Humanities and Social Sciences
2019; 7(4): 132-140
http://www.sciencepublishinggroup.com/j/hss
doi: 10.11648/j.hss.20190704.13
ISSN: 2330-8176 (Print); ISSN: 2330-8184 (Online)

Policy to Prevent and Combat Cyber-crime in Africa

Izabela Oleksiewicz

Department of Security Science, Rzeszow University of Technology, Rzeszów, Poland

Email address:
oleiza@prz.edu.pl

To cite this article:
Izabela Oleksiewicz. Policy to Prevent and Combat Cyber-crime in Africa. *Humanities and Social Sciences.* Vol. 7, No. 4, 2019, pp. 132-140. doi: 10.11648/j.hss.20190704.13

Received: July 8, 2019; **Accepted**: August 6, 2019; **Published**: August 23, 2019

Abstract: The global nature of the Internet has enabled extremely fast communication and transfer of most forms of human activity to the network, including those negatively received. Cyberspace is increasingly being spoken of as a new social space in which the same problems are reflected in the real world. Cybercrime is therefore a modern form of crime, exploiting the possibilities of digital techniques and the environment of computer networks. The research subject of this article is the policy of combating and preventing the phenomenon of cybercrime, while the research subject is Africa. At the beginning, the following research hypotheses were adopted: the slow pace of economic development of African countries is conditioned by the lack of appropriate legal regulations in the field of policy against cybercrime. This favors the development of economic cybercrime, which in turn testifies to the lack of measurement and control tools to limit and counter the very phenomenon of cybercrime in this area. Secondly, more importantly, the slow pace of ratification of international agreements also indicates that it will probably take longer than originally assumed that appropriate instruments of public international law could be legally binding within the African Union. Thirdly, the assumption was made that Africa is a potential for future economic development. In turn, the increase in the absorption and use of the Internet will contribute to its economic growth over time, which will continue to lead to the growth of cybercrime. The author, within the framework of this, publication, tries to show institutional and legal deficiencies on selected examples and indicate scenarios for preventing this phenomenon.

Keywords: Cyber-Terrorism, Policy, Prevent, Cyber-Security, Africa

1. Essence and Scope of Cyber-Terrorism Phenomenon as a 21st Century Challenge

The notion of cyber-terrorism is becoming an increasingly more popular topic in the literature of the subject, even though it is not yet defined from the normative point of view. On the other hand, cyber-crime is described as a subcategory of computer-crime including any kind of crime that is committed with the use of the Internet or other computer network. However, computers and computer networks may contribute to crime commitment in a variety of ways, such as: a crime instrument, a crime objective or as support in performing additional tasks (e.g. storing data that results from crime)[1]. The phenomenon refers to any kind of offence against connected computer systems aiming to disable either their proper functioning or operations of the data stored on a single PC (or several PCs connected in a common network). The most characteristic feature of cyber-crime is that particular attacks are performed by means of a computer connected to the Internet or internal Intranet networks [2].

Cyber-crime is referred to as such a form of using telecommunication systems, computer network or Intranet that aims to violate any right secured by law [3]. What makes it different and distinct from classical type of crime is its direct relation to a computer technology environment and using computer networks to commit such crimes [4]. However, it is not determined by preservation of a common good [5]. Nowadays, almost each and every illegal activity can be traced in the Internet. Global character of the Internet enables extremely swift communication as well as convenient transfer of most human activities into the global network, including those that hold negative connotations. Cyberspace is more and more commonly referred to as a new social space reflecting similar issues to those real ones. Thus, cyber-crime is regarded a modern form of crime benefiting from digital techniques and the environment of computer

networks. Cyber-crime is a relatively recent phenomenon that is spreading dynamically in societies that are highly computerised and operating in strong networks. It is considered as a major threat, extremely hard to combat. It is due to particular features that the phenomenon holds. First of all, it is a fact that the cyber-criminal activity easily overcomes barriers, such as country borders. Even though cyber-criminals pursue their actions in one place, the consequences are often revealed in other destinations, sometimes as distant as hundreds of kilometres away, in different countries or even continents. This prevents identification of a legal system that should be in force during such crimes' prosecution. Simultaneously, it makes it harder to appoint entities responsible for undertaking protective and prevention measures. Another key feature is the anonymity - it certainly does not support swift identification of the offenders or their behavioural patterns. It is extremely difficult and requires arduous investigation, as well as implementation of well-considered and planned actions. Convenience and time-efficiency which characterise modern computer and network techniques contribute significantly to dramatic boost in this type of crime in developed countries [6].

All of the above aspects make the protection against the threats of cyber-crime fairly difficult and require undertaking numerous actions including multi-layered and wide range of international cooperation. In order to ensure effective protection a cooperation of particular countries is regarded essential, as it comes to a common policy to combat cyber-crime, then the policy specification should be made by listing key priorities and unified principles of common actions. These overall principles need to be incorporated into national laws of the countries and become legal basis for institutional and functional set of instruments used to fight the crime. Development of successful system of combating cyber-crime is not simple, it requires an in-depth enquiry in the phenomenon in a long-time perspective, and it shall be clear that in the course of creating such a system a number of issues regarding adaptation of domestic law to the European or international laws may occur.

