West Asia and Africa

No. 03, 121–137, 2016

Citation: XIAO Yingying, YUAN Zhengqing. **A primary exploration on cyber security governance in Africa**, West Asia and Africa, 2016 (03): 121–137.

A primary exploration on cyber security governance in Africa

XIAO Yingying [1], YUAN Zhengqing[2]

[1]*the Graduate School of Chinese Academy of Social Sciences;*
[2]*the Institute of World Economics and Politics of the Chinese Academy of Social Sciences*

Abstract The internet history in Africa is short, but this new technology is spreading fast on the continent. Along with this, cybercrime in Africa is becoming increasingly rampant, while the relevant legal institutions and law enforcement capacity are lagging behind, with public and private cyber security awareness being relatively weak. In recent years, African countries start accelerating the design of institutional framework concerning cyber security governance. Besides e-transaction and cybercrime, personal data protection is also part of Africa's cyber security governance, which is the result of the "impartment" from Western developed countries and the active advocacy from NGOs. Whether at the national level, sub-regional organization level, the African Union level or NGO level, those Western developed countries and western-dominated international organizations have played a role in the institutional design of African cyber security governance, some of which referred to or even copied the original designs of the Western countries. This may lead to the African continent being "recolonized" in cyberspace, with no autonomous decision-making power in global cyber security governance. Besides, from design to implementation, African countries still have a long way to go, and whether the institutions based on the western experience are suitable for the culture and ideas of the African countries, remains to be tested with practice.

About the author: XIAO Yingying, Ph.D. student at the Graduate School of Chinese Academy of Social Sciences (Beijing 102488);YUAN Zhengqing, Researcher at the Institute of World Economics and Politics of the Chinese Academy of Social Sciences (Beijing 100732).

Translated by ZHONG Yehong

Supported by the Project of National Social Sciences Fund which is chaired by Yuan Zhengqing (11BGJ003).

Keywords cyber security, cybercrime, data and privacy protection, governance approach, the African Union

With the rapid development of information and communication technology, the Internet has become an important basis for economic and social development of countries in the world. In cyberspace, due to anonymity of cyber attackers, limited traceability of cyber technology and interconnection of cyberspace itself, cyber security has global [①] and borderless characteristics. This means that cyber security governance status of any country or region has links with the rest of the world and African continent is no exception. In recent years, with a substantial increase in Internet penetration in the African continent, as well as the international community's increasing emphasis on cyber security governance, all actors in Africa have begun to accelerate Africa's institutional framework design on cyber security, therefore understanding and mastering of these latest developments has a great practical significance for China.

According to case studies from home and abroad, before 2010, academic articles about Internet in Africa basically discuss the impacts of information and communication technology on economic development, education, health and other aspects in Africa or opportunities and challenges faced by African continent in bridging the "digital gap," and so on. There are few academic articles about cyber security in Africa let alone articles talking from the perspective of cyber security governance in Africa. Since 2010, many foreign academic articles have begun to talk about the African cyber security (especially cybercrime). Features of these articles are: most of them are country-based studies, descriptive reports and short reports or comments on specific events or seminars which have improvement space for both systematic and theoretical aspects. Chinese domestic research on African cyber security is more backward and typing in "Africa," "Cyber," and "Security" as the keywords for search on China

[①] From a broader perspective, the paper understands cyber security in forms of cybercrime, cyber espionage, cyber terrorism, cyber warfare, online privacy and data protection and so on.

National Knowledge Infrastructure (CNKI), you will find few articles.

What is the status quo of cyber security in African continent? In order to develop cyber security governance, what institutional arrangements do African countries make at different levels? What are the problems and challenges? These are the questions to be studied in this paper.

1 Status quo and concept of cyber security governancein Africa

1.1 Status quo of African cyber security

Cyber security situation in each country and region is closely related to its development level of the Internet, which is the same as African countries. Due to weak economic base, the development of information and communication industry in Africa has always been lagging behind the rest of the world. In recent years, a few submarine cables linking other continents and terrestrial cables linking landlocked countries have been laid in African continent; broadband network coverage has increased significantly and there is a rapid increase in the number of Internet users in Africa. As of December 31, 2014, there were more than 300 million Internet users in Africa, the figure of which increased by 6958.2%, compared with that in the end of 2000. While the growth rate ranking first in the world, the Internet penetration rate (ratio of Internet users to the local population) is only 27.5%, which is still the world's lowest level.[①] In addition to the overall low Internet penetration, there is a big difference for the development level of the Internet among African countries. By the end of June 2014, African countries that have higher Internet penetration rate include Madagascar (74.7%), Mali (72.1%), Malawi (70.5%), Morocco (61.3%), Seychelles (54.8%), Egypt (53.2%) and South Africa (51.5%), which are all higher than that (47.4%) in the same period in China. But Africa is also the continent that has largest number of countries whose Internet penetration rate is less than 2%, including Ethiopia (1.9%), Guinea (1.8%), Niger (1.7%), Sierra Leone (1.7%), Somalia (1.6%) and

① Http://www.internetworldstats.com/stats.htm,2015-06-19.

