The Impact of Digital-Driven Warfare on Africa

By Anthoni van Nieuwkerk | Peer Reviewed

Abstract

Modern warfare is becoming more technological and increasingly employs advanced technologies. Advances in precision location, targeting and strike, navigation, large data transmission, weapon-system range and manoeuvrability, and the growing importance of the outer space and cyber domains are collectively altering the 'spatial dimensions' of warfare. But are these rapidly evolving technologies and their use in defence and warfare relevant to developing nations and Africa in particular? There still exist high barriers to implementation, especially in countries with weak military research and development infrastructures. This article examines these 4IR-induced shifts in warfare thinking and practice, and focuses on the implications for Africa. It also probes the options open to states to prepare for the use of digital technologies in the warfare domain, in particular drones and their application. It concludes with a number of recommendations for African security decision-makers to enhance innovative, effective, and efficient security sectors [1].

Introduction

Hypersonic weapons travel fi e or more times the speed of sound. The Indian/Russian BrahMos is currently the fastest operational supersonic missile capable of speeds around 3,700 km/h. Technologically advanced nations are scrambling to develop a deterrence against this latest threat. Clearly, modern warfare is becoming more technological and increasingly employs advanced technologies. This phenomenon shifts the nature of confli t and the international legal context within which it takes place. The fourth industrial revolution (4IR) is being shaped by a fresh wave of innovation such as Autonomous Vehicles, Smart Robotics, Materials Engineering, Big Data, the Internet of Things (IoT), and 3D Printing. Overall, the 4IR could have a dramatic impact on operational capabilities. As Bitzinger (2021) points out, advances in precision location, targeting and strike, navigation, large data transmission and discrimination, weapon-system range and manoeuvrability, and the growing importance of the outer space and cyber domains are collectively altering the 'spatial dimensions' of warfare.

But are these rapidly evolving technologies and their use in defence and warfare relevant to developing nations and Africa in particular? There still exist high barriers to implementation, especially in countries with weak military research and development infrastructures. In fact, most militaries operate in the context of the second industrial revolution.

Is digital-driven warfare relevant for Africa? A recent survey of threats facing the Southern African region (Van Nieuwkerk, 2021) notes data fraud and theft, cyber-attacks, and risks associated with fake news and identity theft. The potential vulnerability of critical technological infrastructure is also fl gged as a growing national security concern. However, given that many African militaries and national security structures suffer from capacity constraints and remain wedded to conventional warfare mindsets, how could they go about preparing and defending against such advanced technological attacks?

This article examines these 4IR-induced shifts in warfare thinking and practice, and focuses on the implications for Africa. It also probes the options open to states to prepare for the use of digital technologies in the warfare domain, in particular the implications of drones and their application and how to apply these to their benefi whilst upholding the human rights of their citizens.

The article uses secondary data sources as its main data collection method, although interviews were conducted with experts on the subject matter who provided in-depth insight. Interview requests were sent to several peace and security practitioners but few were able to elaborate on the impact of 4IR on South African and African security, which presumably speaks to a lack of focus and/or expertise regarding this area of the region and continent's defence capabilities. As a result, it is important to pay close attention to this space and identify where Africa can enhance capacity at a pace suitable for the continent. The Global South, including African countries, are not yet equipped to compete with developed nations in terms of 4IR capabilities vis a vis weapons and security apparatuses but it is in Africa's interest to develop a strategic perspective on the need for cooperation, collaboration and deployment of advanced warfare capabilities.

Global trends

The 2021 Global Risks Report of the World Economic Forum points out that Covid continues to widen inequalities and societal fragmentation. In this context, two global risk perceptions dominate current research and analysis. These are extreme weather, climate action failure, and human-led environmental damage, as well as digital power concentration, digital inequality and cybersecurity failure (WEF, 2021). Technology continues to play a profound role in shaping the global risks landscape for individuals, governments, and businesses. A previous report (WEF, 2019) identifie massive data fraud, theft and cyber-attacks as high-profile threats, and noted that risks associated with fake news and identity theft increased. The potential vulnerability of critical technological infrastructure has increasingly become a national security concern. A frequently cited risk interconnection was the pairing of cyber-attacks with critical information infrastructure breakdown (WEF, 2019).

