency, they have improved job satisfaction and are motivated, there is also high adaptability in handling apparent complex work tasks and handling of new technologies, as well as, be amenable and less resistance resistant to change. Besides all the foregoing, training and development enhances problem solving capabilities of trained staffers, boosts their confidence, leads to increased engagement and less labour turnover, as a result of commitments,


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

last but not the least, is the alignment of employees' desires with set organizational policies and goals [107].

This research holds the view that it is through training and development that the main roles and responsibilities expected of investigators, could be effectively realized, which said roles includes evidence collection from various ICT sources, digital forensics via analysis of computer systems, cyber event analysis, providing legal documentation to be tendered in court by prosecutors, working hand in hand that is in collaboration with others in the war against cybercriminals, carrying out threat intelligence, vulnerability assessment and forensic examination [108]. In order to aid prosecutors in the effective performance of their onerous duties, this study hereby strongly recommend training and development, such roles and responsibilities of cybercrime prosecutors includes initiation of legal proceedings against malicious cyber actors, with the principal aim of conviction, evidence analysis and guidance to investigators on collection, preservation, and analysis of digital evidence regarding the integrity of said evidence and admissibility, provision of technical and legal expertise, prosecutors collaborate and coordinate with other law enforcement agencies, home and abroad, intelligence sharing and capacity building, brings forth global cooperation on training, intelligence, investigations, capacity-building related to cybercrime prevention and prosecution, employs strategic disruption to cyber actors machinations, provide professional counseling on emerging cyber threats, contribute to policy and law development [109].

In addition to training and development of investigators and prosecutors, this study also recommends a commensurate remuneration and fair terms and conditions, adequate security and maximum protection for these categories of personnel, this would not only encourage and motivate them but certainly obviate the possibility of being compromised by cyber actors, who are believed to be moneybags. With regards to section 6 of this paper, as radical as the challenges of jurisdiction is in cybercrime cases, same are minimizable through the instrumentality of the following legal and quasi-legal means: International cooperation is advocated between countries facilitated through treaties, sub-regional and regional agreements, particularly with respect to mutual legal assistance (MLA) and suspect or criminal extradition, this step goes a long way to paving way for nation-states to cooperate, in the efforts towards investigation and prosecution of cybercrimes

Training and capacity building connotes that investment must be made in advanced training for law enforcement agents and criminal justice professionals, that is, the prosecutors, particularly in evidence collection, digital forensics and advanced investigative techniques. Public-private partnerships are essential between governments, law enforcement agents, technology companies, and civil society to share information, develop solutions, and enhance investigative capabilities. One critical area as far as jurisdiction is concerned, in cybercrimes issues is standardization in the handling of digital evidence, and the solution is developing and implementing uniform standards for the gathering, preservation, and analysis of digital evidence so as to be certain regarding the integrity, and admissibility of the evidence in courts. There is need for the development of flexible legal instruments primarily crafted and adaptable to the borderless nature of the internet, so as to properly address the cross-border nature of cybercrimes.

In addition to the above is the continuous revision of legal frameworks in order keep phase with rapid technological advancements and the evolving nature of cybercrime [110].

It should be carefully borne in mind that the concept of sovereignty and territorial integrity confer absolute powers on each country of the world, to make laws regulating activities of all persons and inanimate things situate in a country, that blanket authority has not worked and will never work where the issue of cybercrimes is concerned because, this novel offence, have no respect for jurisdiction. Bearing in mind the foregoing submission, the first and foremost recommendation which this study proffers is legislative and legal reform and that starts with harmonizing the extant laws to lessen the disparities currently thwarting cybercrimes investigation and prosecution across the globe, closely following that, is the dire need to gravitate towards greater standardization of nation-state cybercrime laws, not only that but also the evidentiary rules, to be in tandem with global standards regarding the collection, storage and of course, admissibility of digital evidence. Further, there is the necessity to constantly update nation-states laws to be at par with daily evolving cyber threats, so as to ensure that the updated laws take care substantially the facets of evolving cybercrime.

In addition, to mitigate the adverse effects of jurisdiction on the path of cybercrimes investigation and prosecution, aside from making necessary adjustment to the law as stated in the above paragraph, are international cooperation recommendations which means there is necessity for the establishment and utilization of networks for contact points, which in turn shall enable the timely communication and much needed coordination amongst law enforcement, prosecutors and judicial personnel worldwide, thus, there is invariable need to share not only information but best practices, particularly with exchange of information on cyber threats, methodologies, tactics, and nation-state modalities to address cybercrime frontally. Further, to make the international cooperation as recommended in the above paragraph work as effectively as possible, it is expedient to pay massive attention to the development and improvement of MLA frameworks, so as to quicken not only the gathering but the sharing of the much-needed digital evidence, across boarders.