other countries.[①] Another feature of African Internet development is that the mobile terminal is the main access route. Most places in Africa have not experienced fixed line network in the development stage and have directly rushed into the mobile Internet era, and the majority of Africans use the Internet for the first time through their mobile phones. This is related to factors like the continent's unique geographical environment, underdeveloped land cable, unstable power supply and lower price of mobile than that of PC and so on. At present, Africa has the most rapid growth in the global mobile Internet. Data from the International Telecommunication Union (ITU) shows that from 2011 to 2014, the growth of mobile Internet subscribers in Africa went over 40%, which is twice than that of the global average level; in 2014, fixed-line Internet penetration rate in Africa was only 0.4%, while Africa Mobile Internet penetration rate grew from 2% in 2010 to nearly 20%.[②]

Due to the short Internet history and rapid development in Africa, there are abnormally rampant cybercrime, backward capabilities in legal system and law enforcement and relatively weak awareness of public and corporate cyber security and many other issues. Specifically, cyber security in Africa has the following characteristics:

First, cybercrime [③] is the focus of cyber security governance in Africa. In terms of the specific form of cybercrime, in recent years, most in Africa are related to financial fraud and digitalization level is relatively low. From a technical perspective, the more serious cybercrime requires higher-end bandwidth devices and Internet penetration rate, and 10%–15% of Internet penetration rate is the minimum requirement for large-scale

---

[①] Ibid.

[②] ITU, "The World in 2014 ICT Facts and Figures", http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsF igures2014-e.pdf,2015-04-17.

[③] The concept of cybercrime can be explained in narrow and broad sense. Concept in narrow sense refers to the criminal act violating the confidentiality, integrity and usability of cyber data and systems, such as a variety of cyberattacks carried out by hackers; concept in broad sense refers to any criminal act through the cyber data and systems. Apart from the mentioned above, it also includes those bringing traditional crime new attributes and impact through the cyber, such as financial fraud, drug smuggling, human trafficking and other crimes with the cyber. In this paper, the concept of cybercrime in broad sense is adopted.

hacker activity.[①] Since most African countries do not have laid fiber-optic cables and can only rely on slower speeding satellite connections, which means the longer time when attacking local sites. From the point of view of cybercriminals, this condition is not reliable for the effective implementation of cyber-attack, so 419 Scam [②] is one of the main forms of cybercrime in Africa a few years ago. This form of crime simply takes email as transmission route of fraud and needs the interaction between the offender and the victim. However, in recent years, with the completion of several fiber submarine cables and terrestrial cable, an increasing number of organized criminal groups in Africa (including pirates, terrorists, drug smugglers and human trafficking groups, etc.) are turning to the Internet for crime activities. Because these criminals mastered higher technology means (such as malware and zombie-mail), the forms and the frequency of cybercrime is escalating. Kaspersky Lab's data shows that during the first quarter of 2014, there were more than 49 million attacks in the African continent, most of which occurred in Algeria, followed by Egypt, South Africa and Kenya; cybercrime in South Africa is most rampant, according to Norton, a cyber-security company, 70% of South Africans have all been victims of cybercrime, while the global average is 50%.[③] Especially with the increase of mobile Internet users, mobile banking is becoming a new target for cybercriminals. Many financial institutions' applications in Africa are not ready to cope with security issue, lack of encryption procedures and vulnerable to malicious "phishing" attacks.

[①] M Reilly, "Beware, Botnets Have Your PC in Their Sights", *New Scientist*, Vol. 196, 2007, pp. 22–23.

[②] "419 Scam," also known as the "Nigerian Scam," originates from No. 419 Law which was specialized for prohibiting financial fraud in Nigeria. This is a form of financial fraud that became popular from the 1980s. Its name comes from Nigeria and has no direct relationship with that country. Scammers often claim that they have large sum of money which needs to be transferred and promise that as long as the victim pay a fee in advance, he can get a considerable amount of commission. However, after obtaining the trust, scammers will charge a service fee or other charge for various reasons and immediately disappear after successful frauds.

[③] Tom Jackson, "Can Africa Fight Cybercrime and Preserve Human Rights?", April 10, 2015, http://cybersecuritycaucus.com/can-africa-fight-cybercrime-and-preserve-human-rights, 2015-06-02.

Second, cyber security awareness of public and enterprises in Africa are weak; there is lack of appropriate legal framework at national and regional levels; and shortage of capacity-building is also a serious issue. Although there are many cyber cafes in Africa, most of the supplier failed to provide adequate anti-virus software, so that these computers can easily become target of botnets controllers and hackers. According to the estimation of cyber security experts, about 80% of PC in the African continent have been experienced virus invasion or inserted by malicious programs.[①] Once these computers hijacked by individuals or organizations with bad intentions, these zombie computers will be controlled to send spams or viruses. In addition, there is still lack of a complete and coherent legal framework at national and regional levels in Africa; officers, intelligence and infrastructure are still in shortage in law enforcement agencies.[②] A survey of the United Nations Office on Drugs and Crime (UNODC) shows that more than half of the African countries considered that they are lack of law enforcement resources to investigate the cybercrime, and all African countries expressed the need for technical assistance, in particular the technology regarding the investigation of cybercrime.[③]

Third, under the "impartment" of Western developed countries and the advocacy of civil society represented by local NGOs, privacy and data protection have become an important part of cyber security in Africa. Compared with the former drafts, Convention on Cyberspace Security and Protection of Personal Data adopted by the African Union (AU) in June 2014 covers the content concerning data protection, thereby making Africa became the first area accepting convention on data protection outside Europe. At present, 14 African countries have already started legal framework for privacy and a certain type of data protection administrative authorities, once the Convention of the AU is approved by the member

---

① Gady, F. *World Journal* (世界报), (2010–4–14).

