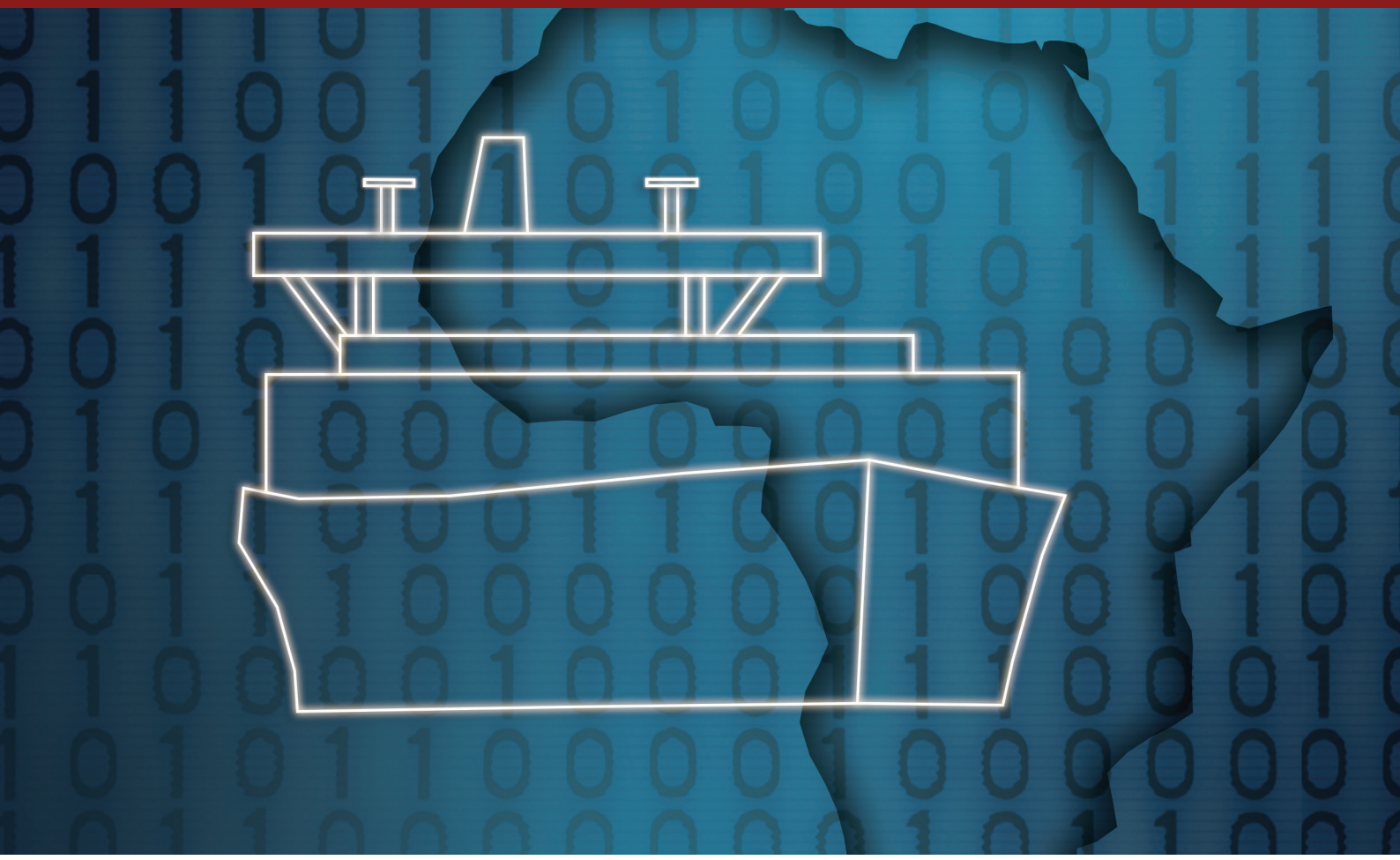
INSTITUTE FOR SECURITY STUDIES

Maritime cyber security

Getting Africa ready

Denys Reva



Africa's future development objectives are anchored in well-functioning shipping and ports industries, whose cyber security is vulnerable to breaches and disruptions caused by deliberate and indiscriminate attacks. These industries are facing a number of challenges related to efficiency and effectiveness, and their continual innovation and transformation is critical if they are to serve Africa's socio-economic needs. While cyber security is slowly becoming recognised as an important dimension of maritime security, its integration into African maritime security instruments and frameworks must be accelerated.

Key findings

- The shipping and ports industries are undergoing rapid digital transformation, as new technology improves their efficiency and effectiveness.
- New technology presents new opportunities, and new threats, given the increasing number of cyber security incidents that are affecting ports and ships across the world.
- Maritime cyber security risks vary in terms of their potential impact, but evidence suggests that an attack on a logistics hub, such as a port, could quickly disrupt a supply-chain network with tremendous financial damages extending far beyond the point of the attack.
- The digital transformation trend is currently more prevalent in developed countries, but will become more widespread as technology is becoming cheaper and more accessible. This may lead to an increase of cyber incidents in developing countries in the future.
- There is a lack of Africa-specific research and knowledge on maritime cyber security. However Africa is in an advantageous position to learn from external experiences to mitigate future maritime cyber threats and address vulnerabilities.
- Cyber security, including in the maritime space, cannot be achieved in isolation, and the African Union and regional economic communities have a central role to play regarding adoption and harmonisation of national policies and laws.
- Most African states are not yet dedicating sufficient resources to address current and future cyber security challenges.

Recommendations

At the state level:

- African Union member states need to sign and ratify the AU Malabo Convention, as cyber security depends on collective security and capacity to deal with risks and threats.
- African states need to adopt relevant national laws. Adopting some of the Malabo Convention's key points could be the first step.
- African governments need to follow best practices with regards to ensuring the cyber security and safety of their port infrastructure, and ensure compliance with the latest International Maritime Organization guidelines for cyber security for vessels.
- African governments need to work together with local owners and operators of ports and vessels to effectively respond to maritime cyber security challenges.

