УДК 323.28(6)

THE PROBLEMS OF INFORMATIONAL TERRORISM IN AFRICAN COUNTRIES

Vozniuk E.V.

The features of informational terrorism in African countries, especially in SADC countries, are analyzed as well as the ways to combat information terrorism in this region. The major issues related to information terrorism are highlighted, which include data exfiltration, social engineering, insider threats, database breaches as well as poor identity and access management. The essence of Computer Security (Cyber Security) is revealed and its main tasks are characterized: accessibility, integrity, including authenticity and confidentiality. The main threats for cyberspace are distinguished.

Keywords: informational terrorism, African countries, SADC, international security, cyber security.

ПРОБЛЕМА ИНФОРМАЦИОННОГО ТЕРРОРИЗМА В АФРИКАНСКИХ СТРАНАХ

Вознюк Е.В.

В статье проанализированы особенности информационного терроризма в африканских странах, особенно в странах САДК, а также исследованы пути борьбы с информационным терроризмом в регионе. Выделены основные вопросы, связанные с информационным терроризмом, включающие эксфильтрацию данных, социальную инженерию, инсайдерскую угрозу, нарушение базы данных, а также плохую идентичность и управления доступом. Раскрыта суть понятия компьютерной безопасности (кибербезопасность) и охарактеризованы основные ее задачи: доступность, целостность, включая аутентичность и конфиденциальность. Определены основные угрозы для киберпространства.

Ключевые слова: информационный терроризм, африканские страны, САДК, международная безопасность, кибербезопасность.

Nowadays informational terrorism is a general threat not only to a specific region, but also to the whole world. Many highly developed states counteract this threat to national security in different ways, but everyone has one goal to unite and reduce the impact of cyber terrorism and the number of cyber attacks. Speaking of the various geopolitical regions of the world, and also the impact of all kinds of terrorism, namely informational, we cannot ignore them in rapidly developing African countries which reach a rather new level of economic development and political influence, therefore, the primary task for them is to secure from negative informational influences and from hacker penetration into the database of enterprises and state structures.

The aim of the work is to analyse the features of informational terrorism in African countries, especially in SADC countries and to explore ways to combat information terrorism in this region.

The term "information policy" has been used to refer to policy initiatives that promote the use of tools and concepts associated with the "global information society", with a view to realizing their potential in achieving national, social and economic development goals [2, p. 2-4].

Three hierarchical levels for information policy used in African countries:

Infrastructural Policies. Apply across society and affect the information sector both directly and indirectly. Infrastructural Policies would deal with the development of national (or more recently also regional) infrastructures required to support an information society. The absence of infrastructural policies and implementation strategies would make it virtually impossible to deliver on any other vertical or horizontal ICT-related policies'. Policy development in Southern Africa' reflects this reality in that generally telecommunications policies are the first to be revised, followed by a focus on separate policies in areas such as education, e-Commerce, freedom of information, universal service, etc.

Vertical Information Policies. Apply to a specific part of the information sector for a particular application. Vertical Information Policies would include sectoral policies such as education, tourism, manufacturing, health, etc.

Horizontal Information Policies. Apply across society and affect the information sector both directly and indirectly. Horizontal Information Policies refers to those policies that impact on broad aspects of society, e.g. policies relating to freedom of information, tariffs and pricing, and the use of ICTs by government internally and in its relationships with citizens, business, labour, academia, etc. The need for integrating national ICT strategies' overlaps with four well-established policy fields: technology, industry, telecommunications and media [9, c. 113-114].

Information terrorism – is the use of information technologies, mass media, dissemination of information for the purpose of targeted influence on the selected object, its discredit [1, c. 128]. There is another widespread name of it – Cyber terrorism – the use of computer and telecommunication technologies (especially the Internet) for terrorist purposes. Legislation of Ukraine defines: "Cyber terrorism is a terrorist activity carried out in cyberspace or with its use". This is a killing attack aimed at intimidating in order to achieve political results or harming computer networks, especially personal computers connected to the Internet, using such means as computer viruses.

Cyber attack in its turn is an attempt to damage or disrupt a computer system, or obtain information stored on a computer system, by means of hacking [4].