It should be carefully borne in mind that the above two recommendations of updating the laws and international cooperation may not achieve the desired effect of lessening the adverse effects of jurisdictional challenges on cybercrimes


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

investigation and prosecution, if the nation- states human capital are not overhauled and positioned to face challenges associated with jurisdiction regarding investigation and prosecution of cybercrimes, it is on that ground that this paper recommends there must be heavy investment by national governments to provide specialized and comprehensive training for law enforcement personnel, prosecutors, as well as judicial officers in digital forensics, cybersecurity and evidence handling. Specialized national / state cybercrime units (NCCUs) to centralize expertise and coordination of efforts towards prevention, investigation, and prosecution of cybercrimes. Public-private partnerships must be developed between government and private sector entities for the purposes of improved investigative capabilities, and improved sharing of cyber threat intelligence. Above all, there is the non-negotiable need for the creation of online national reporting centers, a platform which must be easy to access and use by the general members of the public for reporting cybercrimes, and on the other hand, for investigators to gather the much need information on cybercrime threats and trends [111].

Under section 7 of this research, the apathetic disposition of victims towards the reporting of cybercrimes and data dearth was discussed. The starting point to changing the attitude of cybercrimes reporting to the concerned authorities, is for the governments and other stake holders to set up awareness campaigns, so as to inform people across the world that, it is not a crime to be scammed by malicious cyber actors, that, there is no stigmatization in that respect, because any one be it individual or business, could be a victim. Aside from using radio and TV for public service announcements, social media should be massively employed to create indelible public awareness, such that, the general members of the public are roundly educated as to the impact and destructive tendencies of cybercrimes on the people and economy of countries across the globe. Besides the foregoing, handbills should be printed and distributed at public places, such as, schools, hospitals, pharmacies, parks, recreation centers, post offices, banks, etc., and also at fast foods, canteens, bars, offices, sporting avenues etc., to show awareness. The importance of reporting even the most trivial cyberfuneral should be emphasized to the effect that, same leads to the tracking of cybercriminals. It is hereby recommended that nation-states across the globe, should as a matter of urgency set up digital, simple to understand and operate reporting of cybercrimes systems, preferably that would not reveal the identities of the reporting victims, by this, victims would be free to express their ordeals. The suggested system would be an excellent means of gathering pertinent information by law enforcement agencies, with the view to tracking, locating, arresting, prosecution and where necessary, the conviction of cyber offenders.

This paper under section 8, discussed the absence of standardised international protocols for cyber security, as a challenge confronting investigation and prosecution of cybercrimes, this development is perceived as a man-made one, and same could be totally obliterated and if not, reduced to the barest minimum by the recommendation to the effect that, international cooperation and governance should be established to encourage global standards through collaboration between governments and industry for unification of cybersecurity standards, via the building on the extant models, such as, ISO 27001 [112] and the NIST [113], Cybersecurity Framework.

Further, as a recommendation, the enhancement of Public-Private Partnerships is advocated towards strengthening the collaboration between public institutions and private companies, to not only drive the development, but effective implementation of the recommended standards. With the view to promoting harmonized certification, governments across the globe are enjoined to work cooperatively together, so as to define broad certification schemes, thereby allowing final consumers to verify that products and services, actually comply with international security standards. Finally, in a bid to realize standardised international protocols for cyber security, it is indispensable that national modalities and enforcement must be put in place via the incorporation of standardization into nation-states strategies, whereof governments should make standardization a fundamental component of national cybersecurity modalities, thereby creating a link between policy, and effective operational levels.

It should be added at this juncture that, nation-states regulatory authorities should cooperate and use standards agreed-upon, as a measure for enforcement of cybersecurity regulations. Having exhaustively recommended for the private-public partnership, it is necessary to address what industry and organizational actions should do, to wit, there should be adoption of frameworks and of best practices by implementation of frameworks, such as, NIST CSF with the view to identifying and managing of cyber risks, a theme which covers areas from threat intelligence, the assessment of risk, and the necessary response.

This paper strongly recommends the implementation of solid foundational security measures, like strong access controls, adoption of multi-factor authentication (MFA), constantly carrying out the updating of software, as well as, carrying out beneath-the-surface risk assessments, and mandatory vulnerability assessments. It is recommended that a zero-trust policy to security should be implemented, which connotes that, no user, no matter the status or device, no matter the level of mechanical accuracy, should be automatically trusted, this policy measure, of course, strengthens the security posture.

In addition to above is the recommendation that, education in the form of cybersecurity training and development and awareness regarding cyber threats, should regularly and constantly be embarked upon throughout all cadres of the organization, and as a matter of unwaivable obligation, a very high level of cyber hygiene must be maintained, such as, secure network practices, strong password management, and extra vigilance against phishing and other forms of cyberthreats, for all stakeholders, be it individuals or organizations [114].


