CYBERWATCH FINLAND

Country Analysis AFRICA

This time around, the country analysis will focus on the entire continent of Africa. The cyber security of this 54-nation body is currently in a much worse position in comparison to the rest of the world. The cyber education is subpar, citizens' cyber skills are underdeveloped, pirated software is widely used and cybercrime is on the rise. Other states and international cybercriminals use Africa as an arena for their activities, mainly due to a lack of legislation and cyber defence capabilities. The technological void in Africa is of interest to China and Russia, which have succeeded in spreading their own technology to the region.

Country Analysis: Africa

1. China and Russia have a geopolitical interest in Africa and both trade with various African countries and invest in the area. Commercial activity also provides a good opportunity for both countries to influence decisions regarding technology, which can contribute to their goals in cyber operations.
2. The cyber warfare capabilities of African countries are still subpar. Nigeria is emerging as Africa’s leading country in cyber warfare.
3. Africa is susceptible to cybercrime and espionage. At a societal level, not enough has been invested in cyber security and only a few countries have cyber strategies or legislation. Citizens’ cyber skills and companies' investment in cyber security are inadequate and no rapid improvement is expected.

From a cyber security perspective, Africa, a continent comprised of 54 countries, is very different from other continents. The telecommunications and technology infrastructure is underdeveloped and technical know-how is very much in the hands of non-African companies and states. The same is true for other critical infrastructure. IT systems and equipment come almost entirely from outside the continent, there is no in-house production. The current situation could be regarded as typical of the former colonies. Knowledge was in the hands of the former colonial power and was not transferred to the local population.
Several former Asian colonies, most notably India, have been able to reverse the situation and are currently the world’s leading producers of ICT technology and services. African countries have not been able to develop technology and knowledge capital as effectively and are still highly dependent on external actors for cyber security.

The technology and knowledge gap has increased foreign investment in Africa in recent years. Of the former colonial powers, the United Kingdom, France and the Netherlands, as well as the United States, are generally at the forefront of foreign investment. However, more recently, China has also become one of the most active investors. In addition to investment, China is an active trading partner with several countries and has been actively involved in high-tech projects in Africa. Chinese network technology has been used to build the telecommunications infrastructure, and several positioning systems built in Africa are based on the Chinese BeiDou navigation service. In addition to China, Russia is also an active trading partner, especially in countries in northern Africa. Russia exports arms to several African countries and has participated in the training of local armed forces. In addition, Russia, like China, has shown interest in high-tech exports.

Foreign states are interested in Africa mainly for its natural resources, such as oil, agricultural raw materials and mining. Africa is currently experiencing a technological void in many areas, making it a fertile ground for high-tech trade as well. In areas in which the United States and much of Europe reject Chinese network technology for example, in Africa it is welcomed with open arms. Indeed, Africa provides China and Russia with an excellent platform for their own cyber-influencing goals, which is important for Western powers to keep in mind when operating in Africa.

The cyber capabilities of African armed forces have developed in recent years, but are still at a very early stage. In the mid-2010s, various Ministries of Defence woke up to the need to develop cyber defence capabilities, and in recent years a few countries have established their first cyber warfare units. In this field, Nigeria is one of the most developed countries in Africa. The Nigerian military has announced that it will now also be training in cyber warfare in its annual war exercise, *Exercise Crocodile Smile*. The exercise will be held in late 2020 and is reportedly the first cyber warfare exercise ever organised by the armed forces of an African country.

The pressure to develop a cyber defence has arisen due to two different factors. Other states, as well as international cybercriminals, have taken advantage of Africa’s undeveloped cyber defence capabilities by channeling cyber attacks through Africa. African countries want to prevent the use of their telecommunications infrastructure as a platform for state actors and cybercrime operations. Another factor is the growing use of the cyberspace by local criminal and terrorist groups. In Nigeria, for example, the Boko Harum terrorist organisation is making effective use of the cyberspace to recruit members and spread its ideology.
The State Security Service wants to address the situation through cyber operations. The armed forces of various countries are continually improving their cyber capabilities, but progress has been slow so far.

The number of Internet users in Africa is rising faster than the development of citizens' cyber skills. At the beginning of 2020, there were approximately 570 million Internet users in Africa, representing just over 40% of the total population. The number of Internet users is predicted to exceed one billion by the end of the 2020s. National cyber capability inadequacy is a widely recognised problem. Every day, thousands of Africans connect a recycled IT device to the Internet for the first time in their lives, without guidance or knowledge on the basics of cyber security. The situation is not much better in the business sector either. There is a limited amount of employees with practical cyber security experience. The international organisation ISACA, which certifies security professionals, estimates that less than five percent of all security certificate holders in the world live in Africa.

Africa is at the forefront of pirated software in the world, and in Libya and Zimbabwe, for example, it is estimated that up to 90% of operating systems are unlicensed copies. If your operating system is not licensed you will not receive vital security updates, due to which your IT device will quickly be infected with viruses and malware. In addition to the weak protection, cybercriminals are also interested in the lack of cyber law in Africa. Only about half of African countries have cyber legislation in place or under construction. Cybercriminals have been found to change the area in which they act according to the developments in legislation. Once a state has enacted cyber security legislation including sanctions, criminals have moved to a weaker country. Admittedly, the resources for cybercrime investigation are also limited in Africa than in the rest of the world, so legislation per se is not a very strong deterrent.

Cybercrime is growing rapidly in Africa and unfortunately a sudden turn for the better cannot be predicted. Cyber security training opportunities are slowly increasing. Improving know-how will bring much-needed cyber security manpower,but will also enable skills to be used for criminal activity. Developments in cyber security legislation and other societal activism are important factors in changing attitudes to ensure that the next generation of cyber experts develop in the right direction. About a year ago, the African Union Cybersecurity Expert Group (AUCSEG) was set up by the African Union to improve cooperation between countries. Their work is still at an early stage and their resources are limited, so the positive effects are likely to be seen only in the longer term.

Sources:
https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527
https://army.mil.ng/?p=3659
https://www.defenceweb.co.za/cyber-defence/armscor-cybersecurity-unit-up-and-operational/
https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf