INTERNATIONAL JOUNAL OF: SCIENCE RESEARCH AND TECHNOLOGY

TIMBOU-AFRICA ACADEMIC PUBLICATIONS
INTERNATIONAL JOURNAL, FEBRUARY, 2023 EDITIONS
VOL. 12 NO. 9 ISSN: 2623-7861

CYBER SECURITY CONCERNS AND THE IMPACT OF BREXIT ON THE SUB-SAHARAN AFRICA.

***RUMANA KABIR AMINU; **MUHAMMAD ALIYU; & **ZAINAB ALIYU MUSA**

*Department of Computer Science, FCT College of Education, Zuba, Abuja, Nigeria. **Department of Computer Science, Federal Polytechnic, Bauchi, Bauchi State, Nigeria

ABSTRACT

Cybersecurity, which refers to the methods, procedures, and safeguards that support the defense of computer networks, devices, and data against tampering, theft, and damage, has not been a key focus of Brexit discussions, either diplomatically or publicly. In fact, it feels fairly underappreciated considering its critical role in promoting economic growth and political stability. criminal cyber actors take advantage of the borderless nature of the internet coupled with the confusion that comes with brexit. While other articles focus

INTRODUCTION

The economies of Africa and other developing nations are financially significantly reliant on the former colonizing nations and western finance in general. Even when they have formed free trade zones for themselves, these economies of the global South have found it extremely difficult to detangle themselves from the trade liberalization promoted by the global North because of this dependency. As a result, the dependent South is the one who suffers the most when a significant change affects the North's economy. According to this theory, economic protectionism for South American nations would reduce their reliance on North American integration and development models. The economies of Africa and other developing nations are financially significantly reliant on the former colonizing nations and western finance in general. The biggest economies in Africa are expected to suffer as a result of Brexit, according to forecasts. Bilateral trade between Nigeria and the UK, was valued at £6 billion (about $8.3 billion) and projected to reach £20 billion by 2020, but because of the disruption "The total trade in goods and services (exports plus imports) between the UK and Nigeria currently stands at £5.5billion in November 2022. Additionally, according to figures from the National Bureau of Statistics, Nigeria's top foreign investor in 2015 was the United Kingdom. Because of this type of dependence, the recession in the UK brought on by the Brexit has severely hurt Nigeria's economy. Beyond commerce and investment, the UK also plays a significant role in Nigeria's Cybersecurity. In Nigeria's Cyberspace the European Union is a

on trade and development. economic , geopolitical , social implications of brexit, this paper focuses on the implications of brexit on CyberSecurity, we presented the implications of brexit on uk cyber security policy, the African Cyber Security Land Scape and the Possible cyber security implications of brexit on sub-Saharan Africa. We concluded by recoomendations on how to strengthen the subsaharan Africa cyber security.

significant partner. For instance, the EU plans to invest 820 million Euros through its EU-Nigeria Digital Economy Package (Global Gateway Initiative) to support Nigeria's digitalization strategy through investments in digital infrastructure, the digitization of public services, digital entrepreneurship, digital skills, and digital governance. Nigeria's cyberspace is governed by several agencies including the Nigerian Communications Commission (NCC) and the National Information Technology Development Agency (NITDA).

The Cyber security Landscape

Given the nature of the internet and other information networks, which stretch over numerous nations and regulatory boundaries, cyber security is a naturally global endeavor.

With major attacks like Wannacry and NotPetya, more businesses and people being victimized by cybercrime, efforts to deal with illegal activities and content online, and accusations of attempted political interference in elections, cybersecurity has quickly moved up the political agenda in recent years. These have all aided in raising awareness of the significance of safeguarding our digital selves, safeguarding the vital digital plumbing, and taking action against those who abuse and misuse it to hurt us. There's a limit to what a country can do on its own; inevitably there's a lot of cooperation, and a good deal has been done in the EU (King, 2020). So how will Brexit affect that cooperation?

In order to achieve effective cyber security, key stakeholders, including government security and intelligence agencies, cyber security companies, organizations like computer emergency response teams (CERTs), and a variety of other concerned actors, must exchange high-quality cyber threat intelligence (CTI) and take subsequent remediation and mitigation measures. The majority of CTI data comes from public sources, therefore its origin need not be hidden. However, it may occasionally be supplemented by knowledge of notable cyber actors learned from covert sources. A precise understanding of the cyber threat landscape provided by effective CTI enables organizations to prevent, discourage, or at the very least, prepare for future adversary activities. This is acknowledged in the Political Declaration, which lists "cyber-threats" as a particular justification for "timely and voluntarily" intelligence exchanges. Brexit might have negative consequences in one particular area of intelligence and security collaboration. Cybercrime is by far the largest cyber security concern in terms of scale, and Brexit will have an impact on the UK's judicial and policing counter-cybercrime capacities (Stevens & O'brien, 2019).