At the AU and RECs level:

- More research is required to address a crucial gap caused by the lack of African-centric research on maritime cyber security.
- The African Union (AU) must launch an intensive advocacy campaign to create awareness, promote ratification and build capacity for the implementation of the Malabo Convention among member states.
- Cyber security needs to be integrated into AU and Regional Economic Community maritime security frameworks, particularly as part of the African Peace and Security Architecture roadmap from 2021 onwards, and as part of the 2050 Africa's Integrated Maritime Strategy review process.

Introduction

Ports, shipping companies and maritime businesses are now integrating new innovative technological solutions at a greater rate, including automation, big data and the internet of things. Greater reliance on these technologies leads to enhanced operational efficiency, improved effectiveness and increased profitability for the shipping and ports industries.

But with this digital transformation come new threats that can undermine the effective functioning of these systems. The severity of such cyber security incidents, like data breach, malware attacks and hacking, can range from negatively affecting a workplace to potentially disrupting entire supply chains. There is a growing realisation among businesses and governments of the need to develop resilience and appropriate measures to respond to insecurities in the cyberspace.

While most maritime cyber security incidents have so far not targeted African maritime actors, available evidence from elsewhere in the world can provide valuable lessons for African decision makers.

Most African trade is seaborne, and due to the highly interconnected and networked nature of African and international economies and transport systems, the impact of maritime cyber security threats may have a devastating effect on the stability and well-being of African states.

> Ports and shipping sectors are set to become completely dependent on information technology in the future

The strategic importance of cyber security for Africa's development and security agendas is recognised in both the African Union's (AU) Agenda 2063 and African Peace and Security Architecture.[1]

This report aims to raise awareness among African decision makers about the current trend regarding the emerging nexus between cyber and maritime security. In doing so it strives to contribute to a nascent discourse on the relationship between cyber and maritime security in Africa and address a crucial gap caused by the lack of African-centric research on maritime cyber security.

The report begins by looking at current trends regarding the integration of information and communication technologies in the maritime sector, as Africa's future development objectives are anchored in the well-functioning shipping and ports industries that are vulnerable to attacks by cyber criminals.

The second part looks at some examples of cyber security incidents involving ships and ports across the world to discuss the nature of maritime cyber security. This section illustrates the scope of challenges and potential effects that such incidents may have in Africa.

The final section looks at current discussions surrounding cyber security in Africa in a maritime context. The section examines existing cyber security policies and instruments on the continental and regional levels to underpin recommendations for African decision makers.

Meeting Africa's development goals

Information technology is increasingly becoming part of the maritime space, and the ports and shipping sectors are set to become completely dependent on it in the future.[2] The process broadly refers to incorporation of automation, artificial intelligence, big data, the internet of things and blockchain technology to enhance operational efficiency, improve effectiveness and increase profitability in the maritime sector.[3]

Greater integration of new technology results in improved safety and security, better optimised and streamlined management, and allows for better planning.[4] For example automation could enhance competitiveness for ports, with programmed equipment like automated cranes, traffic control and power management systems improving the efficiency of day-to-day operations.

Big data technologies and the internet of things allow the shipping and ports sectors to improve efficiency of logistics by collecting and using relevant data through tracking and analysing the location and movement of goods and ships.[5] Information technology allows companies to manage and monitor their operations more effectively, and to better use real-time data to save time, improve efficiency and optimise costs.[6]

These new information and communication technologies facilitate a transition into a new environment or ecosystem that exists in cyberspace, defined by increased interconnectedness between all the entities within this space.[7]

This environment by its networked nature exposes ports and ships to new risks and vulnerabilities, like malware attacks disrupting industrial control systems, or hackers obtaining personal data by exploiting software vulnerabilities, among others.

The process of integrating information and communication technologies into the shipping and ports sectors has so far been more prevalent in developed countries, as new technologies are costly. Developed countries were also the first to encounter problems related to cyber security in the maritime space.

As maritime technological solutions are becoming cheaper and more accessible, they will play an ever-increasing role within the maritime sector across the world, including in Africa.[8] This makes maritime cyber security crucial for Africa.

> The socio-economic role of the shipping and ports industries is set to increase due to a number of ongoing trends in Africa

Africa relies on seaborne trade, as an estimated 90% of all African trade is conducted by sea, mostly via 90 major ports.[9] Africa's large ports often serve entire regional markets and the national economic interests of neighbouring states, as 16 of the continent's 55 states are landlocked. For example South African ports and especially the Port of Durban are central to the economy of the whole Southern African region.[10]

The socio-economic role of the shipping and ports industries is set to increase in the future due to a number of ongoing trends in Africa. Firstly, port infrastructure and security will be critical to Africa's human security as population growth rates rise. The African population is set to double by 2050, crossing the two billion people mark by 2040.[11]

The coastal population, historically low compared to the inland population, is expected to triple, putting coastal communities under immense pressure.[12] The increase in population will be accompanied by an increased pressure on port infrastructure, with higher volumes of cargo and people to transport and process.

The ports and shipping sectors will be central to Africa's food security, given that demographic trends coincide with negative climate projections, with a decrease in agricultural output in Africa in the next 30 years. One assessment suggests that overall crop yields could fall by up to 20% across Africa by 2050.[13]

Meanwhile the United Nations Food and Agriculture Organization estimates that food production may need to increase by up to 70% by 2050 to respond to the increase in populations worldwide, with Africa being among the regions with the highest expected population growth.[14]

90%

OF ALL AFRICAN TRADE IS SEABORNE

Secondly, maritime transport infrastructure and security will be crucial for Africa's future economic security and prosperity. African states have taken big steps towards establishing a common market, which necessitates greater economic and social integration, which requires a well-functioning transport system. In 2019, the African Continental Free Trade Agreement (AfCFTA) entered into force, signed by 44 states and ratified by 22.

According to the World Bank, the AfCFTA could significantly boost intra-African and international trade, and lift approximately 90 million people out of extreme and moderate poverty in the next 15 years. The study emphasises the importance of well-functioning and efficient maritime transport and port infrastructure for achieving the AfCFTA's full potential, especially for landlocked states dependent on coastal countries for import and export.[15]

Finally, the importance of cyber security must be seen against the backdrop of efforts to address the negative socio-economic effects of COVID-19 on Africa. The economic toll and costs of recovery will seriously impede and set back the progress of African states towards achieving the objectives of the Sustainable Development Goals and the African Union's (AU's) Agenda 2063.[16]

Against the backdrop of this socio-economic impact, non-traditional and broader challenges, like cyber security, may now receive less attention in Africa due to scarcity of resources. A cyber security incident, for instance in the maritime space, may put additional pressure on the already fragile economic and human security.