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

Section 9 of this study discussed the challenges associated with inadequate and or non- existent uniform extradition treaties. It is well known and a settled fact that, when criminals have committed infraction against the law, they usually escape to other jurisdictions to avoid prosecution and punishment, should they be found guilty. The only option left to the law is extradition, but this process is laden with so many exceptions, so much so that, the exceptions have almost overridden the rule. The first and most important recommendation which this paper proffers regarding extradition of persons accused of criminal act involving cybercrime, is the immediate and total abolition of the "dual criminality principle" on the ground that, a crime is a crime, and once a crime is committed and an entity, human or inanimate is a victim, punishment must be meted out to the perpetrator or better still, if the offence is tortious, the doctrine of *restitutio in integrum,* must apply [115].

To do otherwise, amounts to gross injustice to the victim(s) who bear the burden without restitution or reprieve. More importantly is the unassailable fact that, the dual criminality principle emanated from the very old matter of USA and UK which culminated into the signing of the Jay Treaty [116], also referred to as the Treaty of Amity, Commerce, and Navigation dated 19th November 1794, that is, three hundred and thirty one (331) years ago, long before the Internet offence of cybercrimes, made its advent into the global legal landscape. This research unflaggingly holds the view that whatever justification(s) prompted the dual criminality principle in 1794 particularly with respect to cybercrimes nowadays, is no longer in tandem with the reality of the modern time, where a cyberspace crime committed at one jurisdiction can have very adverse effects at other faraway jurisdictions [117], therefore, the dual criminality principle, should be completely expunged from international statute books, regarding extradition, with particular reference to cybercriminals.

The next recommendation towards minimizing the challenge of extradition, is the invariable need by nation-states to give unalloyed support by throwing their political and diplomatic weights, to the encouragement and promotion of universal treaties, such as, the Budapest Convention [118], a model law, and which other countries could use as a framework towards the drafting and enactment of their respective cybercrime laws, and of course the recently enacted United Nations Convention on Cybercrime [119], a global instrument, targeted at the unification of legal frameworks for worldwide cooperation and harmonization of cybercrime enactments, across the globe. The said cooperation and harmonization are applicable to cyber infractions, with the view to easing the conduct of extraditions and the much-touted mutual legal assistance (MLA), all over the world.

It is in the light of the foregoing, that this paper recommends the building up of the MLA with the view to aiding the unhindered and swift collection, as well as, the preservation, and of course, the electronic evidence sharing amongst law enforcement agencies, a development which would with certitude, lead to the cracking of complex and trailblazing cybercrime cases. To further strengthen the cooperation between continental, international and regional bodies, there is dire need to effectively make use of services provided by Australian Border Force who specializes in regional border security for the Oceania, the European Border and Coast Guard Agency (Frontex) and the European Union Agency for Criminal Justice Cooperation (Eurojust) for the European continent, the United States' Department of Homeland Security for North America, Regional Security System (RSS) for Caribbean nations, Joint Task Force Support Forces Antarctica (Operation Deep Freeze) and international security organisations, such as, International police (Interpol) and renown entities like FBI, CIA etc., with the view to facilitating swift communication, as well as, effective cooperation amongst law enforcement agencies and the judicial authorities in all the nation-states, of the world.

This paper holds the view that no matter the level of investment committed against cybercrimes would make a meaningful impact, if the personnel saddled with the onerous duties are not empowered with human capital training and development, it is in the light of this trite submission that more resources should be globally committed to the training and development of cybercrime investigators and court prosecutors, so as to be abreast of developments regarding rapidly evolving technologies and cybercrime trends, it is in doing this that the "cybercrime war," could be effectively won. Section 10 of this research addressed the need for the balancing of individual privacy and data protection with law enforcement agencies needs to access data, with the view of investigation and prosecution of cybercrimes, it is hereby submitted as hereunder: The view is held that, the right to privacy of the citizenry is an inalienable one, as such, that right must be preserved, however, in the face obvious exacerbation of cybercrime threats to humanity whose dependence on the Internet is beyond doubt, it is strongly recommended that law enforcement agencies should have access to people's data, but that right should be with caution, to the effect that, only relevant data to investigation of cybercrimes should be accessed.

Further, this paper is of the firm believe that whosoever does not desire that his or her data accessed by law enforcement agencies should not use the Internet. The population of human rights activists and those that they are advocating for non-accessibility of data, are far less than all the people of the world, as such, the number of those who have no objection to law enforcement agents accessing our data, are far more than those who do not, this study believes in democracy and way of the people, democracy is a game of numbers, ipso facto, those who do not want their data accessed, might as well stay off the Internet.

In a bid to achieve transparency and accountability regarding accessed data, an oversight function is prescribed for law enforcement agencies to oversee and monitor which data are being accessed and for what reason(s), there is also the need


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

to conduct regular auditing processes, if after monitoring and auditing are carried out, should any law enforcement officer(s) are found wanting, they should be heavily sanctioned for infraction and for abuse of office, according to laid down procedure. In as much as this paper believes that law enforcement agencies should have latitude to access people's data, there must be clear legal framework regarding data collection, how the said data is protected and made use of, nay, should there be any need for monitoring and or surveillance, unambiguous policy guideline must be in place so as to avoid ambushing the people and denying them their inalienable right to privacy. Finally, to achieve probity and effectiveness in data access, there is need for training and development of the personnel involved, this to aid them in precisely knowing their duties and obligations, in these onerous tasks.