That's why we have to mention Computer Security (Cyber Security), which is the set of tools, strategies, principles and guarantees of security, approaches to risk management; actions, training, insurance and technologies used to protect the cyber-environment, resources of organizations and users. The main tasks of security are: accessibility, integrity, including authenticity and confidentiality. Cybercrime is a prerequisite for the development of an information society [3].

According to Gady (2010) statistics presented at a Cybercrime conference in Cote D'Ivoire have shown that Africa has the fastest growing cases of informational terrorism more than any other continent. This is a worrying trend considering that it is also the fastest growing continent in terms of computer and mobile technology all of which are vulnerable to informational terrorism. This discussion shall tackle the

various aspects of informational terrorism in Southern African Development Community (SADC) and how it affects regional development [5].

Grobler and van Vuuren, (2012) have argued that cyberspace [Information terrorism] comprises complex and dynamic technological innovations to which no current legal system is well suited [6, p. 64]. Zimbabwe has come up with a full Ministry designed to fight information terrorism called the Ministry of Cyber Security Threat Detection and Mitigation designed to curb crimes related to cyber wars especially malicious activities circulated via social media platforms.

Although Lee acknowledges that African Governments have not shown their statements of intent in fighting cybercrimes, the SADC region has suffered patches of attacks ranging from government internet sites shut down to circulation of malicious social media content meant to cause damage or hamper government operations [8].

The growing access to internet connectivity in southern Africa is a factor which makes the threat of informational terrorism real as opposed to perceived. Kigen et.al. (2015) as cited in Oladipo, (2015) have indicated that "businesses are losing about $146 m (£96 m) every year to cyber-crime" and to have such huge losses is far much more than losses incurred from other conventional crimes [7]. In South Africa alone has witnessed more than 6000 cyber attacks in the month of October 2017 alone according to the Sunday Times newspaper which is an indication that something needs to be done to curb this worrisome trend.

The sad part of the story is that most African businesses large and small are too ill equipped to withstand the threat of cyber warfare especially if their account has been hacked. In southern Africa, South Africa is one of the biggest cyber hotspots due to its large population and advances in economic and technological development as well as the increasing capacity to host large data volumes.

Major Information terrorism issues in Southern Africa. The major issues related to information terrorism include data exfiltration, social engineering, insider threats, database breaches as well as poor identity and access management [7].

In Kenya alone according to Kapersky Lab experts, about 20% of computers being used in Kenya are vulnerable to malware which is a serious threat to doing

business in that country. This is due to the fact that many people are not computer literate and if they are they are at least to the level of being a user and not a programmer so most of the hacking and information terrorism will happen without their knowledge.

This is even applicable to many other SADC countries that happen to have fewer computer programmers than computer literate people. In another instance, the growing number of mobile users without the knowledge of how cellphone hacking takes place adds to the information terrorism problem.

According to Check Point Software technologies, 2015 statistical reports of cybercrimes, Tanzania – another SADC country was the highest attacked country in October of 2015 with Malawi (4), Namibia (5) and Mauritius (7) and South Africa (67) in their rankings of the most attacked countries in terms of information terrorism [7].

Now Data exfiltration refers to an action by criminals and trusted employees with access to large volumes of data to siphon that data out of the company without the knowledge of the management. This is done maliciously to use it against employees of the company or to gain access to sensitive information including passwords and account numbers so as to steal money under the guise of internet anonymity.

Social engineering is the use of social media to attack the reputation of a certain individual or company. For instance, companies with social media pages face the vulnerability of having their pages either hacked or people send information that is not appropriate for the clients. For instance, pornographic materials being posted on an social media account. This has also a potential to drive away customers.

A database breach occurs when the company cannot readily access information from their database due to it being breached. Normally hackers breach and change passwords as they access volumes of data. An instance is when the American FBI was hacked into and the video of the killing by gunfire from a helicopter by American troops was illegally released. Such breaches will often have grave

consequences as they expose sensitive information and secrets that are key to company.

Poor identity and access management can also lead to information terrorism as information that is not supposed to be in the terrorists hands ends up in their hands which will affect the company operations. An example is the sharing of access passwords with friends which will lead to information terrorism. This problem might be very difficult to do away with because it hangs parasitically on the technological developmental progress sweeping across Africa especially with the advent of fiber optic network.