It's estimated that it could take African countries up to 10 years to recover from the socio-economic impact of COVID-19.[17] This context places shipping and ports at the core of Africa's economic growth, human security and post-COVID-19 recovery, given the centrality of ports and shipping for African economies.

African ports have traditionally performed at less than optimal levels of efficiency, struggling with frequent delays and backlogs, due to lengthy trade procedure times and insufficient or degrading port infrastructure. A 2018 report by the United Nations Conference on Trade and Development, assessing port efficiency in sub-Saharan Africa, argues that dwell time in African ports is abnormally long, with an average cargo spending 14 to 16 days in the port.[18]

Long dwell times result in higher costs of export and import to and from African ports that negatively affect Africa's ability to grow and develop, and undermine job creation and poverty alleviation efforts. Costs are on average three times higher than in other regions of the world.

For example in 2014 the AU Specialized Technical Committee on Transport noted that 'average container export and import costs in Africa, excluding North Africa, were reported to be US$ 2 201 and US$ 2 931 [for export and import respectively]. The equivalent costs in East Asia and Pacific over the same period, amounted to US$ 868 and US$ 902 respectively.'[19]

Existing and future African ports must improve both capacity and efficiency as soon as possible to achieve the developmental aspirations expressed in Agenda 2063. There are many possible solutions to the effectiveness and efficiency of port infrastructure that a country can pursue, and challenges are not the same across all African states.

Current international trends suggest that to meet Africa's development objectives and to maintain competitiveness, African ports and shipping companies will have to increase their reliance on information and communication technologies in the future.

Cyber-attacks are on the rise, targeting crucial infrastructure and organisations

This convergence between operation and control systems and the information technologies in the maritime space requires us to change the way we think about threats, risks and vulnerabilities, as well as actors and perpetrators of crime.[20]

As a consequence of similar processes taking place in other sectors, the number of overall cyber-attacks is on the rise, targeting crucial infrastructure and important organisations, including nuclear arsenals being targeted by hackers.[21] Another notable example includes an alleged data-theft incident at the AU headquarters.[22] Cyberspace is a dynamic environment, and threats and risks that exist within this ecosystem are constantly evolving and changing.[23]

The technological evolution within the maritime space has been slow and often reactive, as the return on investment for companies usually takes a long time.[24] As the digital transformation within the ports and shipping industries has been gradual over time, the sector has been slow to recognise the safety and security implications attached to the cyber environment.[25]

A direct consequence of the slow response to the changing ecosystem from within the maritime sector has been the increase in cyber incidents involving seaports and vessels. And as the African shipping and port industries increasingly integrate into the cyber environment, they need to prepare for the new security and threat landscape, so they can be resilient to future cyber threats. Given the growing reliance on, and integration of, information technology into maritime activities, an African maritime cyber incident is not a question of if, but when.[26]

This requires Africa's shipping and ports industries to begin planning on how to improve cyber security, which offers an opportunity to improve Africa's maritime transport and port efficiency more broadly, and in line with current continental needs. Implementing information and communication technologies in line with current requirements of the cyber security environment has the potential to make the ports more efficient, safer and more resilient to cyber-attacks.

Cyber and maritime security

In 2019 there were 310 reported cyber-attacks on ships and ports – a big increase from the estimated 120 attacks in 2018, and 50 in 2017. In 2020, the number of cases is expected to exceed 500.[27]

It is probable that the number of cyber incidents is drastically under-reported due to potential reputational risks or insurance problems, which further underscores the significance of cyber security in the maritime space.[28]

Some examples of incidents include cyber-attacks by hackers and viruses, potentially disrupting operation of the port, and criminals exploiting vulnerabilities in the system. As the number of cyber-attacks has soared over the past decade, and is expected to increase, the challenge that cyber insecurities carry for the maritime sector, and by extension countries and even whole regions, has gradually been recognised worldwide.

The emerging nexus between maritime and cyber security is captured in the latest report of the European Union Agency for Cybersecurity. This is a special agency established by the European Union in 2004, dedicated to responding to cyber security threats, including maritime cyber security.

> Due to the nature of cyberspace no entity can be fully protected against a cyber incident

The report provides a useful taxonomy of seven cyber threats to maritime security in terms of impact, with a specific focus on ports.[29] These include eavesdropping, interception and hijacking, nefarious activity and abuse, disaster, system outage, unintentional damage, physical attack, and failures and malfunctions.

These incidents cover a wide scope of activities, from terrorism and sabotage to identity theft, disruptions caused by natural disasters that result in port paralysis, systems destruction, illicit trafficking, theft of cargo and data, and environmental disasters.

There are numerous practical examples that illustrate the scope of the challenge. For instance, the ports of San Diego and Long Beach in the United States were hit with ransomware attacks, causing disruptions to their operations.[30] Similarly, criminals targeted port servers and systems at the Port of Barcelona, with land operations affected by the attack.[31]

Of particular interest is the incident that occurred at one of Antwerp's port terminals in Belgium over two years, starting in 2011. A drug cartel enlisted help from hackers to monitor and control containers' movement, retrieving data on those containing drugs.

The containers were then retrieved by lorry drivers before the legitimate owners. The scale of the operation illustrates some of the vulnerabilities to corruption that may be exploited by criminals within the cyberspace.[32]

Most attacks are directed at exploiting vulnerabilities contained within the system, most commonly resulting in financial and reputational losses for the company, and may lead to a system outage on shore.[33] In that regard, cyber security threats are partly similar to piracy, as they are primarily opportunistic in nature.

Due to the nature of cyberspace no entity can be said to be fully protected against a cyber incident, but safety and security risks to companies, entities and workers are different for each individual attack.[34] A recent cyber security survey by IHS Markit and BIMCO confirmed that 77% of respondents perceived cyber-attacks as a high or medium risk to their organisation.[35]

However, in the same survey only 8% of respondents reported experiencing a system outage on board the vessel as the result of an attack, and most such incidents were localised when a specific entity like a ship was being targeted.[36]

The impact of cyber threats may sometimes extend far beyond a particular vessel, a port facility, or even a country. The University of Cambridge's Centre for Risk Studies found that an attack targeting cargo database logs at major ports in the Asia-Pacific region could result in $110 billion in damages.