More specificall , the United States of America, which maintains one of the most powerful armies in the world, is a good demonstration of advancements in digital-driven warfare. When he took over as US President in

2016, Donald Trump loosened the reins of the US drone programme, as he lowered the standards for who could be targeted by the programme and where. As we will note later in this article, the impact on counterterrorism operations in Africa has been severe—especially in the Horn of Africa and the Sahel. In summary, the Trump rules gave the United States the right to kill virtually anyone it designates as a terrorist threat, anywhere in the world, without regard to human rights laws prohibiting extrajudicial killing (Shamsi, 2021).

In the meantime, the Pentagon has developed a plan to promote the innovation referred to as Direct Energy Weapons (DEWs), which weaponize lasers to be used against military targets. Between 2017 and 2019, the US military significantly increased its spending on DEWs, from $535 million to $1.1 billion (Cohen, 2021).

DEW systems are also being developed by other nations, such as China and Russia. According to reports, China may have used microwaves against Indian troops in 2020 (Cohen, 2021). High-energy lasers, high-power radiofrequency or microwave devices, and charged or neutral particle beam weapons are examples of DE weapons. Both microwaves and lasers are part of the electromagnetic spectrum, including light energy and radio waves (Obering, 2020).

How do global developments impact Africa?

Africa is not spared from evolving digital threats. In July 2021, Transnet—a South African state-owned enterprise that manages the nation's rail, port, and pipeline infrastructure— reported problems with its information technology networks. The disruption affected operations in several container terminals, interrupting cargo movement. Transnet eventually confi med it had suffered a cyber-attack (Naidoo, 2021). Reva (2021) noted that following the Covid-19 pandemic, the number of cyber-attacks has been increasing worldwide and in South Africa, infli ting fina cial losses across the manufacturing, banking, and energy sectors. The recent incident was the fi st time the operational integrity of the country's critical maritime infrastructure has suffered a severe disruption (Reva, 2021).

Apart from the cyber domain, we have to point to drone warfare. Drones are formally known as unmanned aerial vehicles (UAVs) and can be described as autonomous robots, remotely controlled through software-controlled flight plans in their embedded systems, working in conjunction with onboard sensors and GPS (Lutkevich, n.d.). In addition, Underwater Unmanned Vehicles (UUVs) or Remotely Operated Vehicles (ROVs) are submersible, waterproof drones that enable users to explore marine environments remotely. The PRC seems to be at the forefront of developing this technology for military purposes (Seidel, 2020; Sutton, 2021).

Drones have long been associated with global wars, but are assuming a new role in Africa where they have played a critical role in humanitarian services such as providing medical supplies to remote areas, mapping displaced people, assisting anti-poaching rangers, and helping with precision farming (Koigi, 2019).

“Drones have long been associated with global wars, but are assuming a new role in Africa where they have played a critical role in humanitarian services such as providing medical supplies to remote areas, mapping displaced people, assisting anti-poaching rangers, and helping with precision farming (Koigi, 2019).”

However, as reported by Allen (2021), the risk of militarisation of drone technology in Africa represents a new asymmetric tool that violent nonstate groups may deploy to extend the reach of their coercion, reshaping the African battlefield

What are the challenges with drone application?

While commercial drone usage increases in Africa, with humanitarian aid agencies and agricultural institutions using UAV technology to streamline their work, the lack of standardised regulations to ensure safety and security remains a major concern (Khanyile, 2019).

In many African nations, the civil aviation authorities are struggling to ensure that the presence of drones in the sky does not present significant risks to aircraft

as they try to integrate them into their air navigation and surveillance systems (Khanyile, 2019). Privacy is also a big concern as UAVs equipped with cameras, scanners, and sensors could be used by individuals with insidious motivations to collect and record sensitive or damaging information on civilians, businesses, and other organisations (Joshi, 2018).

A further issue is that drones are being used to kill people in war, as many African countries are in a state of protracted confli t (Allen, 2021; Krähenmann, Call and Dvaladze, 2020). In confli t zones, drones may be difficu t to distinguish from the military drones that are used in battles resulting in a scenario where even a helpful drone may be perceived as a threat by local residents.

Lastly, electronic systems used by drones for navigation, data gathering, and other procedures also need to be safeguarded from hackers. Many UAVs can be easily hacked and hijacked by malevolent forces to conduct criminal activity (Yaacoub et al., 2020).