The potential of new technologies, particularly information and communication technologies (ICTs), to support economic development is widely recognized. For example, there is an estimated 1.38% increase in gross domestic product (GDP) for every 10% increase in broadband penetration in low- and middle-income countries [6, p. 65-66]. If the information terrorism succeeds to penetrate in a country, it will likely affect the progress by reducing the potential for development.

While the potential use of ICTs for development, governance, and peace has posed questions about how to govern the Internet, issues related to security – and to Cyber Security in particular – have made these questions more urgent. As the barriers to entry in the cyber domain are low, cyberspace includes many and varied actors – from criminal hackers to terrorist networks to governments engaged in cyber espionage. Cybercrime and cyber attacks can undermine the safety of Internet users, disrupt economic and commercial activity, and threaten military effectiveness. Moreover, conflict that takes place in the cyber domain often mirrors conflict in the physical world.

The growing interest and contention around the so-called “duty to hack” also raises question related to international humanitarian law and security. International humanitarian law requires states to use the least harmful military means available for achieving their strategic objectives, which in the case of this theory could mean using cyber operations as the predominant least-harmful response. Such cyber operations

could help avoid physical attacks that risk causing greater damage and casualties. This theory thus assigns states the "duty" to invest in offensive hacking capacities.

At the conclusion of the 37th SADC summit in Pretoria which ran between 9 and 20 August 2017, the SADC secretariat was ordered to set up a department which deals with drug abuse as well as information terrorism otherwise better known as Cyber-crimes [8].

In 2014 a cartel of cyber criminals were discovered by mistake when a fire broke out in one of the compound where the cartels were staying. Now the fact that they were accidentally discovered speaks of many others who operate in Kenya and many other SADC countries away from the authorities and as a result the problem of information terrorism is only starting and might take ages before it finally comes to be eradicated if it shall ever be eradicated.

This means that the future of information terrorism shall see it rising beyond manageable levels by 2020 as technology to hack will be available even to ordinary citizens.

The other factor which might be the cause of the rise in information terrorism in SADC is because say for instance in Kenya alone, ITC contributed to 12.1% of the GDP in that country so that could be a target for hostile governments to attack this sector or malicious individuals with the intention of making money out of it [7]. The introduction of fibre optic has been the reason why information terrorism is on the rise in Africa. Countries which must boost their infrastructure include countries with more advanced economies like South Africa, Kenya and Tanzania within the SADC region.

Information terrorism is a rising global threat and even sophisticated economies like United States of America have shown that they can be vulnerable as was seen in the alleged hacking of the DNC servers as well as the elections by suspected Russian hackers. Africa is no exception and SADC in particular must be very vigilant in fighting this new world war whose perpetrators are unknown and often hide behind the veil of anonymity.

The following are some of the strategies that must be employed to curb information terrorism:

– Countries should be in a position to enact legislation that makes it a crime to engage in information terrorism acts. For instance, Zimbabwe is currently running a bill which is code named *The Cyber Crime and Cyber Security Bill* which will be tabled soon in parliament for deliberations which has specific provisions that makes it a crime to have hack or maliciously use or spread information without the consent of the owner of the data.

– Countries must further promote international standards, including the protection of intellectual property and commercial trade secrets from theft by putting mechanisms in place that ensure that the threat is detected, dissipated as well blocked from recurring again.

– The next item which is that of enhancing security, reliability and resiliency through the promotion of cyberspace cooperation. This entails working with other friendly countries so as to share information on the new threats and share intelligence on the various cyber threats that might arise.

SADC countries should be prepared for 21st century security challenges by recognizing and adapting to the military's increasing need for reliable and secure networks as well as by building and enhancing existing military alliances. This is a key mitigating factor in confronting potential threats in cyberspace and fighting information terrorism in the region.

So, Information terrorism – is the use of information technologies, mass media, dissemination of information for the purpose of targeted influence on the selected object, its discredit. According to statistics, Africa has the fastest growing cases of informational terrorism more than any other continent. This is a worrying trend considering that it is also the fastest growing continent in terms of computer and mobile technology all of which are vulnerable to informational terrorism.