It estimated that an event of such magnitude could have a devastating impact on countries and companies connected to the target, yet weren't the intended victim – in other words the collateral damage of a cyber-attack can be huge.[37]

> An attack on a port could quickly disrupt a supply chain network with tremendous financial damages extending far beyond the point of the attack

Arguably the most well-known attack that supports these estimates took place in 2017, when a cyber-attack initially targeting a Ukrainian software company ended up infecting and corrupting the whole computer network at the headquarters of the world's biggest shipping line, Maersk. The attack shut down the operations of the office for almost two weeks and caused approximately US$300 million in collateral damages to Maersk.[38] As a result, Rotterdam's fully automated port terminal was shut down for over a week.[39]

A similar incident occurred again in April 2020, when the data centres of the Mediterranean Shipping Company (MSC), a global shipping and logistics company, were targeted in a malware attack. The incident was quickly resolved with minimal loses for the MSC, but a targeted attack of this nature could have had a far more devastating impact.[40]

An attack on a logistic hub, such as a port, could quickly disrupt a supply-chain network with tremendous financial damages extending far beyond the point of the attack. A port system is especially vulnerable, as it can involve a number of stakeholders in port operations, from shipping to logistics, and other companies who are interconnected and interdependent. Each stakeholder represents a potential point of entry for criminals, increasing the possibility of a successful disruption.[41]

The shipping and ports industries extensively rely on external suppliers and vendors for maintenance and cyber security, as their infrastructure

ACCORDING TO A SURVEY,

77%

OF RESPONDENTS PERCEIVE CYBER-ATTACKS AS A HIGH OR MEDIUM RISK TO THEIR ORGANISATION

is becoming progressively more connected with information and communication technology systems.[42] An inability to timeously update and replace hardware and software due to COVID-19 has resulted in a 400% spike in cyber security incidents targeting ports and ships between February and May 2020.[43]

It therefore becomes increasingly difficult for any entity to protect against cyber-attacks or other incidents. The interconnected nature of cyber security requires a collective approach based on cooperation and harmonisation of responses and common standards.

Attainment of enhanced cyber security is now being sought through institutions at the international and regional level. The problems related to maritime cyber security started getting international attention relatively recently, with the first edition of BIMCO Guidelines on Cyber Security Onboard Ships published in 2016.[44]

The International Maritime Organization (IMO) has a central role to play, adopting the Maritime Cyber Risk Management in Safety Management Systems (MSC.428(98)) in 2017. The resolution requires shipowners and managers to include cyber risk management into their Safety Management Systems under the International Safety Management Code by 1 January 2021.[45]

> The nature of cyber security requires a collective approach based on cooperation and harmonisation of responses and common standards

In support of the resolution, the IMO has published guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) referring to best practices and guidelines on cyber security.[46] This is the first international attempt to set minimal international standards for vessels in line with safe practices for ship operation, raising awareness about cyber security risks and threats.

Countries such as the United States and Singapore have recognised and directed significant attention to the maritime dimension of cyber security.[47] Other countries pursue closer regional cooperation on cyber security, which could be seen as an important step towards improved maritime cyber security.

For instance, in South-East Asia the Association of Southeast Asian Nations established a new cyber security cooperation agreement that includes a focus on advancing partnership and increasing cooperation and information sharing between member states for common cyber security.[48]

The EU embraced maritime cyber security as part of a holistic approach to acquiring overall cyber security. Through the European Union Agency for Cybersecurity, the EU facilitates cross-border cooperation, policy standardisation and capacity building among member states with regard to cyber security. The agency covers a number of aspects related to

CYBER SECURITY INCIDENTS INCREASED BY

400%

SINCE FEBRUARY 2020

cyber security, including maritime transport and ports cyber security.[49]

The EU Directive on security of networks and information systems (2016) underscores the importance of a holistic and collective approach to the protection of critical infrastructure, including water transport and ports, from a national and international level.[50] Due to the interconnected nature of cyberspace, harmonisation of policies and approaches on a regional level leads to improved collective security, which then improves national cyber security.

Improving Africa's cyber responses

African policymakers need to pay attention to the functions and results of these approaches and determine what can be learnt to best suit the African context, given current developments on the continent.

The potential risks related to cyber security and cyberspace are well recognised by the AU and Africa's Regional Economic Communities (RECs), who have adopted numerous critical instruments defining the scope, nature and parameters of cyber-related risks and vulnerabilities.

At the regional level, the Economic Community of West African States (ECOWAS) has developed a directive (C/DIR.1/08/11) on fighting cybercrime within ECOWAS in 2011.[51] In the same year, the Common Market for Eastern and Southern Africa adopted a model cybercrime bill.[52] This was followed by the Model Law on Computer Crime and Cybercrime adopted by the Southern African Development Community in 2012.[53]

On the continental level, the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) was adopted in 2014.[54] The convention strives to harmonise cyber laws across Africa, and encourages the states to develop cyber security governance mechanisms.

In 2018, at the recommendation of the Specialized Technical Committee on Communication and ICT, the AU Executive Council included cyber security as one of the flagship projects of Agenda 2063, recognising the increasingly important role it will play in achieving African development aspirations.[55]

In December 2019 the AU further convened the inaugural meeting of the AU Cyber Security Expert Group, comprising volunteer experts from across Africa.[56] The group is expected to meet at least once a year to advise the AU Commission on the latest cyber security issues and policies. This is a good indication that the recognition of cybercrime within the African Peace and Security Architecture as a strategic security issue for African Union member states has started to be taken very seriously.[57]

Progress regarding ratification and implementation has been slow. The Malabo Convention has been signed by only 14 countries, and ratified by only eight since 2014. AU member states lag behind regarding efforts to approve required legislature and create the necessary frameworks in line with the requirements contained in the Malabo Convention. In 2015, the AU Commission surveyed 35 African countries to determine the state of cybercrime legislation and existent mechanisms to deal with incidents.