Cyberspace enters into relations with cyber-objects since it allows the transfer of information from one destination to another, due to appropriate software and wire connection resulting in the occurrence of cyber-objects on computer displays. While demanding the access to a particular cyber-object, e.g. www website, it is searched in its storage, sent via the cyberspace, re-identified by the addressee's search engine and displayed on the screen according to the author's preferences. Thus, the cyberspace comprises deconstruction and reconstruction of cyber-objects proving that it holds the features of both absolute space and the real one [7].

In the expert literature apart from the notion of a cyber-crime other terms can be found, such as: "computer crime", "computer-related crime", "internet crime". The notions, even though often used interchangeably, have not been defined since there is no general consent regarding their in-depth meaning. A. Adamski [8] argues that the notion of a computer crime can be discussed from both substantive or procedural point of view. From the perspective of substantive criminal law two types of computer crime can be distinguished. The first group encompasses all offences regarding systems, data processed and stored in the systems or computer software. Systems or computer networks serve as subjects or environment for the offence. On the other hand, the second group includes crimes committed with the use of computers with the aim to violate rights traditionally secured by criminal law.

Cyber-aggressive countries perform organised infowar and cyber-espionage. The evaluation of the cyber-threat analysis led by experts in the field clearly shows that countries, such as China, Russia, the USA, Iran and the Northern Korea are the most cyber-aggressive. According to the experts China systematically improves network techniques of cyber-fight eclipsing the United States of America slowly in this aspect. Chinese army forms hacker units, where the most brilliant computer experts are employed. WikiLeaks messages concerning American diplomats in Beijing reveal that Chinese cyber-attacks are politically motivated. The disclosed reports say the following "the embassy found out that the action was coordinated by the Chinese State Council Information Office, the main executive body in charge of the media and the Internet"[9]. Simultaneously, China admits being the subject of numeours cyber-attacks, which results in over a billion of Chinese accounts becoming controlled by foreign entities.

Table 1. *Fundamental typology of cyber-threats.*

Phenomenon	Characteristics
Cyber-violation	Using the cyberspace to force accepting unwilling messages containing information (such as e.g. data, images or text) against the addressee's values.
Cyber-crime	Using the cyberspace to commit common crimes targeted to individuals or organisations (institutions).
Cyber-targeting	Using the cyberspace to supervise or gain information on behaviour of individual residents (communities or whole nations), so called "Big Brother" effect.
Cyber-terrorism	Using the cyberspace to lead terrorist attacks (both national and international).
Cyber-autocracy	Using the cyberspace in reference to country's political affairs against the rules of liberal democracy (it contradicts cyber-democracy).
Cyber-war	Using the cyberspace to fulfil political tasks performed by the armed forces (so called cyber-warriors) targeted to resources and structure of the opposing country (also in reference to events other than wars).

Source: M. Górka (ed.), Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa XXI wieku, Warszawa 2014, p. 71.

The period of 2016 and 2017 was regarded a key turning point in the cyber-attacks, when Ransomware was used [10]. It served as the opening of a new stage in the field of cyber-crimes. As the example may serve the case of Mirai; on October 21, 2016 DDoS's (DNS system) attack was noted, which directly made some of the DNS-based services unavailable in the United States. This happened in the case of PayPal, Twitter, Netflix, Spotify or Play Station internet services. Devices previously unsecured or not supported by antivirus software became infected on a large scale. Then, they searched for similar files in order to pass on the infection. The set of infected zombie-devices was formed by means of malicious software called Mirai (meaning "future" in Japanese) gradually spreading and pending further instructions. Finally, the Dyn provider restored its functionality but the impressive scale of the Mirai offence encouraged proper reflection on the issues of security in the field of "smart" devices.

WannaCry is another example, a real plague indeed, since 150 countries worldwide experienced its harmful hacker attacks. The latter ones targeted hospitals, telecommunications enterprises or banks and used a device earlier stolen from one of the American credit information agencies. The hackers claimed ransom in return for unblocking computers. The attacks' consequences included British hospitals being forced to dismiss their patients. The cyber-attack was defined as "unprecedented" by the Europol and international investigation was initiated to track down the violators [11]. The hackers clearly took advantage of the Microsoft system security flaw identified and described by the NSA, an American intelligence agency in charge of electronic intelligence among others. Even though the Microsoft security loophole was generally known not only to the NSA, business corporations unfortunately did not get informed about the threat. What is more, methods of using the loophole were stolen from the NSA by a group called Shadow Brokers and published on-line.