② Fawzia Cassim, "Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players", *The Comparative and International Law Journal of Southern Africa*, Vol. 44, No. 1, March 2011, p. 127.

③ UNODC, "Comprehensive Study on Cybercrime(draft)", February 2013, p. xxiii, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf,2015-06-17.

states and entered into force, a number of other countries are likely to develop a data protection law in accordance with the requirements of the Convention. Analysts believe that the AU's Convention copied the EU data protection model, that each member state has its own data protection law and regulatory agencies.[①]

Fourth, being different from privacy and data protection that are mostly influenced by the West, the contents of e-transactions and the fight against cybercrime of cyber security are the required contents to be constructed of all interested stakeholders in Africa out of their own reality. Increasingly rampant cybercrime has already started to make African countries recognize the need to establish relevant laws and regulations to ensure the security of e-transactions and cyber environment in order to promote the rapid development of the Internet economy and benefit from it. At the same time, compared with Western countries and the Shanghai Co-operation Organization (SCO) member states, African countries pay less attention to the problems of cyber war and cyber terrorism, which is actually the manifest of African countries' general attention to lower rather than higher political issues in security governance.

1.2 African cyber security concept

In June 2014, the Convention on Cyberspace Security and Protection of Personal Data [②] was adopted in the AU Summit held in Malabo, the capital of Equatorial Guinea. Although the Convention covers words about cyber security, "cyber security" concept is not explained in the full text, we have to deduce the AU countries' understanding and perception on cyber security only from the content of the Convention text. The preface of the Convention mentioned that "Aware that it is meant to regulate a particularly evolving technological domain, and with a view to meeting the high expectations of many actors with often divergent interests, this

---

[①] Cynthia O' Donoghue, "New Data Protection Laws in Africa", 19 February, 2015, http://www.technologylawdispatch.com/2015/02/regulatory/new-data-protection-laws-in-africa,2015-06-02.

[②] African Union, "African Union Convention on Cyber Security and Personal Data Protection", pp. 1–3, http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberS ecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf,2015-06-19.

convention sets forth the security rules essential for establishing a credible digital space for electronic transactions, personal data protection and combating cybercrime." This proves that to some extent, the AU's cyber security concept includes mainly electronic transactions, personal data protection and cybercrime.

Sub-regional economic organizations in Africa also play an important role in the collective security mechanism in the region. These sub-regional economic organizations also emphasize the cyber security on e-commerce, cybercrime, data protection and other aspects. For example, in 2009, the East African Community became the first African sub-regional economic organization to accept cyber law framework. According to this framework, the concept of cyber security in Africa is divided into two phases, the first covers electronic transactions, electronic signatures and identification, cybercrime, data protection and privacy; the second phase covers intellectual property, competition, electronic taxation and information security.[①] In the council of ministers held in Botswana in 2012, the Southern African Development Community adopted model laws on data protection, cybercrime and electronic transactions. Economic Community of West African States has also established legal frameworks on electronic transactions (Supplementary Act A/SA. 2/01/10), cybercrime (Directive 1/08/11) and protection of personal data (Supplementary Act A/SA. 1/01/10).[②]

For cyber security policies or regulations enacted in some African countries, they contain the fuzzy definition of cyber security, which have large room for interpretation and may be deemed to include e-commerce, cybercrime, data protection and even more contents. For example, the South African Department of Telecommunications & Postal Services in 2009 launched the cyber security policy which states that "cyber security" means the protection of data and systems from unauthorized access, use,

---

① UNCTAD, "Harmonizing Cyberlaws and Regulations: the Experience of the East African Community", 16August, 2013, p. iii, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=251,2015-06-19.

② ECOWAS, "Strategy on Cybersecurity", July 21, 2014, http://www.africatelecomit.com/ecowasstrategy-on-cybersecurity,2015-04-20.

disclosure, destruction, modification or the influences of the destruction of Internet.[①] National Cybersecurity Strategy, proposed by Kenya's Ministry of Information and Communications and Technology in 2014, defines the cyber security as follows: protection of computer-based equipment, information and services from unexpected or unauthorized access, modification or destruction processes and mechanisms.[②]

African scholars once have defined the concept of cyber security. Nigeria scholar Olayemi suggested that cyber security is the protection of cyberspace from threats, and it usually includes three aspects: first, a series of activities and measures for protecting computers, computer network, related software and hardware equipment and information, software, and data contained therein from a wide variety of threats (including threats to national security); second, the protection level for the abovementioned objects brought by conducting these activities and applying these measures; third, a variety of professional activities including research and analysis in related areas.[③] He also noted that the connotation of cyber security is not just information security or data security, but is also closely related to the latter two, because information security is the core of cyber security. Therefore, it can be seen that the African scholar makes a broad concept of cyber security: cyber security is to protect computers and others against various threats (including threats to national security), which means that cyber war, cybercrime, cyber espionage and other activities should be included.