Out of 35 countries, only 11 had cybercrime laws, 13 had a Computer Emergency Response Team or Computer Security Incident Response Teams, eight had a dedicated national strategy on cyber security and 14 had personal data protection laws.[58] The situation has been gradually improving over time – to date 25 out of 55 countries have developed personal data protection laws.[59] However, as noted by the recent AU Agenda 2063 Progress Report, the change has been gradual and slow.[60]

> Only 14 countries have signed and only eight have ratified the Malabo Convention since 2014

The implication of these challenges is underscored by the Global Cybersecurity Index, published by the International Telecommunication Union in 2018. The report ranks countries based on their perceived level of commitment to cyber security. The report indicates that only four out of 54 top-scoring countries are from Africa, namely Mauritius (14th), Egypt (23rd), Kenya (44th) and Rwanda (49th).

The two biggest African economies, Nigeria and South Africa, were ranked 57th and 56th out of 175 countries respectively.[61] Similarly, the National Cyber Security Index, which evaluates the degree to which a country is ready to prevent and manage cyber incidents, rates Nigeria as the highest ranking in Africa (45th out of 160

countries), with Kenya, Egypt and South Africa ranked 76th, 77th and 99th respectively.[62]

Both indices point to an apparent deficit of cyber stability, with the latter understood as everyone's general ability to 'use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner.'[63]

At the state level, it generally refers to a state's responsibility to protect its infrastructure through legal policy and regulatory measures.[64] In other words, the indices point to a disparity that exists in Africa between the resources allocated to ensure cyber security and stability, and the ever-increasing level of cyber threats Africa faces.[65]

This is especially pertinent in the context of potential significant damages that may be caused by a cyber-attack on one of Africa's maritime logistic hubs, by analogy with the 2017 Maersk attack.

> Cyber security needs to be better integrated into African maritime security instruments and frameworks

As the international focus on the nexus between cyber and maritime security has emerged relatively recently, cyber security is insufficiently reflected in both 2050 Africa's Integrated Maritime Strategy and the African Charter on Maritime Security, Safety and Development in Africa (Lomé Charter) of 2016.

The maritime aspects of cyber security are also neither directly reflected in the Malabo Convention nor in other relevant regional cyber security instruments.

The latter is in line with best international practices, as maritime infrastructure, together with other types of critical infrastructure, is covered by the general provisions of these instruments. Employing a broad definition ensures that the legislation keeps abreast of the evolving nature of technology and is not rendered obsolete.[66]

Nevertheless, it is critical for member states, through the AU and RECs, to re-evaluate existing instruments and frameworks in light of the latest international developments, and assess risks and develop appropriate mechanisms to respond to maritime cyber threats.

African policymakers must ensure that the integration of information technology into the maritime operations of ports, shipping and connected infrastructure goes hand in hand with improvements in their cyber security.

Africa has a good opportunity to learn from, develop responses to and to avoid dangerous pitfalls brought about by the cyber environment. The crucial objective of ensuring the cyber security of maritime infrastructure from attacks and disruptions falls under the purview of African multilateral organisations, especially the AU and RECs, as well as African port management associations.

Conclusions

Cyber security needs to be better recognised as an important dimension of maritime security, and should be integrated into African maritime security instruments and frameworks. Similarly, as information technologies are increasingly integrated into all aspects of human life, greater attention should be given specifically to the maritime aspects of cyber security, as the nature of maritime sector requires a nuanced approach.

The interconnectivity brought about by the cyber space makes every African state vulnerable and dependent on collective cyber security. An attack of scale similar to the 2017 Maersk incident would have a devastating impact on Africa's regional and continental stability and prosperity, rooted in growing interdependence and reliance on the maritime trade.

Considerably greater efforts and attention need to be directed towards ensuring Africa's cyber security. For that end, and given the prevalence of non-African evidence on maritime cyber security incidents, increased Africa-specific research and knowledge is required.

African states need to work closely with the private sector, to share knowledge and understanding regarding specific problems the industry faces. The AU needs to institutionalise member states' responses to these types of security risks, and raise awareness about the cyber threats and vulnerability regarding the maritime domain.

Recommendations

At the AU and REC level:

- There is a lack of Africa-specific research and knowledge on maritime cyber security. More research is needed that can lead to concrete provisions for the establishment of the necessary administrative and implementation infrastructure and institutions on the continental and regional levels. Like the survey that the AU Commission conducted with Symantec in 2015, the AU can partner with private institutions to conduct the assessment, including African professional associations and networks.
- The AU must launch an intensive advocacy campaign to create awareness about the Malabo Convention. The AU should promote ratification and build capacity for the implementation of the Malabo Convention among member states.
- There is a need to conduct further research on possible consequences of a disruptive cyber incident involving Africa's maritime port and transport infrastructure, and prepare appropriate response mechanisms on the continental and regional levels.
- Cyber security needs to be integrated into AU and REC maritime security frameworks, particularly as part of the African Peace and Security Architecture roadmap from 2021 onwards. It could for example be the subject of a regular report to the AU Peace and Security Council. Cyber security should be integrated as part of 2050 Africa's Integrated Maritime Strategy review process, addressing among other issues the ports and shipping industries in Africa.
- The AU and RECs should engage in extensive public consultations with high-level stakeholders to facilitate virtual capacity-building meetings between relevant officials to create a common approach to securing African maritime industries from cyber-attacks.

At the state level:

- Cyber security depends on collective security and capacity to deal with risks and threats. Member states need to sign and ratify the Malabo Convention, and increase efforts to create the legal and administrative framework it envisions.
- African governments should become actively involved with regional maritime and cyber security institutions. Given the interconnected nature of many regions, including through trade and infrastructure, African states should pursue a regional approach to cyber maritime security.
- Member states that still have not done so need to adopt relevant laws and create relevant mechanisms to respond to cyber security threats and risks, in line with international best practices.
- African governments need to follow best practices with regard to ensuring the cyber security and safety of their port infrastructure, and ensure compliance with the latest IMO guidelines for cyber security for vessels.
- African governments need to work together with local stakeholders, owners and operators of ports and vessels to understand the real cyber risks they face, and the specific mitigations that would overcome them.

Acknowledgements

The author is grateful to all respondents, who generously gave their time to review this report, for their useful insights, comments and feedback. Their contributions have greatly strengthened the content of the report.