As far as the cyberspace is concerned, Russia is mainly interested in selected aspects of information warfare, which actually happened in the case of Estonia (2007) [12], Georgia (2008) and the United States (in 2016 during the presidential campaigns of Hilary Clinton and Donald Trump, when the election result could have been manipulated). How significant the protection is for Russia in reference to cyber-threats may explain the fact that the Russian Federation's law allows nuclear retaliation or information warfare in response to potential enemy [13]. According to Russians: „Information warfare is understood as a battle between countries in the information space intended to cause damage to information systems, their data or resource processing, structures of fundamental significance or other, destabilise political, economic or social systems as well as to enforce a particular country to undertake actions in favour of its opponent" [14]. Some countries, especially such cyber-powers as Russia, China or the USA, recognised the outstanding potential of cyberspace. It is becoming more often explored with the intention to perform the state's policy, propaganda, surveillance or military actions. It seems very likely that in the future cyberspace will be used even more often and willingly, bearing in mind potential benefits (such as, among others, gaining critical information, confidential data, misinforming and paralysing activity of opponents). The main addressee of cyberspace attacks, including those with cyber-terrorist features, is definitely regarded the United States of America. Vast majority of the attacks is performed by China and the attacks target government and military units as well as business enterprises.

2. Conditions of Policy to Combat Cyber-Crime in Africa

The survey held by the International Data Group Connect [15] revealed that each and every year cyber-crime generated costs of 573 million $ in the South Africa. In the case of Nigeria and Kenya the costs ran at the level of 500 million $ and 36 million $, respectively. The amounts are quite considerable from the point of view of medium size countries.

Another survey held by Deloitte in 2011 indicated that financial institutions in Kenya, Rwanda, Uganda, Tanzania or Zambia generated losses equal to 245 million $ that were related to cyberspace security. Last but not least, a few Zambian commercial banks were defrauded for the total amount of over 4 million $ in the first half of 2013; it resulted from a complex cyber-crime system with the active part taken by both Zambian and foreign citizens.

In the Francophone Africa the phenomenon occurs mainly in regional economies and for instance in 2013 the estimated cost of cyber-crime on the Ivory Coast ran at 26 billion CFA (3,8 million Euro), whereas in Senegal the cost equalled 15 billion CFA (22 million Euro).

During the international forum on cyber-security held in 2016 in Dakar, Charles Kouamé, official responsible for telecommunications management on the Ivory Coast, indicated that the Ivorians lodged 1429 complaints in the courts. In his opinion a global number of cyber-frauds in the African countries noted decreasing trend from 5.8 billion CFA (8.9 million Euro) in 2014 to 4 billion CFA (6.1 billion Euro) in 2015.

The above numbers prove the significance of the problem in this part of the world, where nowadays a dynamic growth is observed as stimulated by the growth in the prices of raw materials, technological boom and increase in the middle class income. Even though vast majority of the society cannot afford a basic computer set (consisting of a PC, a printer, a router, etc.) it is possible to gain the access to the Internet via smartphones and such equipment prices have fallen down significantly over past ten years.

This explains why only in 2013 in the very area of the Sub-Saharan Africa around 311 million of mobile phone users were identified (penetration index 36%). It is estimated

that the numbers will grow to 504 million users in 2020 (penetration index 49%) [16].