Section 12 of this research deals with apparent lack of public-private sectors collaboration and global cooperation between sovereign nation-states. This paper has not alleged total absence of public-private sectors collaboration and global cooperation, but from all indications, efforts in that regard is disjointed and not concerted, it is in the light of that unfortunate development that this paper recommends that, more investment and coordination should be channeled towards sharing of knowledge, expertise and information regarding new technologies particularly the fast-spreading Artificial Intelligence (AI), advanced connectivity, data and computing etc., this would without doubt, appreciably raise the current level of cyber defence, investigations and prosecutions that would yield convictions.

The lack of public-private sectors collaboration and global cooperation was amplified as one of the rationales why cybercrimes continue to grow, because private and public entities are independently tackling the menace, a development which leads to fragmented and uncoordinated efforts, be that as it may, the impact of private sector cannot be over emphasised in terms of their huge contribution to the economic wheels of nation-states [120]. On the strength of the foregoing incontrovertible importance of small and medium firms, there is a great need for collaboration between public and private partnerships with the view to sharing intelligence pertaining to cyberthreat via the putting in place of real-time information exchange mechanism between law enforcement officers, and the cybersecurity outfits of the private sector, so as to facilitate a coordinated, joint and proactively respond to cyber threats, as well as, with alacrity, effectively track malicious cyber actors' to their havens.

In order to effectively confront, particularly assist in the investigation and prosecution of cybercrimes, there is unavoidable need for collaboration with all industry stakeholders, such as, working with ISPs, all online service givers, and infotech companies to go back to the drawing board to expunge cybercrime by in-built security systems and features, including the promotion of risk-free online behaviour. Further, public and private sectors are enjoined to develop and implement joint operations with the principal goal of dealing devastating blows that would scatter criminal infrastructural activities, of the illegal cyber actors.

The paper holds the view that super-experts in cybersecurity matters, are not many across the globe but a good number of them are in the private sectors, where the remunerations and terms and conditions of service are more rewarding than in the public sector, on that note, this paper calls for the establishment of impregnable platforms with the view to sharing real- time information and statistical data with respect to cyberthreat intelligence between private sectors and law enforcement agencies, this development, shall go a long way to minimizing the impact of cybercrimes across the globe.

In order to step up the level of cooperation between private sectors and public law enforcement agencies, this paper advocates that there is a need for exchanging of information and data, arising from cybercrimes investigations, nay, the experiences garnered from prosecution of cybercrimes at various courts seized of cyber offences trials, the advocated experiences, when exchanged or shared, would go a long way to boosting the capacities of cybercrime investigators and prosecutors.

Aside from information sharing about threat intelligence and experiences regarding investigations and prosecution of cyber infractions in courts, as elsewhere advocated, this paper recommends joint training schemes and developments between private-public sectors, this would go a long way to strengthening the collaboration between the parties and make the battle against cybercrimes, a concerted approach. The roles of Internet Service Providers (ISPs) cannot be swept under the rug, when the issue of tackling cybercrimes comes up for discussion, it is on that note that this paper recommends that all impediments to private-public partnerships, be it legal, geographical or technical, and however arising, should be removed in order to swiftly pave way for ISPs to make available all the necessary statistics, data and information, to cybercrime investigators.

The preceding paragraphs essentially addressed collaboration between private and public entities, with the view of joint action and or operation. Cooperation on the other hand, is basically between two or more sovereign or independent countries, working jointly with the goal of achieving a common interest, to wit, drastic reduction or substantially putting cybercrimes at bay. In that regard, there is need more than ever, to cooperate at the international level through the adoption of worldwide conventions, as elsewhere elaborated upon before now that, cybercrimes is a global scourge, as such, it is only global cooperation, joint actions and focused efforts of allied nations, that can effectively address the ever-escalating incidents of cyber threats and cyberattacks issues. The Budapest Convention on Cybercrime 2001 [121], the African Union Convention on Cybersecurity and Personal Data Protection 2023 [122], and the United Nations Convention against Cybercrime 2024 [123], are typical examples of international


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

treaties signposting the global efforts specifically targeted at addressing cybercrimes on cross-countries investigations, and the establishment of legal standards which are common. This paper hereby recommends more cooperation at the international level and urges countries which have not accented to cybercrimes international instruments, to do so as early as possible, it is in doing this, that the menace of cybercrimes can be effectively addressed.