2 African cyber security governance path

Because of the fragility of the African states, the coexistence of the return

---

[①] The Department of Communications of the Republic of South Africa, "Cybersecurity Policy of South Africa", August 2009, p. 18, http://www.ellipsis.co.za/wp-content/uploads/2011/02/CYBER-SECURITY-POLICY-draft.pdf,2015-06-02.

[②] Kenyan Ministry of Information, Communications and Technology, "National Cybersecurity Strategy", 2014, p. 17, http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecuritystrategy.pdf,2015-06-02.

[③] John Olayemi Odumesi, "A Socio-technological Analysis of Cybercrime and Cyber Security in Nigeria", *International Journal of Sociology and Anthropology*, Vol. 6, No. 3, March 2014, pp. 118–125.

of security governance autonomy towards Africa and security dependence on external actors, a multi-level security governance system including six dimensions of the global system, African continent, African sub-regions, African states and civil society involving NGOs as well as private actors has been formed. Among them, the private actors involved means private military companies that participate in traditional African security issues; they are involved in all types of armed conflict in Africa and play a unique role.[①]

Cyber security is a part of non-traditional security. If it is in accordance with the hierarchical analysis mentioned above, cyber security governance in Africa is formed at other five dimensions of security governance system, except private actors. But African continent, sub-regional, national and NGOs governance systems of four dimensions all have cooperation with global system (UN, EU, etc.), so this paper will take global system as external factor affecting the above four dimensions of cyber security governance and respectively discusses African cyber security governance path (institutional design) from four dimensions: the nations, sub-regional organizations, the AU and the NGOs.

In real life, these institutional designs at different dimensions are not absolutely independent; they also learn from each other and have impacts on each other. For example, domestic legislation of states will base on institutional framework of sub-regional organizations and regional organizations, while the AU Convention is also referring to the existing institutional framework of sub-regional organizations in the process of enactment and so on. In addition, various types of governance bodies also strengthen the interaction in regional and global multilateral forums, such as African Internet Governance Forum and so on.

2.1 At the national level

Since the majority of African countries are busy with more pressing issues like poverty, AIDS, energy crisis, political instability, ethnic conflict, and traditional crime, there are fewer efforts to combat cybercrime. Africa is

[①] Wang, X. *International Forum* (国际论坛), (1): 9–12 (2011).

becoming "safe haven" for cybercriminals. Specifically, although the AU has created the Convention on Cyberspace Security and Protection of Personal Data, it has yet been approved in any African country.[①] Among more than 50 sovereign states of the African continent, only 10 countries, namely, Egypt, Ghana, Kenya, Mauritius, Mauritania, Morocco, Nigeria, South Africa, Uganda and Zimbabwe have developed national cyber security strategies [②]; 5 countries, namely, Cameroon, Kenya, Mauritius, South Africa and Zambia established specialized cybercrime laws [③]; 7 countries, namely, Kenya, Madagascar, Mali, Niger, Nigeria, Tanzania and Uganda have developed data protection laws.[④]

South Africa took the lead in the introduction of legislation to deal with cybercrime, and currently has several specialized laws about cybercrime and data privacy protection.[⑤] For example, in 1996, the Constitution approved by South Africa contains privacy protection content. In 2000, South Africa approved the Promotion of Access to Information Act, 2000, so that Article 32 of the Constitution about information access takes effect officially. In 2002 South Africa approved Electronic Communications and Transactions Act, 2002 which aims to facilitate and supervise electronic communication and transactions. In the same year, South Africa approved the Regulation of Interception of Communications and Provisions of Communication-related Information Act 70 of 2002. In 2012, the country launched the National Cybersecurity Policy Framework. In 2013 it promulgated the Protection of Personal Information Act.

However, Africa's largest economy, namely, Nigeria did not have specialized cybercrime law until May 2015. Prior to this, Advance Fee

---

① Eric Tamarkin, "The AU's Cybercrime Response", *ISS Policy Brief 73*, January 2015, http://www.issafrica.org/uploads/PolB rief73_cybercrime.pdf,2015-05-04.

② NATO CCD-COE,"Cyber Security Strategy Documents", Updated on 18 March 2015, https://ccdcoe.org/strategies-policies.html,2015-04-20.

③ See Dana Sanchez,"Without Laws Governing Cyber Crime, Is Africa Safe for Cyber Criminals?", February 16, 2015, http://afkinsider.com/88623/without-laws-governing-cyber-crime-africa-safe-cybercriminals,2015-06-02; also see Judith M. C. Tembo, "Workshop on Tanzania National Transposition of SADC Model Law", 4th–5th February, 2013, http://afkinsider.com/88623/without-laws-governingcyber-crime-africa-safe-cyber-criminals,2015-04-19.

④ Cynthia O'Donoghue, op. cit.

⑤ "Cyberwellness Profile South Africa", http://www.itu.int/en/Pages/copyright.aspx, 2015-05-09.

Fraud and other Fraud Related Offences Act was approved by the country in 2006, which is the only law involving cybercrime in Nigeria. In fact, because 419 Scam and other cybercrime cause serious damage to the national image of Nigeria, in 2004, cybercrime working group was founded, aimed at establishing a legal and institutional framework to ensure computer systems and cyber security, but because domestic interest stakeholders have disagreement on the terms of the cybercrime bill, the text of bill submitted in senate was adjusted for several times, leading to the delay of the approval of bill by the National Assembly. According to a relatively active civil society organization "Paradigm Initiative Nigeria" in Nigeria [①], the organization called for a strong and fair cybercrime law several times. And it claimed that the relevant laws must be sufficient to deter the occurrence of cybercrime, but also must be fair enough to maintain the Internet freedom so that they won't help the government fight against dissidents. The organization also demonstrated that in the future it will promote Nigeria's legislature to pass a bill of protection of civil digital rights and freedom. It is worth mentioning that, although the Nigerians suffer from terrorism [②], the country pays less attention to cyber-terrorism issues. Although the Cybercrime Bill involves the provisions dealing with cyber-terrorism, the content is little and just mentions that for the purposes of terrorism, any access to computers or computer systems will be sentenced to 20 years imprisonment or a fine of 25 million Nigerian naira, or concurrence of both.

Other African countries such as Botswana, Kenya, Uganda and Cameroon have begun to introduce cyber legislation and establish regional cooperation mechanisms to combat cybercrime.[③] In addition, Mauritius is the only African country that signed and ratified the Budapest Convention on Cybercrime [④], South Africa in November 2001 signed the Convention,

---

① "Nigeria's President Jonathan Signs the Cybercrime Bill Into Law", May 16, 2015, http://techloy.com/2015/05/16/nigerias-president-jonathan-signs-the-cybercrime-bill-into-law,2015-06-10.

② http://www.mofcom.gov.cn/article/i/jyjl/k/201411/20141100806763.shtml,2015-04-20.

③ Fawzia Cassim, "Addressin g the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players", pp. 123–124.

④ The Budapest Convention on Cybercrime, approved by the European Commission in November 2001, is the world's first international convention against cybercrime. As of October

but not yet ratified. Morocco and Senegal are considering joining the Convention.

Legislatures in African countries are directly or indirectly affected by multilateral institutional arrangements within and beyond the region. For example, the West African countries will take Commonwealth Model Law on Computer and Computer Related Crime and the Council of Europe's the Budapest Convention on Cybercrime and Directive on Fighting Cybercrime within ECOWAS (2011) as guides.[①] Foreign scholars found that the content of South Africa's Electronic Communications and Transactions Act is very close to the Commonwealth model law, the Southern African Development Community model law and the Budapest Convention on Cybercrime, and in particular highly similar to the terms of the Budapest Convention.[②]

2.2 At the sub-regional level

Different regions of Africa have established a number of sub-regional organizations during and after the Cold War, such as the East African Community, the Economic Community of West African States (referred to as ECOWAS), the Economic Community of Central African States and the Southern African Development Community. Sub-regional organizations created during the Cold War focused on economic cooperation; after the Cold War, the sub-regional organizations have begun to take traditional security and non-traditional security as their cooperation fields and became an important part of Africa's collective security mechanism.

As part of the non-traditional security, cyber security has been covered in the agenda in several African sub-regions. Although sub-regional organizations are seen as supporting forces [③] on the African continent for

---

2014, there were 44 countries that have signed and ratified the Convention in the world, including the United States, Japan, Australia and other countries.

[①] UNODC, Comprehensive Study on Cybercrime(draft), p. 74.

[②] Deutsche Telekom Group Consulting,"Republic of South Africa Review Report: E-commerce, Cybercrime and Cybersecurity-Status, Gaps and the Road Ahead", 26 November, 2013, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/south-africa——status-gaps-and-road-aheadcyber,2015-06-19.

[③] Lyu, S. Master's thesis, China Foreign Affairs University, 18 (2014). In the paper, it proposed that since the Cold War, the "trinity" collective security mechanism has gradually been formed in

the collective security mechanism, in regard to promote cooperation on cyber security, sub-regional organizations show more active and more flexible features than the regional organizations (AU) and form a sub-regional cooperation mechanism network. It is noteworthy that when carrying out cyber security cooperation, these sub-regional organizations have received financial and technical support from the Europe, the United States and other Western countries and Western-dominated international organizations.

For example, most West African countries use ECOWAS to promote cooperation in the field of cyber security. The First West Africa Cybercrime Summit was held during November 30–December 2, 2010 in Nigeria's capital, Abuja. The summit was jointly organized by ECOWAS, the United Nations Office on Drugs and Crime, the Nigerian Economic and Financial Crimes Commission (EFCC) with the theme "The Fight against Cybercrime: Towards Innovative and Sustainable Economic Development." In addition to the African countries, foreign countries like the United States, France, the UK, Austria, Turkey and the United Arab Emirates as well as international organizations like the United Nations Office on Crime and Drugs, the European Commission, the International Criminal Police Organization and the European Union also sent representatives to attend the summit.[①] From September 2012 to January 2013, the US Department of State successively held West African cyber security and cybercrime symposium, participated by Francophone and Anglophone Western African countries, in Dhaka of Senegal and Accra of Ghana to jointly discuss the issues such as strengthening domestic legislation, establishing emergency response mechanisms and promoting a comprehensive cyber security plan of Internet freedom and respect for human rights.[②] In 2014, the ECOWAS and the United States Conference on Trade and Development (UNCTAD) held a joint seminar to help

---

the interior of the African continent, taking the AU as the main force, African sub-regional organizations as the auxiliary force and regional powers as the core force.

① "West Africa Takes Lead in Fighting 419 Scams", http://www.unodc.org/nigeria/en/1st-westafrica-cybercrime-summit.html,2015-04-08.

② US Department of State, Press Release, West African Cybersecurity and Cybercrime Workshop, January 28, 2013, http://www.state.gov/r/pa/prs/ps/2013/01/203379.htm,2015-04-08.

ECOWAS to coordinate cyber-related legislation. The seminar had two themes: one is to coordinate cyber-related legislation in Member States, and another is to strengthen the coping with cybercrime. The former was funded by UNCTAD, while the latter was funded by the European Commission.

Projects in other parts of Africa to prevent and combat cybercrime have also been funded by Western countries. During August 22–24, 2013, a seminar about East African countries to combat cybercrime was held in the Tanzanian capital Dar es Salaam, the seminar was funded by the European Commission and was the cooperative project initiated by the African Center for Cyberlaw and Cybercrime Prevention (ACCP), the European Commission and the United Nations African Institute for the Prevention of Crime and Treatment of Offenders (UNAFRI). At the seminar, the Budapest Convention on Cybercrime of the Council of Europe was regarded as reference materials and guidance for the series of issues (cybercrime, definition of electronic evidence, practice in the process of legislative execution, etc.).

Under the influence of the Council of Europe, many sub-regional organizations have put forward initiatives of preventing and combating cybercrime in Africa. For example, the East African Community approved the EAC Framework for Cyberlaws (2008); ECOWAS approved the Directive on Fighting Cybercrime within ECOWAS (2011); the Common Market for Eastern and Southern Africa (COMESA) also developed the COMESA Cybersecurity Draft Model Bill (2011); and the Southern African Development Community developed The SADC Model Law on Electronic Transactions and Ecommerce (2012).[①] But only the Directive of ECOWAS has the binding force to combat cybercrime. In addition, those legal documents that do not have binding force can provide the legislations of African countries a reference or example; when many countries choose to coordinate the domestic law and model law, documents without binding

[①] ACCP, Workshop Report on Cybercrime Legislation in West Africa, 11 April, 2014, pp. 31–33, http://tftcal.unctad.org/pluginfile.php/12929/mod_resource/content/2/Workshop%20Report%20by%20ACCP%20Ghana%2018%20-%2021%20March%202014.pdf,2015-04-21.

force enforcement can also have an important impact.[①]

On the relationship between these initiatives proposed by African sub-regional organizations and the Budapest Convention on Cybercrime, relevant seminars have pointed out that the spirit of Budapest Convention on Cybercrime is already reflected in these initiatives which increases the possibility of African countries' joining the convention. It also means that there will be further cooperation within African continent and between the African Union Commission and the European Commission.[②] COMESA Cybersecurity Draft Model Bill (2011) is considered very detailed in terms of international cooperation and meets all the criteria of the Budapest Convention on Cybercrime, and the law also includes related terms of consumer protection and service providers' obligations. SADC Model Law on Electronic Transactions and Ecommerce (2012) is not considered up to standards of the Budapest Convention on Cybercrime, because it does not include terms about international cooperation, mutual assistance and extradition provisions.[③]

2.3 At the level of the AU

In fact, the main role AU plays in African security construction for a long time has been extended to the field of cyber security. In June 2014, the AU Summit held in Malabo, Equatorial Guinea's capital and approved the Convention on Cyberspace Security and Protection of Personal Data. The initial version of the Convention was proposed in 2011; but after several modifications before the final version, the draft before the final version was entitled Draft African Union Convention on the Confidence and Security in Cyberspace, which should have been approved in January 2014. However, due to the multi-party opposition, the AU in May 2014 held a meeting of experts and conducted a full review of the Convention and renamed it. These opponents, mainly from the private sectors and civil society groups, believed that the Convention did not reflect their will

① UNODC, "Comprehensive Study on Cybercrime(draft)", p. 64.

② Patrick Mwaita and Maureen Owor, "Workshop Report on Effective Cybercrime Legislation in Eastern Africa", 22–24 August 2013, pp. 2–3, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571_EastA frica_WS_Report.pdf,2015-04-20.

③ ACCP, "Workshop Report on Cybercrime Legislation in West Africa", p. 32.

in terms of protection of privacy and freedom of speech.[①] For example, one NGO from Kenya pointed out that the original draft convention gives too much power to the government, in particular, power to access private information. The relevant provisions allow the government for the purposes of national security and public interest to obtain personal data and sensitive data without the owner's permission. They also pointed out that in Africa, the national security is often understood as regime security, and the draft would allow the government to get access to personal data and fight against dissidents.[②]

After experiencing the multi-stakeholder game, the AU finally approved the Convention on Cyberspace Security and Protection of Personal Data. Many contents regarding the protection of data of the Convention are the reflection of relevant EU system. For example, the AU Convention also requires member states to establish an independent national data processing agency (DPA); the institution must have broad powers, including the investigation, evaluation, warning, notification and fining. The Convention requires data holder not to transfer personal data to the country outside the African Union, unless the receiving state can ensure an appropriate level of protection, the term "appropriate" is the same to that of Article 25 in the Data Protection Directive of the EU.[③]

Overall, there are still many deficiencies in the Convention. First, the scope of the AU Convention is too broad, including e-commerce, data protection and cybercrime, which make the content cumbersome. African countries should first concentrate on the terms about its cybersecurity and cybercrime.[④] Second, many elements of the AU Convention "transplant" the laws and regulations of the Western countries which are beyond the existing law enforcement capacity of African countries and bring them

---

[①] "African Union Adopts Convention on Cyber Security", 14 July 2014, https://ccdcoe.org/africanunion-adopts-convention-cyber-security.html,2015-04-22.