Notes

1 African Union, Flagship Projects of Agenda 2063, https://au.int/en/agenda2063/flagship-projects, accessed 11 September 2020. See also African Union Commission, African Peace and Security Architecture: APSA Roadmap 2016–2020, 2015, https://au.int/sites/default/files/documents/38310-doc-9_2015-en-apsa-roadmap-final.pdf, accessed 11 September 2020.

2 M Mylly, ICT in Maritime Transport Chain – Unleashing Potential for the Future, www.seafocus.fi/ict-in-maritime-transport-chain, 16 June 2016, accessed 11 September 2020.

3 More specifically, the process refers to growing convergence between information and communications technology and operational technology, as systems responsible for critical operational processes in ports and on board vessels that were previously siloed are now being increasingly connected to broader networks. Some examples may include electronic access control systems, automated cranes in ports, and power management systems on board a vessel. As a result, vessels and ports become dependent on the effectiveness and functioning of these systems. See for instance T Seals, CEOs Could Be Held Personally Liable for Cyberattacks that Kill, *Threat Post*, https://threatpost.com/ceos-personally-liable-cyberattacks-kill/158990, 7 September 2020, accessed 11 September 2020. See also DNV GL, Maritime Cyber Security, www.dnvgl.com/maritime/insights/topics/maritime-cyber-security/index.html, accessed 11 September 2020.

4 Port Technology, What is a Smart Port?, www.porttechnology.org/news/what-is-a-smart-port/, 9 August 2019, accessed 11 September 2020.

5 'Internet of things' refers to the connectivity between objects or sensors that enable objects to be linked into a network. See for instance R Karimpour and M Karimpour, Digitalisation and ICT innovations – A focus on port logistics, www.docksthefuture.eu/digitalisation-and-ict-innovations-a-focus-on-port-logistics/, 21 May 2018, accessed 11 September 2020.

6 M Mylly, ICT in Maritime Transport Chain – Unleashing Potential for the Future, www.seafocus.fi/ict-in-maritime-transport-chain, 16 June 2016, accessed 11 September 2020.

7 National Institute of Standards and Technology, cyberspace, https://csrc.nist.gov/glossary/term/cyberspace, accessed 11 September 2020.

8 M Mylly, ICT in Maritime Transport Chain – Unleashing Potential for the Future, www.seafocus.fi/ict-in-maritime-transport-chain, 16 June 2016, accessed 11 September 2020.

9 Export-Import Bank of India, Connecting Africa: Role of Transport Infrastructure, Working Paper No. 72, www.tralac.org/images/docs/12896/connecting-africa-role-of-transport-infrastructure-exim-bank-working-paper-march-2018.pdf, 10–11, March 2018, accessed 11 September 2020.

10 SG Nabee and J Walters, Liner shipping cascading effect on Southern African Development Community port strategies, *Journal of Transport and Supply Chain Management*, 12, https://jtscm.co.za/index.php/jtscm/article/view/394, 2008, accessed 11 September 2020.

11 J Cilliers, Getting to Africa's demographic dividend, *Institute for Security Studies*, https://issafrica.s3.amazonaws.com/site/uploads/ar13-2.pdf, August 2018, accessed 11 September 2020.

12 J-L Merkens, L Reimann, J Hinkel and A Vafeidis, Gridded population projections for the coastal zone under the Shared Socioeconomic Pathways, *Global and Planetary Change*, 145, www.sciencedirect.com/science/article/pii/S0921818116301473, October 2016.

13 J Cairns, J Hellin, K Sonder, J Araus, J MacRobert, C Thierfelder and B Prasanna, Adapting maize production to climate change in sub-Saharan Africa, *Food Security*, 5, https://link.springer.com/article/10.1007/s12571-013-0256-x 2013.

14 Food and Agriculture Organization, How to Feed the World in 2050, 2, www.fao.org/fileadmin/templates/wsfs/docs/expert_paper/How_to_Feed_the_World_in_2050.pdf, accessed 11 September 2020.

15 World Bank Group, The African Continental Free Trade Area: Economic and Distributional Effects, 2020, 121–122, https://openknowledge.worldbank.org/bitstream/handle/10986/34139/9781464815591.pdf?sequence=2&isAllowed=y, accessed 11 September 2020.

16 United Nations Economic Commission for Africa, Facilitating Cross-Border Trade Through a Coordinated African Response to COVID-19, 6, www.uneca.org/sites/default/files/PublicationFiles/facilitating_cross-border_trade_through_a_coordinated_african_response_to_covid-19_fin_4aug.pdf, 2020, accessed 11 September 2020.

17 J Cilliers, M Oosthuizen, S Kwasi, K Alexander, TK Pooe, K Yeboua and J Moyer, Exploring the impact of COVID-19 in Africa: a scenario analysis to 2030, *Institute for Security Studies*, https://issafrica.org/events/how-will-covid-19-change-africa, 25 June 2020, accessed 11 September 2020.

18 G Raballand, S Refas, M Beuran and G Isik, Why Does Cargo Spend Weeks in Sub-Saharan African Ports? Lessons from Six Countries, 4, https://unctad.org/meetings/en/Contribution/dtltlbts-AhEM2018d3_WorldBank_en.pdf, 2012, accessed 11 September 2020.

19 African Union, Maritime Transport; Increasing African Ports Capacity and Efficiency for Economic Growth, 3, https://au.int/sites/default/files/documents/32186-doc-maritime_transport_increasing_african_ports_capacity_and_efficiency_for_economic_growth-e.pdf, 2017, accessed 11 September 2020.

20 The US Department of Commerce provides useful definitions for a cyber security threat, risk, vulnerability and incident: a threat is any 'circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability'; a risk is the 'level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring'; a vulnerability is a '[w]eakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source', and; an incident is an 'occurrence that actually or potentially jeopardizes the

confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies'. See United States of America, Federal Information Processing Standards Publication, Minimum Security Requirements for Federal Information and Information Systems, https://csrc.nist.gov/csrc/media/publications/fips/200/final/documents/fips-200-final-march.pdf, March 2006, accessed 11 September 2020.

21 B Farmer, Cyber attacks on nuclear arsenals 'could lead to inadvertent launches', think tank warns, *The Telegraph*, www.telegraph.co.uk/news/2018/01/11/cyber-attacks-nuclear-arsenals-could-lead-inadvertent-launches/, 11 January 2018, accessed 11 September 2020.