UAVs must obtain an insurance policy to cover their liability if, while operating their drones, they cause physical or bodily damage to another (Khanyile, 2019). Other important regulatory acts include requiring a permit to fly over areas where citizens reside, as well as requiring drone operators to obtain a special permit from the civilian aviation authority (South African Civil Aviation Authority, n.d.). Many African countries are still struggling to put the necessary regulations in place to support UAV operations. There are still drones in those countries, but they are operated illegally by untrained and unlicensed operators (Khanyile, 2019).

How does the African peace and security environment respond to these emerging and growing high-tech challenges and opportunities?

The African Union (AU) established the African Peace and Security Architecture (APSA) and the African Governance Architecture (AGA) in response to ongoing and deepening insecurity, but the reality is that democracy and development struggle to flou ish in insecure environments.

Under such environments, confli t resolution becomes critical—but also contested. Stakes are high, especially in areas rich in minerals and other potential resources. Hence, outsiders and insiders compete amongst and between themselves with intervention logics that tend to promote narrow interests instead of advancing human security agendas. This includes the application of 'stabilisation' and 'liberal peace' logic. These are attractive options to outsiders. It tends to 'freeze' a confli t in space and time, allowing for the threat to be minimised (particularly refugees and migrants) and for economic opportunities to be pursued (arms trade, humanitarian and peacekeeping activities, access to mineral resources). Consequently, a pattern often emerges of collaboration between local actors (victorious rebels, ruling elites, business) and external forces (donors, International Cooperating Partners, business interests, arms dealers), which tends to postpone confli t resolution and therefore the achievement of human security.

The Southern African region is not spared in these dynamics. Below, we profile t e region's capabilities.

Figure 1: Profile of sele t SADC defence forces

SADC member state	Budget in USD	Active Personnel				
	2019	Total	Army	Navy	Air	Other
Angola	1.70bn	107,000	100,000	1,000	6,000	10,000 Rapid-reaction police
South Africa	3.54bn	74,850	37,600	7,000	9,650	7,6000 Military Health Service 15,000 Reserve
Tanzania	827mn	27,000	23,000	e1,000	3,000	1400 Police Field Force inlc. Marine Unit

Source: The Military Balance, 2020

The security landscape in the SADC region in the last fi e years has generally been stable compared to other regions on the African continent. However, it suffers from protracted confli t in the Democratic Republic of the Congo (DRC) and Mozambique, and political instability in eSwatini, Zimbabwe, and some Indian Ocean Islands. The region's 'superpower,' South Africa, suffers from violent crime and growing poverty, aided by a toxic mix of economic stagnation, grand corruption, ruling party instability, and state fragility.

Violent extremism and cyber threats stand out as rapidly evolving trends.

Southern Africa is experiencing an upsurge in violent extremism (VE). The DRC, Mozambique, and Tanzania have all experienced attacks, with events in Cabo Delgado, Mozambique making international headlines. The Southern African Development Community (SADC) has been called on to provide support to Mozambique and has deployed a SADC Standby Force to the area. Although a force intervention limits the number of violent attacks, it cannot bring sustainable peace to the area. Lasting peace requires interventions that address the socio-political, security, and economic complexities that have enabled the rise of violent extremism.

The digital age realities tend to enhance integration (in particular, ease of communication) and act as an aggravating factor (in particular, abuse of communication). Increasingly, social media are being used to promote fake and false news and information peddling for political reasons.

Closely related is the reality of cyber threats, including cybercrime and cyber-terrorism. SADC displays little understanding of the nature and magnitude of this threat, and has little capacity to detect or prevent this rising phenomenon.

This view is supported by research that points to the changing nature of cybersecurity threats in Africa (Mills, 2020). Cybersecurity and crime are hardly unknown to Africa. But the format of African cybercrime is rapidly changing. There have been rapid changes in telephony and broadband, which have and will continue to change continental connectivity and the opportunities, thus, for cyber-malfeasance. In the mid-1990s, for example, Africa's telephone density was at just 5%. Today, one-third of African mobile users, some 250 million people, already have a smartphone, which is projected to double by 2025, when over half of the continent will subscribe to mobile services, and when one-quarter will have access to 4G or 5G.

This raises the question of how civil society, in particular, could guard against election and other national narrative manipulation, and whether heightened cyber-threats, in general, can best be countered through partnerships with commercial or state-centred agencies outside of Africa.