Brexit and implications on cyber security in the UK

1. Compliance and Data protection challenges
   The incoming EU General Data Protection Regulation (GDPR) demonstrates a clear need for increased transparency across the EU at a time of escalating threats.(Sharf, 2016). The GDPR has significantly increased consumer and citizen data protection awareness, the UK's data protection framework will continue to be heavily influenced by the EU's GDPR (Stevens,2021).
2. Confusion
   There is chaos as to how companies will respond in a situation of cyber attack. Many in the UK security industry are unsure which decision is better for UK businesses and what impact Brexit—the UK's withdrawal from the EU—will have on this relationship and the industry's future. This confusion stems from the conflict between what the current UK Government wants and what the EU believes is best for its citizens.
3. Skills shortage
   As the global cybersecurity workforce grows so does the gap of professionals According to 2022 cyber workforce study, Globally , the year 2022 records the highest so far in cyber security professionals shortage which is estimated to reach 3.7 million and the highest estimated size of the global cybersecurity workforce in 2022 is 4.7 million people (Study, 2022).
   To adequately protect cross-industrial enterprises from increasingly complex modern threats, organizations are trying to fill the worldwide gap of 3.4 million cybersecurity workers.
   The demand for cybersecurity services is increasing even more quickly than the workforce. The cybersecurity workforce gap analysis by (ISC)2 showed that despite the addition of more than 464,000 workers in the past year, the gap has increased by 26.2% year over year, growing more than twice as much as the workforce, making it a profession in desperate need of more people. Due to a shortage of talent and the estimated 142,000 open positions throughout Europe, Brexit will certainly make it more difficult for UK businesses to hire employees from the EU. (Button,2018).
4. Data Access and sharing
   There is more need for a systematic monitoring and information sharing. How simple it will be for cooperative data-sharing programs to continue once the UK exits Europe is one of the major challenges posed by Brexit. The UK's cyber-defence plan must prioritize information-sharing initiatives because numerous businesses experience comparable threats. Threats can be dealt with more quickly and successfully by sharing and pooling their knowledge.
5. Reduction in the operational effectiveness and cyber security decision making of both UK and EU(Version, 2021)

The African Cyber security landscape

Africa is a continent with diverse population that is rapidly growing in terms of population , economy and global influence. Africa has a population of about 1.21 billion people (up from just

800 million in 2000) having the youngest population in the world with a median of 19.5 years. With the growing number of youth comes need for increased global connectivity as well as a productive social engagement. In addition, more people are adopting technology, as evidenced by the exponential growth of mobile device ownership, rising social media usage, and the impending commercialization of the Internet of Things (IoT). Even the most conservative metrics indicate that Africa is in a strong position to advance and contribute to future global growth. Along with this quick economic expansion, a thriving e-commerce sector has also emerged, with projections for it to reach $75 billion USD by 2025. However, with this escalating wealth and digitization, new risks and weaknesses appear that could thwart advancement. The global increase in cybercrime is foremost among these concerns. A more skilled group of cybercriminals are becoming attracted to the population of the African Continent, their computer systems, and the continent's information technology (IT) infrastructure as the economy of the continent moves online. Cybercrime is becoming more prevalent worldwide, not only in Africa.(GFCE,2016)

Possible Cyber security implications of Brexit on Subsaharan Africa

1. Lack of Detailed and reliable threat information regarding cybercrime threats in Africa. Lack of this data is prone to affecting our decision making process and how to identify gaps as well as strengthen protection, prevention and response mechanisms to confront the diverse range of cyber threats.
2. Maintainance of data protection requirement and information exchanges
   For Africa to have full control of its data, a platform must be created to have its data resident within the African continent. The Malabo Convention sets a strong intention for the protection of personal data and ensuring cybersecurity in Africa. The Convention seeks to establish a credible framework for cybersecurity in Africa through organisation of elec-tronic transactions, protection of personal data, and promotion of cybersecurity, e-governance and combating cybercrime. Countries like Nigeria, Kenya, Senegal, Rwanda and SouthAfrica have comprehensive data protection laws however (Tomiwa, 2020) finds that the status of the data protection in Africa is inadequate as a result of dependence on Data protection Authorities and lack of institutional capacity and others.

Table 1 Data protection across 4 major sub regions in Africa

Key data protection issues	Senegal	Nigeria	Kenya	Uganda	Morocco	Tunisia	South Africa	Mauritius
Legislation (Status)	[23] ✓ (Enforced)	[24] ✓ (Enforced)	[25] ✓ (Not yet enforced)	[26] ✓ (Not yet enforced)	[27] ✓ (Enforced)	[28] ✓ (Enforced)	[29] ✓ (Partially enforced)	[30] ✓ (Enforced)
Rights of data subjects	✓	✓	✓	✓	✓	✓	✓	✓
Data protection principles	✓	✓	✓	✓	[31] ✓	✓	✓	✓
Legal basis for processing	✓	✓	✓	✓	✓	✓	✓	✓
Data security	✓	✓	✓	✓	✓	✓	✓	✓
Data breach notification	×	[32] ×	✓	✓	×	×	✓	✓
Cross-border data flow	✓	✓	✓	✓	[33] ✓	[34] ✓	[35] ✓	✓

Registration with supervisory authority	✓	x	✓	x	[36] ✓	✓	x	✓
Data protection impact assessment	x	[37] x	✓	x	x	x	✓	✓
Privacy by design and default	x	x	✓	x	x	x	x	x
Appointment of data protection officer/information officer [38]	x	✓	✓	✓	x	x	x	✓
Supervisory authority	[39] ✓	[40] ✓	[41] ✓	[42] ✓	[43] ✓	[44] ✓	[45] ✓	[46] ✓
Remedies, enforcement and sanctions	✓	✓	✓	✓	✓	✓	✓	✓

(Tomiwa, 2020)

A seen in Table 1. while all of the countries have data protection laws, in some the laws are not yet in force. Kenya and Uganda fall into this category. Also, while some are in force, they are not fully enforced. South Africa is an example of such a country.