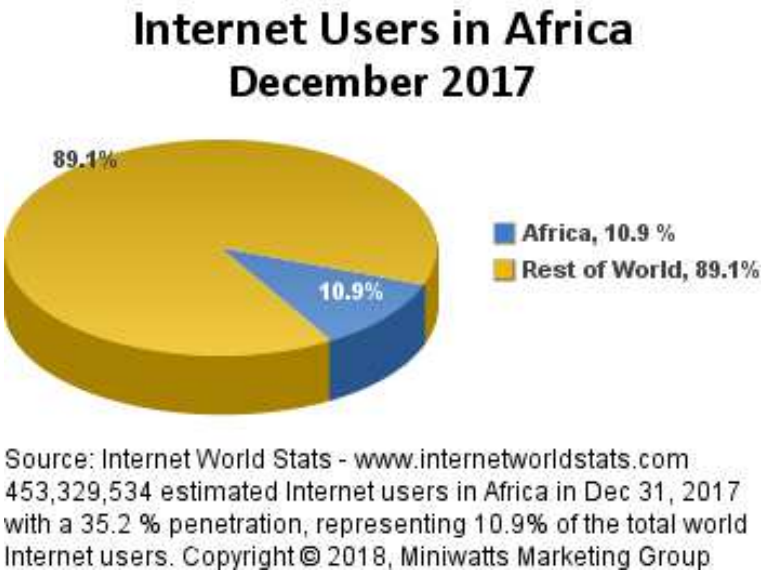


Figure 1. *Number of Internet users in Africa as on December 31, 2017.*

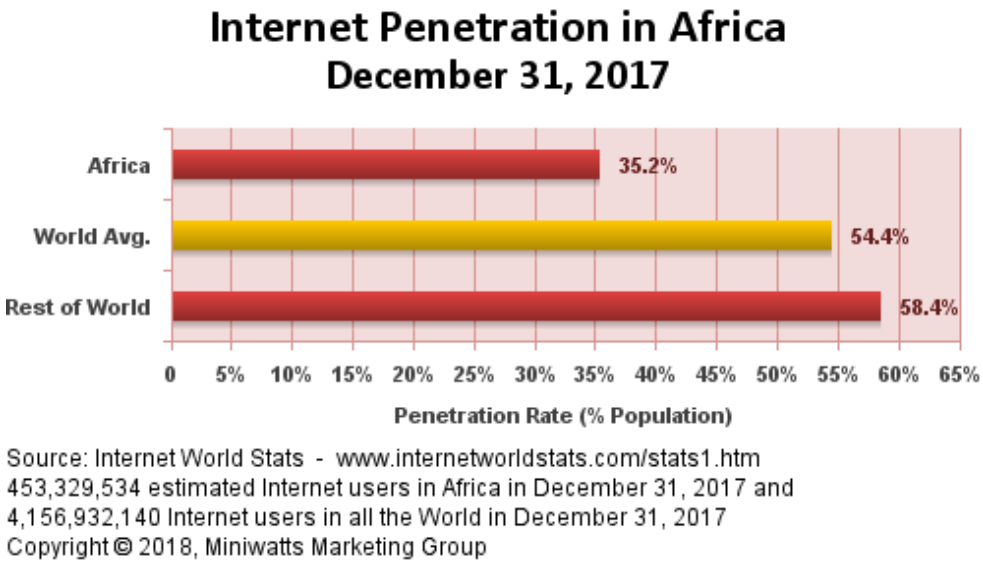


Figure 2. *Number of mobile device users in Africa as on December 31, 2017.*

International Telecommunications Union (ITU) estimates that every fifth African citizen uses the Internet. However, simultaneously a high level of computer piracy is observed. Since there is an obvious and strong relation between computer piracy and cyber-crime still the most popular method applied by cyber-criminals is using infected devices that are supported by counterfeit software.

What is more, another the research of 2013 held by International Data Corporation (IDC) showed that 33% of worldwide software was counterfeit and the phenomenon in a global scale cost approximately 114 billion $.

In Africa there are twelve countries with the most infected IT infrastructure, namely: Libya (98%), Zimbabwe (92%), Algeria (84%), Cameroon (83%), Nigeria (82%), the Ivory Coast (81%), Kenya (78%), Senegal (78%), Tunisia (74%), Morocco (66%) and Mauritius (57%). Earlier research was held by BSA in 2011 and confirmed that the counterfeit software share in Africa and Middle East was as high as 58%. The share of the counterfeit software on the very Kenyan market is evaluated 78% with the value of 12 billion Kenyan Shilling (approx. 120 million $).

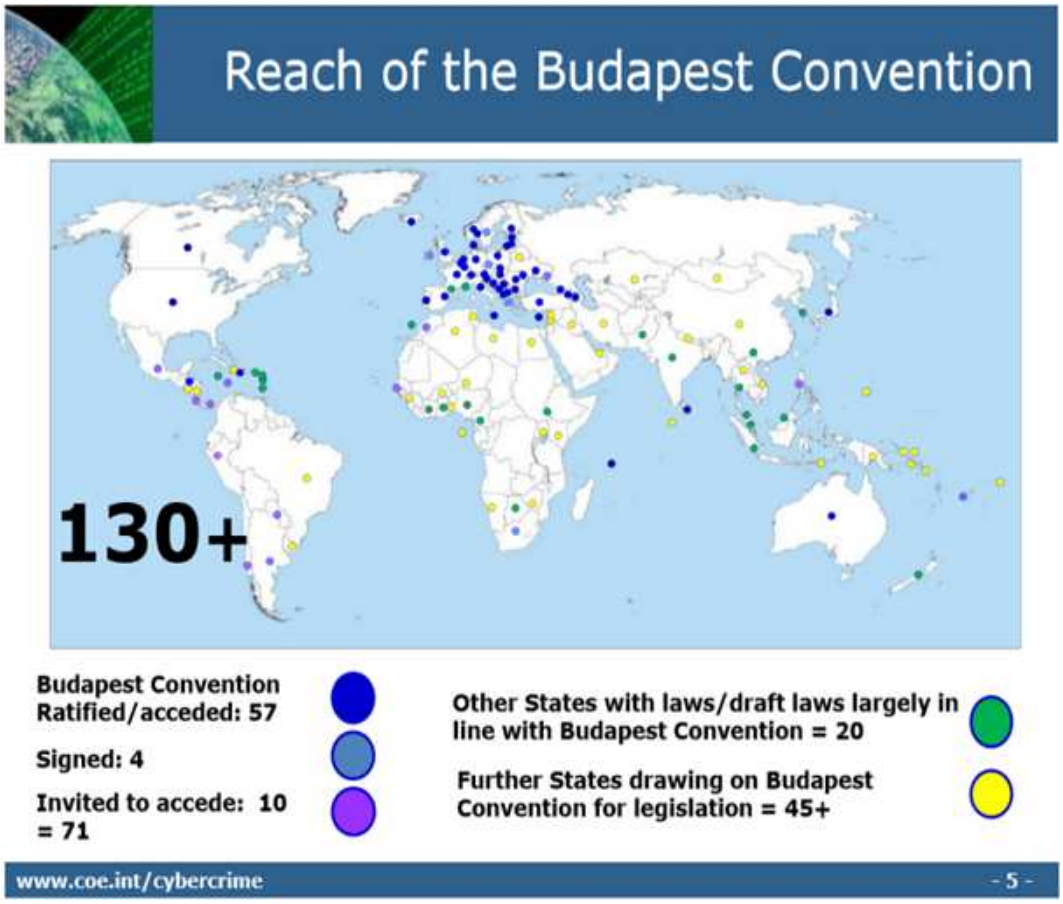
3. Legal Framework for Legislation and Cyber-Crime in Africa

With respect to the African continent there is less data available which, to certain extent, explains the lack of instruments to measure or supervise the cyber-crime in the

area under consideration in this article. The state of the art of cyber-crime legislation in Africa is currently evaluated within the project of the European Council entitled Cybercrime @ Octopus1 [17].

Brief revision of fifty five African countries focusing on selected aspects of criminal law on cyber-crime and on-line crime evidence suggests that since April 2018 eleven countries, such as Botswana, Cameroon, the Ivory Coast, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia, have got fundamental substantive and procedural law at their disposal. Twelve countries - Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, the South Africa, Sudan, Tunisia i Zimbabwe - seem to possess incomplete law. However, the majority of African countries do not work with specific provisions concerning cyber-crime and on-line crime evidence. Bearing in mind that only 20% of African countries possess fundamental law in the area of cyber-crime and on-line crime evidence, the status quo cannot be treated as satisfactory. Many countries are currently working to introduce essential amendments, unfortunately often with little progress.

In relation to the issue of cyber-crime, a number of African countries are adapting data protection regulations. This allows additional protection with respect to individual's rights. Mauritius, Morocco i Senegal not only act as parties or were invited to join the Council of Europe Convention on cyber-crime but also themselves requested to join the Council of Europe Convention no 108 on the protection of personal data [18]. The Africa Union (AU) Convention on cyber-security and the protection of personal data of 2014 [19] also addresses the issue of personal data protection in one of the chapters.



Source: Analysis of the Council of Europe, Report of March, 2018 retrieved from: http://coe.int/cybercrime, p. 5.

Figure 3. *World map showing geographical range of the Council of Europe Convention on cyber-crime.*

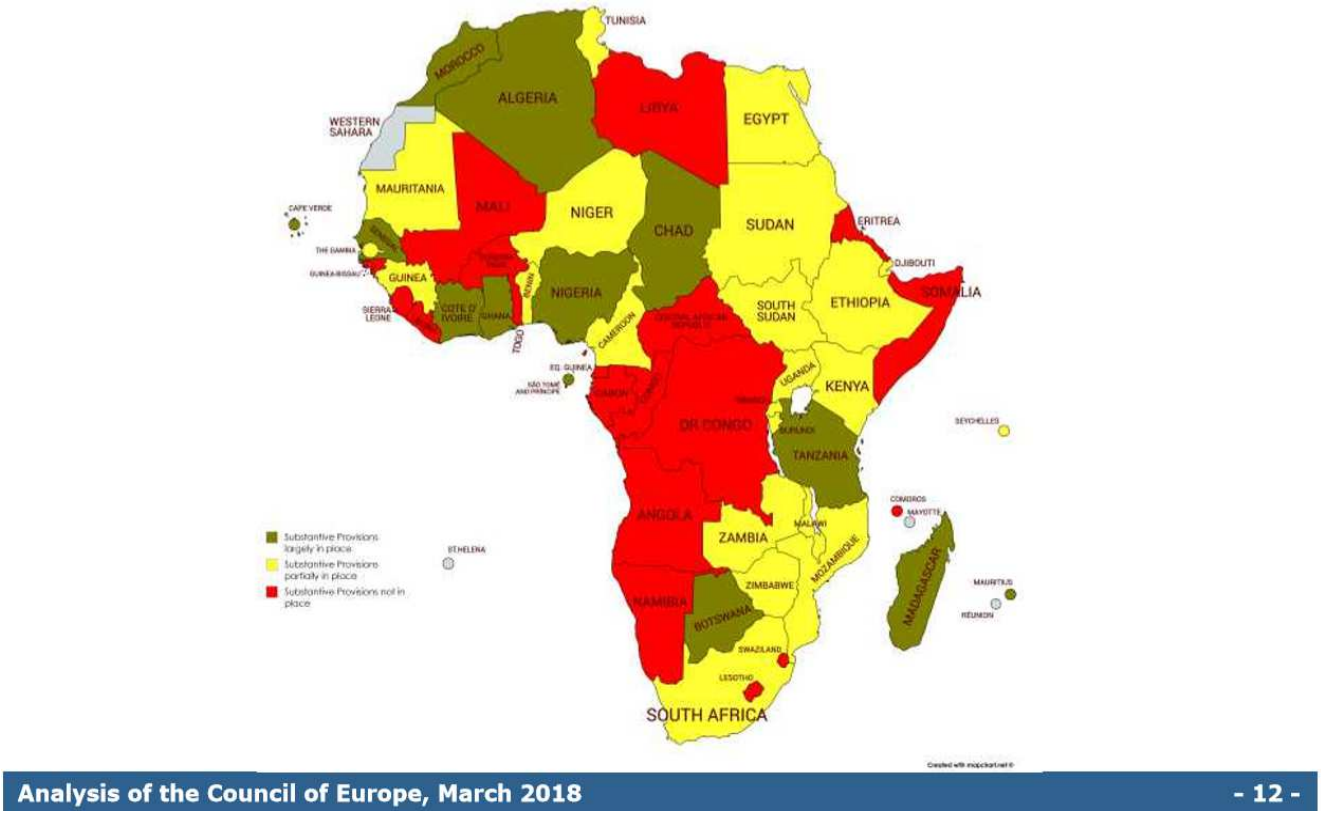
The Council of Europe Convention on cyber-crime (so called "Budapest Convention") is regarded one of the most significant acts dealing with the problem of combating cyber-crime [20]. Addressing the issue on the global scale was justified by the necessity to develop a decisive measure aimed to unify rules of fighting and prosecuting cyber-criminals, as well as to develop extradition procedures for the countries of both liberal and restrictive policy.