Intelligence information obtained regarding cyber threats and not shared, is not only useless but indeed counter-productive, malicious cyber actors would naturally continue to unleash mayhem on hapless people, it is in the light of this development that this paper strongly recommend that there is need for the expansion and intelligence exchange as a form of cooperation between different countries law enforcement agencies, such that, when threat intelligence is shared, joint and cooperative efforts can be harnessed, to tackle whatever cyber threat challenges posed to the critical infrastructures of nation-states, this development would go a long way to stemming the tide of cybercrimes.

As another brand of international cooperation between countries, this study recommends human capacity building by the developed nations for the less privileged ones, by provision of training and development of human capital and technical assistance to developing countries with the view to upgrading their cybersecurity infrastructure and architecture, in order to assist developing countries to strengthen their national capabilities, in the fight against cybercrimes. At the global level particularly with respect to cooperation between nation-states of the world, one of the greatest encumbrances militating against cybercrime war is the concept of territorial integrity, subsumed under sovereignty and independence of nation-states, such that, when cybercriminals escape from where they are wanted, they take refuge in other countries which makes it difficult, if not impossible, to investigate and prosecute the cyber offenders, it is on the ground of the foregoing assertion that, this paper highly recommends that there is dire need to build a more friendly and robust diplomatic relationships between countries of the world, rooted in trust, confidence and cooperation with one another, such that, the cybercriminals would have no hiding places, particularly in cyber cases traversing several countries of the world.

In consonance with the foregoing recommendation, is the hard truth that the state of global extradition legal framework is laden with loopholes, it is amorphous, sometimes contradictory and offensive to the sensibility of a discerning mind, it is on this basis that this paper recommends that there is need for unification and standardisation of the global legal frameworks with respect to extradition laws, so as to ensure harmony and effective extradition of cybercriminals. As elsewhere stated before now to the effect that, individuals and corporates are cagey about sharing information regarding their cybercrime's setbacks, particularly because of the reputational damages which could arise, ditto are nation-states, on that note, one pertinent area of global cooperation advocated by this study, is the need for truthfulness and transparency in data, statistics and information sharing, regarding cyber threats and cyber breaches to showcase the patterns, the severity and types, the mitigation strategies adopted and their impacts, all these would go a long way to providing the elicitation of better measures to adopt, at the global level in addressing the scourge of cybercrimes.

This research is of the view that all nations of the world have cybersecurity ministries or agencies protecting their critical infrastructures, in a bid to strengthen the existing fragile global cooperation on cybercrimes, it is hereby recommended that a Regional Cybersecurity Union should be created which after sometime of operation at the regional level, could metamorphise into Continental Cybersecurity Union and later to Global Cybersecurity Union, this proposed bodies should share real time information, data and statistics on cybersecurity and work with existing global bodies tackling crimes, such as, United Nations Office on Drugs and Crimes (UNODC) and International Police (INTERPOL), this recommendation would appreciably strengthen the fragile global cooperation, and give a fillip to the cyber war.

This paper is on all fours with some cerebral legal wigs to the effect that, international law is no law because, it has no enforcement mechanisms, be that as it may, it is hereby recommended that at the diplomatic level, nation-states authorities should unanimously impose heavy pecuniary fines and other punitive measures, such as, suspension for countries not acting as they should, and that includes willful refusal to cooperate with others in the investigation and prosecution of cybercrimes, or aiding and abetting cybercriminals by providing safe haven for them, which of course makes prosecution practically impossible, and in turn, emboldens the cyber actors to commit more cyber breaches.

## The need for heavy investment in ICT infrastructures

Finally, there is no doubt that the cybercriminals, their sponsors and those benefitting from the illicit activities are by all indications very rich as a result of the easy proceeds derived from cybercrimes, which they invest heavily on tools and machinery, to further their nefarious activities, it is in the light of this unassailable fact that, this research calls on governments across the globe to also invest in high tech tools and machinery for the benefit of protecting their respective critical infrastructures, so as to forestall irreversible damages to power supply, oil and gas, water, cybersecurity etc. Not only the above but also, the call for investment by governments all over the world, would also benefit the people and save innocent souls from activities of cybercriminals and their accomplices.

This paper further calls on corporate bodies to also invest heavily in ICT infrastructures because, the said corporates, bear the worse consequences of cybercrimes more than all other


How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

sectors of any economy, besides the indisputable fact that, the sum of expenditures channeled to after-effects of cybercrimes, is humongous. Aside from the foregoing, all the adverse consequences and costs of cybercrimes which includes but not limited to, customer turn away arising from reputational damages [124], supply chains disruption [125], intellectual property loss, employment disruptions and job losses, cost of mitigation and repairs to damages of work tools and equipment, insurance premiums, legal fees, fines and penalties levied by authorities, can thus be usefully used in other areas, such as, more investment opportunities that would generate multiplier effects, on the economies of countries and appreciably improve the Human Development Index (HDI) of the global citizenry.