The state of the region's defence

SADC has produced sophisticated peace and security frameworks, but to what extent does it have the hardware and tools to implement these?

An interview with an academic expert reveals that conventional military assets are here to stay in Africa, for several reasons. As he put it:

> One, they are affordable; two, they're tried and tested. Three, our geographies are such that they require that kind of equipment. Four, our mindset, the mindset of warring parties that we know of today, are still very much embedded in their beliefs in conventional warfare.

At the same time, the size and preparedness of the SADC member states' defence and security sectors constitute a mixed bag. On the one hand, two member states maintain sizeable defence forces and budgets: Angola and South Africa. On the other hand, several member states have miniscule defence and security sectors and budgets: Lesotho and Eswatini, and Comoros and Seychelles. Many with small defence and security sectors rely on bilateral arrangements—many with India and some with NATO countries—for protection.

Indian Ocean member states focus on maritime security issues and maintain coast guards. Except for South Africa, none have a defence industry. Equipment is increasingly obsolete or poorly maintained. Few have the ability to participate meaningfully in UN or AU peacekeeping operations.

It is doubtful that the collective can mount a SADC Standby Force operation to deal with a breach of peace and security or a substantial natural disaster. International cooperation is therefore unavoidable.

In this context, one interviewee was of the view that SADC ought to capitalize on its bilateral and multilateral agreements with entities like the Brazil/Russia/India/China/South Africa alliance (BRICS) because the global powers continue to play a role on the African soil, and they have a keen interest in what is happening here. As he noted: 'now and then they (BRICS) would like to demonstrate their willingness to support regional initiatives, I think we'll have to rely on them to help us with it.' Arguably, the region's attempt to deal with violent extremism in the Cabo Delgado region of Mozambique requires such collaboration and coordination, not only from the global South but also from Africa's international cooperating partners, particularly the European Union as well as a range of UN agencies (Chingotuane et al., 2021).

Is it possible to close the gap?

How can the rapidly evolving global technologies and their use in defence and warfare be made relevant to developing nations and Africa in particular?

Until recently, the South African cybersecurity response capacity was faced with an uncoordinated 'silo' approach (fragmented policy-making and strategic responses), a lack of public-private partnerships, and the absence of an overall international cooperation framework (Gwala, 2020). To address these, in 2015, it adopted a National Cybersecurity Policy Framework (NCPF) to address national security threats in the cyberspace, create a framework for combating cybercrimes and other cyber ills, build confide ce and trust in the secure use of ICTs, and create policy guidelines to steer PPP and international cooperation (SSA, 2015). However, it is unclear to what extent the policy framework allows for strategic decision-making and threat management (Sutherland, 2017). The case of a cyber-attack on Transnet in July 2021 is deserving of a fuller investigation—even though much detail remains shrouded in secrecy.

A recent feature of modern warfare—drones—deserves the focused attention of African national security decision-makers. The impact of the US drone programme on counterterrorism operations in Africa has been severe—especially in the Horn of Africa and the Sahel (Donnenfeld, 2019).

For example, in 2018, US special forces conducted airstrikes against suspected al-Shabaab militants in Somalia, killing 24 people. Drone strikes in Somalia caused about 300 casualties during Barack Obama's eight years in offi e. Trump nearly tripled that total in less than a quarter of that time (Donnenfeld, 2019).

To what extent can drones be regarded as effective and efficient weapons in the struggle against violent extremism and terrorism, particularly in Africa? Imagine, for example, the rise of a new breed of armed drones capable of swarmed and coordinated attacks, and able to operate in uncertain or changing combat environments. More disturbingly, imagine this tool in the hands of violent extremists. Analysts suggest an increased use of drones by nonstate actors in the Cabo Delgado theatre of confli t (Allen, 2021).

Should the South African defence industry persist in a military drone programme? Who would benefi ? The advantages should be seen against the reality of a struggling defence industry, hobbled by mismanagement and corruption, and a consequent shrinking customer base (Heitman, 2021).