According to the Article 10 of the Convention the Member States should consider crime acts that unlawfully and intentionally contribute to full or partial gaining access to an IT system, intercepting non-public transmission of IT data by technical means, destroying, removing, causing damage, altering data which results in serious interference with the integrity of IT systems, using devices, sharing security codes, software or other kind of information that leads to aforementioned offences (so called: misuses) [21].

IT fraud or forgery, offences related to child pornography,

infringements of copyright and related rights can also be classified as a crime. Criminal liability is envisaged for crime attempting, inciting and acting. Finally, criminal liability is also defined for legal entities prosecuted for the above offences.

The Convention Additional Protocol on cyber-crime of 2003, Article 22, extended the scope of criminalisation to on-line racism and xenophobia. It provided definitions for racist and xenophobic acts in cyberspace, called for countries to criminalise them and extended the Convention's scope to these acts (the Articles 3-6 of the Protocol).



Source: Analysis of the Council of Europe, Report of March, 2018 retrieved from: http://coe.int/cybercrime, p. 12.

Figure 4. *Current status of legislation on cyber-crime in Africa as of March 2018.*

The Convention does not specify precisely criminal measures and penalties to be applied for crimes defined in the document. It only imposes obligation on the countries to guarantee effective, proportionate and dissuasive sanctions, and for legal entities - also imprisonment and pecuniary sanctions (the Article 12 of the Convention).

According to the Article 16 of the Convention, its parties were obliged to take legislative measures enabling to order or gain immediate protection of IT data, including traffic data - especially in case of data loss or alteration risk. The legislative measures are also bound to include powers to freeze and seize IT systems or its parts, create and save copies of obtained data, hide the data from public or remove from the system. Authorities should also be entitled to expand the investigation to other systems on condition there exists justified risk of the searched data being moved to other IT system, than previously assumed [22].

What is more, the Convention imposes obligation on the parties to designate a contact point available 24/7 in order to enable immediate international assistance during IT system/data crime investigations or proceedings. Establishing the network of contact points aims to provide mutual technical assistance, immediate protection or revealing IT data stored on the territory of another country, to enable easier and faster evidence collection, information providing or suspect locating (the Article 35 of the Convention).

The Convention on cyber-crime is the most important but not only one piece of legislation developed by the Council of Europe and referring to combating cyberspace threats. One of the serious threats related to the convenience of communication via the Internet and other computer networks is the opportunity to spread information forbidden by law. Thus, the Convention on the protection of children against sexual exploitation and sexual abuse [23]. Its fundamental aim is to establish a special monitoring system based on both national and international cooperation that could help to prevent and fight sexual abuse of children. The Convention serves as the legal basis for protecting the rights of children - victims of sexual offences [24].

Soaring numbers of sexual abuse and mistreatment of children in sexual context, especially if IT or communication

technologies are involved, led to the introduction of proper regulations included in the Convention. In accordance with the Article 4 of the Convention each party is obliged to undertake some measures to prevent any kind of sexual exploitation and mistreatment of children in sexual context, and to protect children. Various types of offences were listed in the Articles 18-22 of the Convention. However, in the Article 20 there is a provision included stating that the parties should take some action to penalise crimes related to child pornography, including production, offering for sale and sharing, distributing or sending, obtaining, possessing child pornography but also conscious gaining access to child pornography by means of IT and communication technologies.