## References


1. Merriam-Webster (2025) cyber: of relating to, or involving computers or computer networks.
2. T J Holt and A H Bossler (2021) Cybercrime and Digital Criminology: An Introduction 23.
3. EFG Ajayi (2024) The need for the employment of cyber insurance, by global corporate bodies in mitigating the unavoidable risk of cyberattacks. British Journal of Cyber Criminology.
4. Oxford Dictionary of Law, 5th Edition
5. Adebayo A and Kekere A (2016) Electronic Commerce in Nigeria: The Exigency of Combatting Cyber Frauds and Insecurity. J Law, Policy Globa 47: 159-160.
6. Cormier, Monique and McKenzie (2022) Legal Issues in Information Technology Cyber-Dependent and Cyber- Enabled Crime: Legal Responses and Challenges 99-128.
7. EFG Ajayi (2016) Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information 6(1).
8. National Cybersecurity Policy Framework for South Africa, 2012 Cybercrime Definition.
9. EFG Ajayi. The need for the employment of cyber insurance, by global corporate bodies in mitigating the unavoidable risk of cyberattacks. British Journal of Cyber Criminology.
10. Estefania Vergara Cobos and Selcen Cakir, A Review of the Economic Costs of Cyber Incidents World Bank.
11. Cybersecurity Facts, Figures, Predictions and Statistics. Cybercrime Magazine
12. 2023 Official Cybercrime Report.
13. Report Allianz Risk Barometer 2023.
14. Cybercrime To Cost The World USD 9.5 trillion USD annually in 2024
15. World Crime Index University of Oxford
16. How much does each country spend fighting cybercrime?
17. British Journal of Cyber Criminology.
18. Willaim E Wall, Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime 45 (2d ed. 2021)
19. Pew Research Center Anonymity, Privacy, and Security
20. Autogpt. Cybersecurity Is true anonymity online a myth or reality.
21. Havard Kenndy School (2025) Belfer Center for Science and International Affairs Why Online Anonymity Matters.
22. Packtpub. 10 great tools to stay completely anonymous online.
23. Marie-Helen Maras Computer Forensics: Cybercriminals, Laws and Evidence 2014 2nd ed.
24. SCC 43, ([2014) 2 S.C.R. 212
25. (2010) EWHC 3308. See also ZXC v Bloomberg LP (2022) UKSC 5.
26. EFG Ajayi (2016) Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information 6(1).
27. Susan W Brenner. Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law.
28. Claudia Munoz and Micheal Sanders (2022) The Role of Digital Forensics in Modern Criminal Investigations, particularly those Involving Cybercrime. 1 Journal of Cyber-Security 7: 1-18
29. Naeem Allah Rakha (2024) Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mex law rev 16(2).
30. Vahid Alireza and Dehghantanh (2022) The Challenges and Gaps in Digital Forensics and Legal Frameworks for Handling Digital Evidence. Journal of Forensic Sciences and Criminal Investigation 1: 1-10.
31. Anthony Coo (2022) Overwhelming Amount of Data Generated by Modern Devices and Platforms. Journal of Digital Forensics, Security and Law 17: 1-10.
32. Kang Min-Seok, Park Jong-Hyouk and Lee Sang-Ho (2021) Long Delays in Digital Evidence Analysis and Its Impact on Investigations. Journal of Digital Forensics, Security And Law 16: 45-56.
33. Goswami Anushka and Thakur Lokesh Kumar (2021) Challenges of Extracting and Analyzing Digital Evidence from Different Devices and Platforms. International Journal of Cyber Criminology 15.
34. Thomas Holt and Lauren Holt (2021) The Increasing Use of Encryption and Other Security Measures to Protect Digital Data, 4 Journal of Digital Forensics, Security and Law 16: 23-44.
35. Daniel Bamum and Diana German (2021) Accessing and Analyzing Encrypted Digital Evidence Without the Encryption Key. Digital investigation 38: 36-45.
36. Eric Rosenbach and Micheal Sulmeyer (2022) The Balance Between Privacy Rights and Investigative Needs in the Context of Encryption. 1 Harvard National Security Journal 13: 1-22.
37. Onn Kerr (2020) The Curious History of Fourth Amendment Searches. 8 Texas Law Review 98.
38. S Brenner and J Schwerha (2018) Cybercrime and jurisdiction: A Global Problem Requires a Global Solution, Berkeley Journal of International Law 36: 228-283.
39. Naeem Allah Rakha (2024) Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mex. law rev 16:2.
40. S Anchalee and C Thawatchai (2021) The Challenges of Admissibility of Digital Evidence in Court. 1 International Journal of Cyber Criminology 15: 67-85.
41. Kerr O (2021) The Rules of Evidence in the Digital Age, 6 Harvard Law Review 135: 1652-1671.
42. Friedman B and Kamik A (2021) Balancing Privacy Rights and Investigative Needs in the Digital Age. Journal of National Security Law and



How to cite this article: EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

Policy 13: 69-96.

43. Kerr O (2020) The Curious History of Fourth Amendment Searches, 8 Texas Law Review 98.

44. Koops B and Leenes R Privacy (2017) Data Protection, and Cybersecurity in Europe, 2 Computer Law & Security Review 33: 163-175.