South Africa is one of the biggest cyber hotspots due to its large population and advances in economic and technological development as well as the increasing capacity to host large data volumes.

The features of information terrorism in African countries, that cause many problems: many people are not computer literate and if they are they are at least to the level of being a user and not a programmer; the growing number of mobile users without the knowledge of how cell phone hacking takes place; the use of social media to attack the reputation of a certain individual or company; a database breach; poor identity and access management; the growing interest and contention around the so-called "duty to hack"; the introduction of fibre optic; the barriers to entry in the cyber domain are low, cyberspace includes many and varied actors; information terrorism comprises complex and dynamic technological innovations to which no current legal system is well suited; the mass growing access to internet connectivity in southern Africa; the most African businesses large and small are too ill equipped to withstand the threat of cyber warfare

The ways to combat information terrorism in the African countries:

– They've already started to found governmental institutions like *the Ministry of Cyber Security Threat Detection and Mitigation*; to implement new technologies, particularly information and communication technologies (ICTs); to set up a department which deals with drug abuse as well as information terrorism.

– Countries should be in a position to enact legislation that makes it a crime to engage in information terrorism acts, to have their law enforcement collaboration expanded and the rule of law through the participation in international cybercrime policy development and conferences so as to understand the nature and extent of the threats so as to dissipate it; countries must further promote international standards, including the protection of intellectual property and commercial trade secrets from theft; enhancing security, reliability and resiliency through the promotion of cyberspace cooperation.

Information terrorism is a rising global threat and Africa is no exception, as African Governments have not shown their sure statements of complete intent in fighting cybercrimes for now. SADC in particular must be very vigilant in fighting this new world war whose perpetrators are unknown and often hide behind the veil of anonymity.

Bibliography:

1. Бондар Ю.В. Свобода слова як чинник інформаційної безпеки // Актуальні проблеми міжнародних відносин. Міжнародна інформаційна безпека: сучасні концепції і практика. Вип. 102 (Ч. І). Київ, 2011. С. 127-129.

2. An Information Policy Handbook for Southern Africa / Ed. T. James. Canada, International Development Research Centre, 2001. 245 p.

3. Bespalikova O.O., Vozniuk E.V. World Leaders in Cyber Security // Актуальні проблеми регіональних досліджень: матеріали І Міжнар. наук.-практ. Інтернет-конференції (м. Луцьк, 11-12 грудня 2017 р.) / За ред. В.Й. Лажніка. Луцьк: Вежа-Друк. 2017. С. 230-234.

4. Cyberattack [Web resource] // Collins English Dictionary. 2017. URL: https://goo.gl/iE7gea (reference date: 11.12.2017).

5. Gady F. Africa's Cyber WMD [Web resource] // Foreign Policy. 24.03.2010. URL: https://goo.gl/6Q7sEN (reference date: 11.12.2017).

6. Grobler M., Vuuren van J. Collaboration as proactive measure against cyber warfare in South Africa // African Security Review. 2012. Vol. 21 (2). P. 61-73.

7. Kigen P.M., Muchai C., Kimani K. and other. Kenya Cyber Security Report [Web resource] // Serianu. 2015. URL: https://goo.gl/DHX4Yv (reference date: 11.12.2017).

8. Lee R. Governance of the Security Sector in SADC [Web resource] // Open Society Initiative for Southern Africa. 06.08.2012. URL: https://goo.gl/XKTKym (reference date: 11.12.2017).

9. Shimuleni M., Vozniuk E. Regional Integration and Development: a Theoretical Review of the SADC Region // Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини. 2017. № 10 (359). С. 111-116.

Data about the author:

Voznyuk Eugenia Vasylivna – Candidate of Political Sciences, Associate Professor of International Relations and Regional Studies Department, Lesya Ukrainka Eastern European National University (Lutsk, Ukraine).

Сведения об авторе:

Вознюк Евгения Васильевна – кандидат политических наук, доцент кафедры международных отношений и региональных исследований Восточноевропейского национального университета имени Леси Украинки (Луцк, Украина).

E-mail: vozniukjane.vippo@gmail.com.