[②] Joel Macharia, "Africa Needs A Cybersecurity Law But AU's Proposal is Flawed, Advocates Say", January 31, 2014, http://techpresident.com/news/wegov/24712/africa-union-cybersecurity-lawflawed,2015-04-22.

[③] Graham Greenleaf and Marie Georges,"The African Union's Data Privacy Convention: A Major Step toward Global Consistency?", *Privacy Laws & Business International Report*, 2014, pp. 18–21.

[④] Eric Tamarkin, "The AU's Cybercrime Response", p. 4.

difficulties to ratify and implement the Convention. Thirdly, the Convention must be approved by 15 AU member states to take effect, but so far it has not yet approved by any country which makes the prospect bleak. In addition, given the rapid technological development, the relevant institutional arrangement is probably also lagged when the 15 member states ratify the Convention. Fourth, the Convention does not limit the sharing of information between private sectors and governments, and there is no statement that when fighting against cybercrime, the government should be limited to what extend for the power of getting access to information, which is regarded "very dangerous" for civil society.[①] In many cases, the Convention seems to place national sovereignty and discretionary right above the discretion of international law. For example, in Chapter Three about promoting cybersecurity and fighting cybercrime, the Convention adopts the statement of all methods that are considered necessary, appropriate and effective. Such a broad discretionary right will leave countries (particularly undemocratic countries) space of abuse of these powers. Fifth, because there is no direct affiliation between the AU and sub-regional organizations, in the actual operation process, there may be contradictions and conflicts between the institutional arrangements.

2.4 At the level of NGO

Since the 1990s, under the impetus of Western countries, function and influence of African NGOs have rapidly expanded from limited fields of humanitarian relief and social services and so on to other fields of economic, political and social development, and their status in national politics life has risen considerably in Africa. As representatives of civil society, African NGOs also began to share the responsibilities of the social management and services of African countries, and even exert a political function.[②]

Most African NGOs are closely related with Western governments. On

[①] "Africa Must Improve its Cyber-Security", AFK Insider, Feb. 25, 2015, http://umaizi.com/africa-must-improve-its-cyber-security,2015-04-08.

[②] Wang, X. *West Asia and Africa* (西亚非洲), (8): 57 (2009).

the one hand, many NGOs active in Africa are Western NGO branches in Africa. On the other hand, the majority of local NGOs are funded by Western governments and NGOs. Because of this, NGOs in Africa are mostly the "spokesmen" of Western ideas. Reflected at the institutional design level, compared with the previous draft, the AU Convention on Cyberspace Security and Personal Data Protection adds contents like personal data protection, privacy protection and so on, which are in fact supported by the West-supported NGOs. After a few weeks since the AU Convention was approved, 21 NGOs which participated in the Internet security-related activities in Africa, including many well-known human rights organizations, jointly launched the African Declaration on Internet Rights and Freedoms. Among the 12 key principles of the Declaration, there are two terms related to the protection of Internet privacy and data security. The declaration also includes the contents regarding anti-mass surveillance. The declaration also proposed that in order to implement these principles, they should be consistent with those data protection principles which have already been established. Although without explicating the established principles, the analysis supposes that they may be data protection principles in the AU Convention.[①]

Moreover, the African NGOs seldom protest the US's control over the global Internet domain name and the administration over root name server with the help of the Internet Corporation for Assigned Names and Numbers (ICANN). In fact, one of the major challenges of the Internet development facing Africa is the lack of domain name system (DNS). According to the statistics from the African Network Information Center (AFRINIC), as of October 2012, the number of African Country Code Top-level Domains (CCTLD) was 797,952, which only takes 1% of the global total; the number of African Generic Top-level Domains (GTLD) was 122,144, accounting for 0.09% of the global total; for the IPv4 [②]

[①] Graham Greenleaf and Marie Georges, "The African Union's Data Privacy Convention: A Major Step toward Global Consistency?", pp. 18–21.

[②] "IPv4," the fourth version of the Internet Protocol (IP), is the first agreement to be widely used and the cornerstone of today's Internet technology.

address, Africa has 47,522,304, which takes only the global 1%.[①] The comparison of these two can better reflect the interest tendency of African NGOs.