45. Sallmen M, Kukka H (2021) Preserving Digital Evidence: Specialized Tools And Techniques. J Digital Forensics Secl 83.

46. Nwokedi J, Kessler G (2022) Digital Forensics: A Critical Shortage Of Qualified Examiners. J Forensic Sci 266.

47. EFG Ajayi. Challenges to enforcement of cyber-crimes laws and policy.

48. Beebe H, Clark T (2021) Evolving Digital Forensics: Challenges And Opportunities. J Digital Forensics Secl 31.

49. Goodall J, Cate F (2022) Balancing Privacy, Security, and Civil Liberties in Digital Investigations, 11 J.l. & Cyber Warfare 41.

50. EFG Ajayi (2016) Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information 6(1).

51. Sanusi Aiyeriyina Alade v (1988) Olalere Akanji Alemuloke & Ors. 1 N. W. L. R. (pt. 69) 207

52. EFG Ajayi. Challenges to enforcement of cyber-crimes laws and policy.

53. (1988) 1 N. W. L. R. pt. 84 at 587.

54. (1962) 1 All N. L. R.

55. Leflar: Jurisdiction and Conflict of Laws p. 223

56. Latin expression meaning "against a person" opposite of "in rem" against a thing, for example, property

57. 903 N.E.2d 73 (Ind. App. 2009).

58. EFG Ajayi. Challenges to enforcement of cyber-crimes laws and policy.

59. Prof, Ulrich Sieber (1998) The legal aspects of computer related crimes in the information society. Comcrime study. Version 1.

60. EFG Ajayi. Challenges to enforcement of cyber-crimes laws and policy.

61. Harsh Kumar (2024) A Comprehensive Analysis on Jurisdiction Issues in Cyber rimes, International Journal of Research Publication and Reviews 5(4): 4178-4187.

62. 39 326 U.S. 310, 66 S. Ct. 154, 90 L. Ed. 95 (1945).

63. 130 F.3d 414 (9th Cir. 1997).

64. 952 F. Supp. 1119, 1124 (1996).

65. 465 U.S. 783, 104 S. Ct. 1482, 79 L. Ed. 2d 804, 1984 U.S. 41.

66. See generally, Harsh Kumar (2024) A Comprehensive Analysis on Jurisdiction Issues in Cyber rimes, International Journal of Research Publication and Reviews 5(4): 4178-4187.

67. USA Federal Bureau of Investigation Annual Report

68. Nzeakor O, Nwoke C and Okafor R. Why do cybercrime victims fail to report their victimization experiences to the police? a survey of the factors of poor attitude towards reporting cybercrime victimization in Nigeria.

69. EFG Ajayi. Challenges to enforcement of cyber-crimes laws and policy.

70. Novas-Peña A (2024) Lack of International Cyberspace Regulation Threatens Human Rights and International Security. Human Rights Research Center.

71. Generally, see Frank Cremer, Cyber risk and cybersecurity: a systematic review of data availability. National library of science. National center for biotechnology information.

72. United Nations Office on Drugs and Crime Organized Crime Module 11 Key Issues: Extradition. UNODC

73. See https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=92661.

74. Brazilian constitution of 1988, Article 5 www.stf.jus.br/repositorio/cms/...en./constituicao_ingles.

75. Austrian Extradition and Legal Assistance Act Section 12 See http://www.ris.bka.gv.at/geltendefassung.wre

76. Code of criminal procedure (legislative part), Articles 696-1 to 696-7" (PDF). http://www.legifrance.goun.fr.

77. Law of Extradition Japan Article 2 See http://www.moj.go.jp/english/information/loe.01.html.

78. Charter of fundamental rights and freedoms, Article 14 (4) http://www.usoud.cz/en/charter of fundamental right.

79. Basic Law for the Federal Republic of Germany, Article 16 (2) http://www.bundesrecht.juris.de.

80. United Nations Office on Drugs and Crime. Ibid

81. Brenner SW (2025) Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law.

82. It has been submitted that the *aut dedere aut judicare* clause exists in various forms in 30 multilateral treaties and in 18 regional conventions. See Graduate Institute Publications, Sources of the "aut dedere aut judicare" obligation.

83. Vera Alizade, Extradition in the Age of Cybercrime: Legal Dilemmas and Policy Gaps in Cross-Border Prosecution.

84. (2018) EWHC 172 (Admin).

85. INFORMATION AGE Definition and Meaning.

86. How can we balance security and privacy in the digital world?

87. Balancing Privacy and Security and why the two are not mutually exclusive

88. See generally, I. M. Portela and M. M. Cruz-Cunha, What About the Balance Between Law Enforcement.

89. The GDPR was enacted principally with the view to not only protect individuals' personal data but in addition, the privacy of citizens within the jurisdiction of EU and the European Economic Area (EEA).