3. Uncertainties

It is still unclear what the effect of Brexit will be in both the short and long-term. According to reports, one of the top three sources of uncertainty for over 40% of UK businesses over the past two years was Brexit (Bloom et al., 2018). Nigeria, South Africa, Egypt, and Kenya are the African nations most dependent on trade with the UK, hence a recession in the UK would be economically detrimental to these nations. They will also experience the ambiguity that comes with having to renegotiate business deals, which might take years (Ansorg, Toni, & GIGA, 2016).Industries that depend more on trade with the EU and on migrant labor from the EU have seen higher level of uncertainty. Possible confusion, however, could make it easier for cybercriminals to exploit loopholes and lead to, for instance, a rise in new types of attacks, including social engineering scams.

4. Aid

The EU gives billions of euros to African nations, which are often used for democratization, poverty alleviation, and development promotion across the continent. In order to combat terrorism, the EU also offers military support to several nations (including Somalia and Mali).(Blazquez-lopez, 2016)

The UK's capacity to carry out its promises to aid and development will be impacted by a recession. According to early indications, the new administration would prioritize fostering commercial links over providing aid to those in need.

The EU's security policies in Africa will be affected by the UK's withdrawal from the Common Security and Defence Policy. It will have an impact on the financial support provided by the EU for the African Peace and Security Architecture, and consequently, the donors' capacity to continue providing crucial help in this area.(Ansorg et al., 2016). Defense expenditures have been drastically slashed, which will have an impact on future military operations by the EU in Africa and more budget cutbacks for AU missions (Shilaho, 2017)

5. Partnerships

In addition to commerce and investment, the UK is a significant security partner for Nigeria. The UK has played a key role in attracting attention to the Boko Haram insurgency,

which is an Islamist insurgency in Northeastern Nigeria. While negotiating its exit from the EU, there is a chance that the UK could grow preoccupied and ignore dangers to world security, such as those posed by Boko Haram. (Oriloye, 2016)

Recommendations

While African nations outside of this process need to define each of these factors, our degree of interdependence with Europe directly affects us.

The definition of all these aspects is essential for African countries, which are aside of this process, but their level of interdependence with Europe affects them directly.

Africa as a continent has to become less dependent on outside assistance. Africans like Aliko Dangote and Tony Elumelu must start looking inside to help find African solutions for African problems. We should also form Cyber security alliances and partnerships

In assessing how firms prepare for a cybersecurity threat, safeguard customer information, and detect red flags for potential identity theft, we should focus on areas including risk governance, access controls, data loss prevention, vendor management and Cyber Security capacity building.

REFERENCES

Ansorg, N., Toni, H., & GIGA. (2016). *Brexit Beyond the UK ' s Borders : What It Means for Africa Focus | AFRICA Brexit Beyond the UK ' s Borders : What It Means for Africa*. *3*(1862–3603), 0–10.

Blazquez-lopez, T. (2016). *H ow B rexit C an C hange B ritain ' s R elationship with A frica*.

Bloom, N., Bunn, P., Chen, S., Mizen, P., Smietanka, P., Thwaites, G., & Young, G. (2018). Brexit and Uncertainty: Insights from the Decision Maker Panel. *Fiscal Studies*, *39*(4), 555–580. https://doi.org/10.1111/1475-5890.12179

Oriloye, G. (2016). The impact of BREXIT on Nigeria and Africa at large. *Scholarly Journal of Science Research and Essay*, *5*(5), 105–111.

Sharf, E. (2016). Information exchanges: regulatory changes to the cyber-security industry after Brexit: Making security awareness training work. *Computer Fraud and Security*, *2016*(7), 9–12. https://doi.org/10.1016/S1361-3723(16)30052-5

Shilaho, W. K. (2017). the International Criminal Court (Icc), Impunity and the Rise of a Siege Mentality Among Kenya'S Kleptocracy. *BRAZILIAN JOURNAL OF AFRICAN STUDIES*, *2*(2448–3923), 1–223. https://doi.org/10.22456/2448-3923.75067

Stevens, T., & O'brien, K. (2019). Brexit and cyber security. *RUSI Journal*, *164*(3), 22–30. https://doi.org/10.1080/03071847.2019.1643256

Study, W. (2022). *(isc) 2 cybersecurity workforce study*.

Tomiwa, I.(2020) Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions

Version, D. (2021). *King's Research Portal*.