3 Challenges facing the African cyber security governance

Africa has preliminarily established the basic framework of cybersecurity governance, but the challenge remains daunting. This is because the Internet development of the African continent lags behind; system construction starts late; and the majority of institutional arrangements in the governance body still remain on paper, which have no true power. The AU Convention, just passed in 2014, has not yet entered into force. The majority of system arrangements made by sub-regional organizations is not legally binding and can only provide guidance to domestic legislation in member states. Few African countries have specialized laws on cybercrime or data protection, and it is still unknown that whether these countries have the willingness of adjusting their national legislation based on regional or sub-regional institutional arrangements. Challenges facing African Internet governance are mainly:

First, it is to be improved for African stakeholders (particularly governments) to actively participate in international cooperation in cybersecurity management. In terms of international cooperation at the regional level, the African Internet Governance Forum (AFIGF) has only three sessions by now; the number of participating countries and parties involved is to be increased.[②] The only 195 participants in 2nd African Internet Governance Forum were from the governments, private sectors, civil society, regional and international organizations of 29 countries. Participants in the 3rd African Internet Governance Forum had up to 470 people who were from 41 countries; though more participants, it is still a small number when compared with the total 54 African countries. On the

[①] "ICANN's Africa Strategy Document V1.1", October 2012, http://www.afrinic.net/index.php?option=com_content&view=article&id=854,2015-06-23.

[②] The 1st African Internet Governance Forum was held in 2012 in Egypt; the 2nd one and 3rd one, respectively, were held in Kenya in 2013 and in Nigeria in 2014.

global Internet Governance Forum, it is hard to hear sounds from Africa. Stakeholders in Africa currently take a wait-and-see attitude and there are many reasons behind it. In addition to the lack of adequate cyber management experts and other more pressing things to deal with, it is also because that African governments, politicians and the media take global cyberspace governance as the field of super powers' game, and such attitude is seriously affecting the progress of cyber security governance in Africa.[①]

Secondly, the African governance bodies are deeply influenced by Western countries, and almost completely accept their concepts, the core concerns and systems. It may result in the following: the African continent will be once again "colonized" in cyberspace and has no independent decision-making power on cyber security governance issues. In the name of helping African countries strengthen their capacity building, European countries and the United States "impart" their experience and promote institution building in African countries with the power of African NGOs. For example, before the start of the Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial) which held in April 2014 in Sao Paulo, Brazil, there was an open proposal procedure that allowed all stakeholders to submit about their views and suggestions on Internet governance principles and reform road map. At that time, the meeting received a total of more than 180 materials, of which 19 were from Africa—one from the government (Government of Tunisia), nine from civil society organizations, three from the private sectors, one from technology community, one from multi-party stakeholder platform and four from academia.[②] From the content of material, 14 materials were related to human rights and freedom of expression; 11 materials were related to the role of government; and five were security-related materials, four had relation with net neutrality, payable access and the globalization of the

[①] Ephraim Percy Kenyanito, "Internet Governance: Why Africa Should Take the Lead", http://www.circleid.com/posts/20140225_internet_governance_why_africa_should_take_the_lead,2015-06-19.

[②] Ephraim Percy Kenyanito, "Spotlight on African Contributions to Internet Governance Discussions (Part 1: NETmundial)", April 23, 2014, http://www.circleid.com/posts/20140423_african_contributions_to_internet_governance_discussions_part_1,2015-06-19.

function of Internet corporation for assigned numbers; one material was related to functional globalization of the function of Internet corporation for assigned numbers. All of these materials believed that enabling all stakeholders to get involved in the process of cyber management was very important, and they agreed decentralized governance model. Thus, the concepts and core concerns of African countries have a very high similarity with Western countries. The only exception is Sudan, and the content of its material is something other materials did not have. One material mentioned that American political sanction against Sudan was the destruction of the net neutrality. Another one mentioned that the Internet Corporation for Assigned Names and Numbers is an institution controlled by the US government and it would adversely affect the free flow of information in Sudan which was imposed sanctions from the United States.

Third, capacity building of African cyber security management needs to be strengthened. Being limited in finance and technical capacity, the insufficiency of personnel and agencies combating cybercrime in African countries brings barriers to the implementation of institutional arrangements. Information and telecommunication technology sectors are mostly responsible for Internet security in African countries, and there is no similar specialized agency or specialized personnel like Cyberspace Administration of China or White House Cybersecurity Coordinator of the United States. At the AU level, it is lack of institutions like the European Union Agency for Network and Information Security (ENISA), which is responsible for organizing and coordinating information security strategy planning, practice, infrastructure protection and emergency response in the EU member states.

Fourth, in terms of cyber security governance, the AU has yet formed a joint force with the member states, official and unofficial agencies. For African countries, it is worth learning from that the EU has formed a cyber security management system with features of “one theme (cyber security), two levels (the EU and its member states), three bodies (government, private sectors and academia),” and has preliminarily established an

information sharing mechanism between different levels and different bodies.[①] Compared with the Europe, the degree of integration in Africa is much lower and the relationship between the AU and its member states are not very close, therefore, the AU is difficult to play a organizing and coordinating role as the EU and the collective actions of African countries for dealing with cyber threats also face challenges. In addition, the African NGOs are in underdevelopment, and most of them are supported by Western countries or Internet companies, so what they advocate are "liberty" and "democracy" which are western core values and do not fit well with the core concerns of African governments. This also makes it difficult for Africa to form a governance model with combination of official and unofficial channels.

[①] Lei, X. & Li, W. *Information Security and Communications Privacy* (信息安全与通信保密), (239): 56–57 (2013).