In terms of the scope of the Convention, it is broader than the Council of Europe Convention due to the following included:

a) Chapter I - electronic transactions,
b) Chapter II - personal data protection,
c) Chapter III - cyber-protection and cyber-crime,
d) Chapter IV- final provisions.

According to the Article 36, in order for the Convention to enter into force, its ratification by fifteen African Union (AU) Member States is required. The UA report of February 2019 eleven Member States signed the Convention, namely Benin, Chad, Comoros, Congo, Ghana, Guinea Bissau, Mauritania, Namibia, Sierra Leone, St. Thomas and Duke Islands, and Zambia, whereas only four of them: Guinea, Mauritius, Namibia and Senegal ratified the Convention [25].

The AU Convention combines various aspects of IT law, including selected issues concerned with digital dimension and clear criminal record. It is worth at this point to draw the attention to regulations included in the Articles 2, 3 and 7 of the Convention referring to e-commerce, where the Member States allow e-commerce being performed freely in all of the Member States - except for:

a) gambling, even if performed in the form of legally authorised lotteries or betting,
b) legal representation and charitable activities,
c) activities of notaries or held by equivalent bodies, according to proper legal acts.

E-commerce business is governed by the law of the Member State in which the business is registered, unless the transaction parties agree on other terms. Electronic transaction protection is guaranteed with a written agreement prepared in an electronic format. On the other hand, in accordance with the Article 8(1) of the Convention the parties are obliged to specify legal framework aiming to enhance fundamental rights, as well as public freedoms in terms of personal data protection. This kind of mechanism is to ensure that each form of data processing secures fundamental freedoms and rights of an individual while preserving the country of running the business' prerogatives.

Pursuant to the Articles 24 and 25(2) of the AU Convention parties were obliged to adopt appropriate national strategies on combating cyber-terrorism and establish institutions in charge. What is more, according to the Article 27(1), which serves as the extension of the Article 25(2) of the Convention, the Member States are required to adopt essential measures to create a proper institutional mechanism of cyber-security management. The provision's execution will not become fully effective unless the lawmakers ensure three fundamental elements, such as: strategy, institutions (organs) in charge and necessary legal instruments. Without the above elements it is difficult to speak about the effectiveness of the provisions. Although the very provisions are perfectly correct, up to this day they remain defunct in terms of national and international law.

The Article 26 of the Convention imposes obligation on the Member States to internally promote cyber-security culture by raising social awareness and providing education on cyber-security. From this perspective, the Member States are liable to support IT network and system's development, as well as the adoption of new patterns of reasoning and behaviour during the use of IT systems.

In the AU Convention pursuant to the Article 28(1) detailed provisions are included concerning international cooperation in order to ensure that the measures adopted to fight cyber-crime will enhance regional harmonisation and respect the principle of double criminality. The Article 28(2) of the Convention also states that the Member States having signed no mutual support agreements on cyber-crime are obliged to establish agreements on mutual legal support according to the double criminality principle while simultaneously sharing information and data. This implies that the countries without mutual legal support agreement on cyber-crime must get involved in such agreements based on the double criminality principle. However, one needs to remember that the legislation does not serve as legal basis for cooperation between the countries in terms of electronic evidence.

In order to allow effective implementation of national structures of cyber-security the Convention forces the Member States to take necessary measures to limit the access to secured systems classified as the national critical defence infrastructure based on critical national security data, according to the Article 30(1)(d). In spite of that, the Convention does not provide a definition for the notion of "national critical defence infrastructure".

A significant provision is regarded the Article 32 of the AU Convention on cyber-security, which states the establishment of monitoring and operational mechanism in order to implement the Convention. Regional mechanism aimed to monitor the Convention has not been formally adopted, yet. The above mandates under the Article 32 of the Convention may be interpreted very broadly in order to set up a regional agency similar to the the European Network and Information Security Agency (ENISA).

4. Conclusions

The excessively slow pace of the Member States aimed at signing and ratifying the Convention leads to delays in

achieving its objectives, such as provision harmonisation on cyber-security in the Member States. What is even more important is that the slow dynamics of ratification suggests it may take longer that previously assumed for the fifteen countries to ratify in order for the Convention to enter its force within the framework of the AU.

On the other hand, the rise in absorption as well as use of the Internet will lead in the future to economic growth. This, in turns, will contribute to the boost in cyber-crime. Thus, in order to prevent it, certain institutional and legal framework must be introduced in Africa on the international level.

The Member States will need to bring forward changes by:

a) establishing proper state institutions in the area of cyber-security and information,
b) launching well-organised teams aimed at responding to computer incidents (CERT, Computer Emergency Response Team),
c) adopting national strategies on cyber-security and information as well as national cooperation plans concerning cyber-security and information.

Last but not least, every effort must be made to support coordination and cooperation between the government (Cyber-security Advisor Council), private sphere and citizens.

References

[1] Littlejohn Shinder D., Tittel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2004, p. 25.

[2] Skowera D., *Akademia Cyberpolicyjna – Policja i organizacje międzynarodowe wobec wyzwań przestępczości internetowej*, „Zarządzanie publiczne" Zeszyty Naukowe ISP UJ 2006, no 2, p. 142. Compare: Depa M., Pomykała M., *Instytucjonalne aspekty przeciwdziałania cyberprzestępczości*, [in:] Oleksiewicz I., Polinceusz M., Pomykała M. (ed.), Nowoczesne technologie - źródło zagrożeń i narzędzie ochrony bezpieczeństwa, Rzeszów 2014, p. 8.

[3] See: Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa 2011, p. 63; Gniadek A., *Cyberprzestępczość i cyberterroryzm – zjawiska szczególnie niebezpieczne*, [in:] Jemioł T., Kisielnicki J., Rajchel K. (ed.), *Cyberterroryzm. Nowe wyzwania XXI wieku,* Warszawa 2009, p. 222.; Kosiński J., Waszczuk A., *Cyberterroryzm a cyberprzestępczość*, [in:], Bogdalski P., Nowakowski Z., Płusa T., Rajchel J., Rajchel K. (ed.), *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, Warszawa 2013, p 333.

[4] Siwicki M., *Cyberprzestępczość*, Warszawa 2013, p. 20.

[5] Siwicki M., *Cyberprzestępczość*, Warszawa 2013, p. 21.

[6] See more: Polinceusz M., Pomykała M., *Ochrona cyberbezpieczeństwa w Polsce. Kierunki zmian legislacyjnych na przestrzeni ostatnich lat*, [in:], Bogdalski P., Nowakowski Z., Płusa T., Rajchel J., Rajchel K. (ed.), *Współczesne zagrożenia ...,* op. cit., p. 660-661.

[7] W. Krztoń, *Walka o informacje w cyberprzestrzeni w XXI wieku*, Warszawa 2017, p. 145.

[8] Adamski A., *Cyberprzestepczość - aspekty prawne i kryminologiczne,* Studia Prawnicze Kwartalnik" 2005, no 4, p. 166.

[9] *Jak chińskie Politbiuro wojowało z Google.* Retrieved on July 15, 2017 from http://www.tvn24.pl/wiadomosci-ze-swiata,2/jak-chinskie-politbiuro-wojowalo-z-google,154681.html

[10] Ransomware, malware programmed to code data and block the access to its content. All computers have been infected in a similar manner and the displays showed the message forcing ransom in Bitcoin currency in return for unblocking the access.

[11] Approximately 200 hacker attacks were believed to be pursued within four days. This cyber-attack contributed to losses estimated as high as 8 billion $. For more see also: Carson J., *What is fake news? Its origins and how it grew in 2016*, Retrieved on May 12, 2018 from: https://grassrootjournalist.org/2017/06/17/what-is-fake-news-its-origins-and-how-it-grew-in-2016/.

[12] Crandall M., *Soft security threats and small states: the case of Estonia*, Defence studies", 2014, vol. 14/1.

[13] Harrel Y., *Rosyjska cyberstrategia*, Warszawa 2015, p. 206–208.

[14] Harrel Y., *Rosyjska cyberstrategia*, Warszawa 2015 p. 201.

[15] For more see: https://www.idgconnect.com/type/analysis-review/regions/africa (Retrieved on March 15, 2019).

[16] Compare: *Cybersecurity as an Economic Enabler*, position paper. Retrieved on April 19, 2019 from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler

[17] Retrieved on March 15, 2019 from: https://www.coe.int/en/web/cybercrime/cybercrime-octopus.

[18] Dz. U. 2003 no 3 item 25.

[19] Government Gazette Staatskoerant, Republic of South Africa, Vol. 536, 19th February 2010, Pretori, No. 3296319.

[20] Budapest, November 23, 2001, CETS no 185. The Convention was first developed at the end of the 90s of the 20th century and was open for ratification on November 23, 2001 in Budapest. Poland has just ratified the Convention.

[21] Aleksandrowicz T. R., Liedel K., *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia*, [in:] Liedel K., Piasecka P., Aleksandrowicz T. R. (ed.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa 2014. Compare with the case of Ireland vs. Great Britain, January 18, 1978; the case of Soering vs. Great Britain, July 7, 1989, November 15, 1966; the case of Aksoy vs. Turkey, December 18, 1966; the case of Tomasi vs. France, August 27, 1992.

[22] Balocco R., Ciappini A., Rangone A., *ICT Governance: A Reference Framework*, Information Systems Management" 2013, vol. 30/2, Carrapico H., A. Barrinha, *The EU as coherent (cyber) security actor?* Journal of Common Market Studies" 2017, vol. 55/6.

[23] Lanzarote, October 25, 2007, CETS no 201. Poland signed the Convention on October 25, 2007 but did not ratify it.

[24] Compare: M. Grobler, J. Jansen van Vuuren, L. Leenen, *Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward.* Retrieved on March 15, 2019 from https://hal.inria.fr/hal-01525124/document.

[25] Retrieved on March 16, 2019 from: https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_2.pdf.