90. United Nations Office on Drugs and Crime, https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf. (Date of use 15 August 2025).

91. Ni Komang Novia Widiasari and Emmy Febriani (2024) International Journal of Innovative Research in Computer and Communication Engineering 12(2)

92. Sarah Stummer (2016)A Right to Anonymity in the Digital Age: A Discussion of the Opportunities, Risks and Limitations. See also E. Moyakine, Online Anonymity in the Modern Digital Age: Quest for a Legal Right. Journal of Information Rights Policy and Practice 1(1).

93. Naeem Allah Rakha, Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mex. law rev vol.16 no.2 Ciudad de México ene./jun. 2024.

94. EBSCO Research starters home.

95. Blessing Guembe et al., The Emerging Threat of Ai-driven Cyber Attacks: A Review Applied Artificial Intelligence 2022, Vol. 36, No. 1.Taylor and Francis Group See also, The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Journal of Information Security.Vol.15 No.2, April 2024.


**How to cite this article:** EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035

96. DASLEGAL. The challenges of prosecuting and preventing a cyber crime https://www.daslegal.co.in/the-challenges-of-prosecuting-and-preventing-a-cyber-crime/.

97. Stockholm universitetJ. Palme and M. Berglund, Anonymity on the Internet.

98. Pala A and Zhuang J (2019) Information Sharing in Cybersecurity: A Review. Decision Analysis 16(3): 172-196.

99. Cybersecurity Dive What happens if threat data isn't shared?

100. United Nations Office on Drugs and Crime UNODC Civil Society Unit public-private sectors and global cooperation Cybersecurity Dive What happens if threat data isn't shared?

101. Frank Cremer et al (2022) Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract 47(3): 698-736.

102. Share of countries worldwide having active cybercrime legislation in place as of June 2024.

103. 120 Supra, n. 16

104. ISO/IEC 17025:2017https://www.iso.org/standard/66912.html.

105. Govind Bahadur Singh (2013) The SciTech Lawyer, Volume 9, Number 3, Also see Naeem Allah Rakha, Cybercrime and the Law: Addressing.

106. United Nations Office on Drugs and Crime (UNODC).Review. Proceedings of the 26th International Conference on Enterprise Information Systems (ICEIS 2024) 2: 240-246.

107. See generally, Sothy Chhy (2019) The impact of training and development on employee performance: a case study of selected private secondary schools in Phnom Penh Cambodia. Global Journal of Human Resource Management 7(3): 40-49.

108. Cybercrime investigator - Australian Federal Police.

109. Cybercrime Investigator. https://www.sciencedirect.com/topics/computer-science/cybercrime-investigator. (Date of use 3 September 2025).

110. See generally, P. Pawar, Cybercrime in Cross-Border Jurisdictions: Challenges and Solutions. Journal of Legal Research and Analysis. 1 (1). 2024. See also Y. Razmetaeva, H. Ponomarova and I. Bylya-Sabadash, Jurisdictional issues in the digital age. Revista de Derecho. Vol. 10 (I) (2021), pp. 167-183.

111. https://leppardlaw.com/federal/computer-crimes/examining-jurisdictional-challenges-in-cyber-threat- investigations-in-the-us/. (Date of use 6 September 2025). See also V. Manav, Jurisdictional challenges in cybercrime prosecution. Indian JLLR Volume VII Issue II

112. Available at https://www.google.com/search?q=ISO%-2FIEC+27001%3A2022&oq=ISO%.

113. Helping organizations to better understand and improve their management of cybersecurity risk.

114. Mahmood S, Chadhar M, Firmin S (2024) Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective. Applied Sciences. 14(24).

115. In the Law of Torts, restitutio in integrum, a Latin expression, means the compensation paid to the injured party as a result of the harm inflicted by the tortfeasor, principally, the compensation is to restore the victim to his earlier position or situation, had it been the inflicted injury had not happened.

116. Available at https://history.state.gov/milestones/1784-1800/jay-treaty. (Date of use 30 September 2025).

117. https://www.britannica.com/topic/list-of-notable-computer-viruses-and-malware. (Date of use 10 October 2025).

118. Budapest Convention on Cybercrime - Treaty 185 States Assembly. https://statesassembly.je › getmedia ›

119. Basic facts about global cybercrime treaty.

120. Cybersecurity for Small Business https://www.sbir.gov/tutorials/cyber-security/tutorial-1#. (Date of use 2 September 2025).

121. Available at https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e.

122. https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf.

123. United Nations convention against cybercrime 2024 https://docs.un.org/en/A/AC.291/L.15.

124. https://cyesec.com/blog/hidden-costs-cyberattack-impact-reputation.

125. UNDP Human Development Index.


DOI: 10.19080/JFSCI.2026.20.556035




**How to cite this article:** EFG Ajayi. The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes. J Forensic Sci & Criminal Inves. 2026; 20(2): 556035. DOI: 10.19080/JFSCI.2026.20.556035