22 J Sherman, What's the deal with Huawei and a hack at African Union headquarters?, *Medium*, https://medium.com/dukeuniversity/whats-the-deal-with-huawei-and-a-hack-at-african-union-headquarters-1e454c1f31a2, 31 May 2019, accessed 11 September 2020.

23 N Ismail, Protecting the cyber environment from changing threats, *Information Age*, www.information-age.com/protecting-cyber-environment-123470483/#:~:text=The%20cyber%20environment%20is%20a,every%20single%20day%2C%20every%20minute, 22 January 2018, accessed 11 September 2020.

24 W Owen, Posidonia experts expecting change, *LNG Industry*, www.lngindustry.com/liquid-natural-gas/07062018/posidonia-experts-expecting-change/, 7 June 2018, accessed 11 September 2020.

25 R Hopcraft and K Martin, Effective maritime cybersecurity regulation – the case for a cyber code, *Journal of the Indian Ocean Region*, 14:3, www.researchgate.net/publication/327588589_Effective_maritime_cybersecurity_regulation_-_the_case_for_a_cyber_code, 2018.

26 C Kapalidis, Maritime Cyber Security: No Substitute for Testing, *Chatham House*, www.chathamhouse.org/expert/comment/maritime-cyber-security-no-substitute-testing#, 12 October 2017, accessed 11 September 2020.

27 Handy Shipping Guide, As Maritime Cyber-Attacks Proliferate International Ports Warned They Are Particularly Vulnerable, www.handyshippingguide.com/shipping-news/as-maritime-cyberattacks-proliferate-international-ports-warned-they-are-particularly-vulnerable_13084, 20 July 2020, accessed 11 September 2020.

28 Safety4Sea, Why underreporting is a major cyber threat in the shipping industry, https://safety4sea.com/why-underreporting-is-a-major-cyber-threat-in-the-shipping-industry/, 2019, accessed 11 September 2020.

29 European Union Agency for Cybersecurity, Port Cybersecurity – Good practices for cybersecurity in the maritime sector, 27, www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector, 26 November 2019, accessed 11 September 2020.

30 A Ng, Ransomware attack hits Port of San Diego, *CNET*, www.cnet.com/news/port-of-san-diego-hit-with-disruptive-ransomware-attack/, 28 September 2018, accessed 11 September 2020. See also M Nero, Long Beach Port terminal hit by ransomware attack, *Press-Telegram*, www.presstelegram.com/2018/07/24/long-beach-port-terminal-hit-by-ransomware-attack/, 24 July 2018, accessed 11 September 2020.

31 C Cimpanu, Port of San Diego suffers cyber-attack, second port in a week after Barcelona, *Zero Day*, www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/, 27 September 2018, accessed 11 September 2020.

32 T Bateman, Police warning after drug traffickers' cyber-attack, *BBC*, www.bbc.com/news/world-europe-24539417, 16 October 2013, accessed 11 September 2020.

33 IHS Markit, Safety at Sea and BIMCO cyber security white paper, https://cdn.ihsmarkit.com/www/pdf/1019/Safety-at-Sea-and-bimco-cyber-security-white-paper.pdf, 2019, accessed 11 September 2020.

34 L Graham, The new face of piracy: cyber crime is threatening the shipping industry, *City A.M.*, www.cityam.com/new-face-piracy-cyber-crime-threatening-shipping-industry/, 26 November 2018, accessed 11 September 2020.

35 S Cousins, COVID-19 cyber concerns: cyber attacks increase during the pandemic, *Safety at Sea*, 54:620, 2020, 18.

36 T Blake, Overview of Maritime Cyber Security, Presentation at the Cyber Security Webinar: Creating cyber risk plans to meet the IMO 2021 deadline, https://safetyatsea.net/cyber-security/, 6 August 2020, accessed 11 September 2020.

37 Cambridge Centre for Risk Studies, Shen Attack: Cyber risk in Asia Pacific ports, www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/shen-attack-cyber-risk-in-asia-pacific-ports, 2019, accessed 11 September 2020.

38 A Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, *Wired*, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, 22 August 2018, accessed 11 September 2020.

39 Ibid.

40 Mediterranean Shipping Company, Network Outage Resolved, www.msc.com/zaf/news/2020-april/network-outage-resolved, 15 April 2020, accessed 11 September 2020.

41 World Economic Forum, Understanding Systemic Cyber Risk, 11–12, www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf, October 2016, accessed 11 September 2020.

42 L O'Donnell, RSA Conference 2019: Operational Technology Widens Supply Chain Attack Surfaces, *Threat Post*, https://threatpost.com/rsa-operational-technology-supply-chain/142587/, 8 March 2019, accessed 11 September 2020.

43 J Ovcina, Naval Dome: 400% increase in attempted hacks since February 2020, *Offshore Energy*, www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/, 5 June 2020, accessed 11 September 2020.

44 Since 2016 most major classification societies, for instance the International Association of Classification Societies, Lloyds Register and DNV GL, have developed cyber security and safety notations. See for instance BIMCO, The Guidelines on Cyber Security Onboard Ships, https://safety4sea.com/wp-content/uploads/2018/04/Guidelines_on_cyber_security_

onboard_ships_version_1-1_Feb20163.pdf, February 2016, accessed 11 September 2020.

45 International Maritime Organization, Maritime Cyber Risk Management in Safety Management Systems, Resolution MSC.428(98), www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428(98)%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf, 16 June 2017, accessed 11 September 2020.

46 International Maritime Organization, Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3, www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf, 5 July 2017, accessed 11 September 2020. See also: BIMCO, CLIA, ICS, INTERCARGO, InterManager, INTERTANKO, IUMI, OCIMF and World Shipping Council, The Guidelines on Cyber Security Onboard Ships: Version3, www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16, accessed 11 September 2020.

47 United States Coast Guard, Cybersecurity, www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/, accessed 11 September 2020. See also Ship Technology, MPA opens maritime cybersecurity centre, *Ship Technology*, www.ship-technology.com/news/mpa-maritime-cybersecurity-centre/, 20 May 2019, accessed 11 September 2020.

48 Association of Southeast Asian Nations, Chairman's Statement of the 34th ASEAN Summit Bangkok, www.asean2019.go.th/en/news/chairmans-statement-of-the-34th-asean-summit-bangkok-23-june-2019-advancing-partnership-for-sustainability/, 23 June 2019, accessed 11 September 2020.

49 European Union Agency for Cybersecurity, ENISA: 15 years of building cybersecurity bridges together, www.enisa.europa.eu/news/enisa-news/enisa-15-years-of-building-cybersecurity-bridges-together, 20 March 2019, accessed 11 September 2020.

50 European Union, Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://data.europa.eu/eli/dir/2016/1148/oj, 6 July 2016, accessed 11 September 2020.

51 Economic Community of West African States, Directive 1/08/11 on Fighting Cyber Crime, https://issafrica.org/ctafrica/uploads/Directive%201:08:11%20on%20Fighting%20Cyber%20Crime%20within%20ECOWAS.pdf, August 2011, accessed 11 September 2020.

52 Common Market for Eastern and Southern Africa, Official Gazette, 16, www.comesa.int/wp-content/uploads/2020/05/2011Gazette-Vol.-16.pdf, October 2011, accessed 11 September 2020.

53 Southern African Development Community, SADC Model Law on Computer Crime and Cybercrime, www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/cybercrime.pdf, 2 March 2012, accessed 11 September 2020.

54 African Union, African Union Convention on Cyber Security and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf, 2014, accessed 11 September 2020.

55 African Union, 32nd Ordinary Session of the Executive Council, https://au.int/sites/default/files/decisions/33909-ex_cl_decisions_986-1007_e.pdf, 7, accessed 11 September 2020.

56 African Union, African Union Cybersecurity Expert Group holds its first inaugural meeting, https://au.int/en/pressreleases/20191212/african-union-cybersecurity-expert-group-holds-its-first-inaugural-meeting, 12 December 2019, accessed 11 September 2020.

57 African Union, African Peace and Security Architecture: APSA Roadmap 2016–2020, 52-53, www.peaceau.org/uploads/2015-en-apsa-roadmap-final.pdf, December 2015, accessed 11 September 2020.

58 African Union Commission and Symantec, Cyber Crime & Cyber Security: Trends in Africa, www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf, accessed 11 September 2020.

59 H Lovells, Overview of data protection laws in Africa, www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2, 14 October 2019, accessed 11 September 2020.

60 African Union, Agenda 2063 Progress Report, 14, https://au.int/sites/default/files/newsevents/workingdocuments/38223-wd-progress_report_on_the_implemenation_of_agenda_2063_eng.pdf, 2020, accessed 11 September 2020.

61 International Telecommunication Union, Global Cybersecurity Index 2018, www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, 2019, accessed 11 September 2020.

62 e-Governance Academy Foundation, National Cybersecurity Index, https://ncsi.ega.ee/ncsi-index/, accessed 11 September 2020.

63 Global Commission on the Stability of Cyberspace, Advancing Cyberstability, 13, https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf, November 2019, accessed 11 September 2020.

64 U Orji, The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?, *Masaryk University Journal of Law and Technology*, 12:2, 2018.

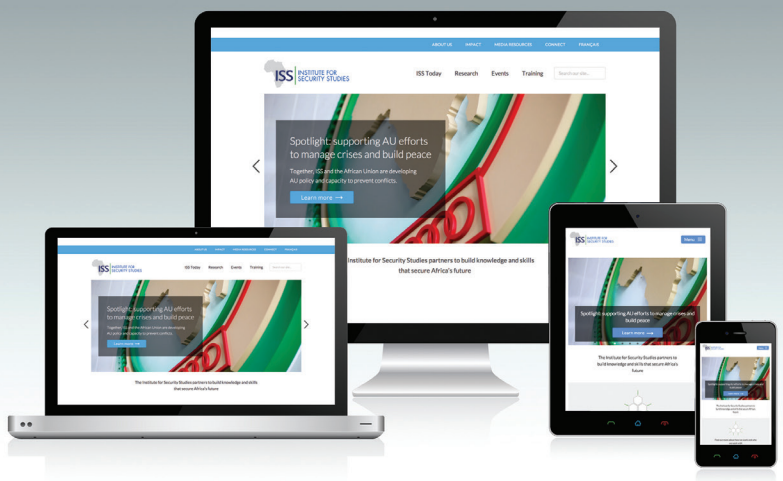
65 V Fundam, Cyber security remains the biggest threat to business in Africa, *Independent Online*, www.iol.co.za/business-report/belt-and-road/cyber-security-remains-the-biggest-threat-to-business-in-africa-32866271, 12 September 2019, accessed 11 September 2020.

66 African Union Commission and Symantec, Cyber Crime & Cyber Security: Trends in Africa, www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf, accessed 11 September 2020.

ISS | INSTITUTE FOR SECURITY STUDIES

Visit our website for the latest analysis, insight and news

The Institute for Security Studies partners to build knowledge and skills that secure Africa's future



Step 1 Go to www.issafrica.org

Step 2 Go to bottom right of the ISS home page and provide your subscription details

INSTITUTE FOR SECURITY STUDIES

About the author

Denys Reva joined the Institute for Security Studies in 2016. He is a research officer working on maritime security for the Peace Operations and Peacebuilding Programme in Pretoria. His areas of interest include international relations, maritime security and human security. He has a master's degree in security studies from the University of Pretoria.

About ISS Africa Reports

The Africa Report series analyses human security problems and solutions at the regional and continental level. It also considers the implications and lessons from Africa for global policy. Reports provide insights into African and global policy on conflict trends, conflict prevention, peacebuilding, terrorism, organised crime, peace operations, maritime security, migration, development and governance.

About the ISS

The Institute for Security Studies (ISS) partners to build knowledge and skills that secure Africa's future. The ISS is an African non-profit with offices in South Africa, Kenya, Ethiopia and Senegal. Using its networks and influence, the ISS provides timely and credible policy research, practical training and technical assistance to governments and civil society.

Development partners

This report is funded by the government of Norway. The ISS is also grateful for support from the members of the ISS Partnership Forum: the Hanns Seidel Foundation, the European Union, the Open Society Foundations and the governments of Canada, Denmark, Finland, Ireland, the Netherlands, Norway, Sweden and the USA.

ISSN 2617-7749 Print
ISSN 2617-7757 Digital