A useful perspective is offered by Dyer (2018) who examined the extent to which drones are able to defend African maritime sovereignty and advance ocean governance. In his analysis, the further development of a South African and African drone sector is conditional upon stakeholder user and producer requirements including cost-effectiveness, mission performance and efficie cy, technologically feasible and environmentally sustainable solutions, with sufficient training, sensor capacity, appropriate autonomy, redundancy and system risk management. He points out that the most significant risks for monitoring and awareness drones include the uncertainty of climate change, and technological and business cycles influe cing uncertain demand and supply (Dyer, 2018).

Indeed, if drones are to be included in future maritime security arrangements, South Africa and Africa need to consider the extent to which effective governance can be enacted and secured. A range of

emergent risks need to be resolved: climate change and environmental uncertainty, cybersecurity, social-religious/other tensions, flu tuating economic and technological cycles, AI and automation, legal risks and increased prospects of militarisation and warfare. These threaten to undermine any arising advantages and opportunities (Dyer, 2018).

Conclusions

It is true that many African militaries and national security structures suffer from capacity constraints and operate with conventional warfare mindsets. How can they go about preparing and defending against advanced technological attacks? Perhaps the question is misplaced. As described above, the African threat landscape is marked by socio-economic deprivation, corruption and poor governance, violent competition for political power, the exploitation of natural resources, transnational crime, and the emergence and spread of violent extremism and terrorism. Conventional warfare and weapons systems remain appropriate for dealing with many of the threats facing Africa. The breakthrough technologies noted in this article—from hypersonic missiles to advanced seaborne second-strike capability, military-grade spyware, to direct energy weapons—are meant to be instruments in the hands of nations striving to become global superpowers, or of those protecting its perceived image as the world's most powerful military and economy.

However, in the long run, for Africa to build and maintain effective and efficient security sectors, able to respond to human and natural disasters, terror attacks, and exploitation by foreign militaries, Africa needs to tap into the innovation brought by the fourth industrial revolution—autonomous vehicles, smart robotics, materials engineering, Big Data, IoT, and 3D Printing. Digitisation can have a dramatic impact on operational capabilities. As noted above, advances in precision location, targeting and strike, navigation, large data transmission and discrimination, weapon-system range and manoeuvrability, and the growing importance of the outer space and cyber domains are collectively altering the 'spatial dimensions' of warfare. These building and maintenance tasks are the responsibility of national security decision-makers and their personnel on the national, regional and continental level, requiring an overhaul of the APSA.

In ensuring Africa's preparedness, they may benefit from the following two proposals: one, education and training of the future soldier, starting with enabling the schooling system to be digitally-capable and ensuring defence colleges and related training and educational institutions are equally made digital-friendly; and two, accepting that the lines between hardcore military and non-military warfare from a cyberspace perspective are blurred—meaning, the military increasingly uses private sector assets in order to implement warfare as part of warfare tactics without importing them fully into their arsenal. This emerging domain of collaboration requires proper governance to prevent abuse. The relationship between civilians and military or security practitioners should be based on respect for human rights so that they don't abuse that landscape for criminal and unconstitutional purposes.

Without a paradigm shift in military thinking, the lofty ideals of the AU's Agenda 2063 will not materialise: a prosperous Africa based on inclusive growth and sustainable development.

Notes

[1] The author recognises the valuable contribution to a previous draft of this article by research intern Daisy Mbutho.

References

Allen, K. (2021). 'Drones and violent nonstate actors in Africa.' Africa Center for Strategic Studies (ACSS) Spotlight [online]. Available at: https://africacenter.org/spotlight/drones-and-violent-nonstate-actors-in-africa/

BBC News. (2021). 'Pegasus: Spyware sold to governments 'targets activists'.' BBC News [online]. Available at: https://www.bbc.com/news/technology-57881364

Bitzinger, R. (2021). '4IR: The RMA we are finally loo ing for?' RsiS Commentary [online]. Available at: https://www.rsis.edu.sg/wp-content/uploads/2021/02/CO21017.pdf

Bowers, I. and Kirchberger, S. (2020). 'Not so disruptive after all: The 4IR, navies and the search for sea control'. Taylor & Francis [online]. Available at: https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1848819
https://doi.org/10.1080/01402390.2020.1848819

Chingotuane, E., Sidumo, E., Hendricks, C. and A. van Nieuwkerk. (2021). 'Strategic options for managing violent extremism in Southern Africa: the case of Mozambique.' Situation Report. Maputo: Friedrich Ebert Foundation.

Cohen, A. (2021). 'How Space Lasers Could Soon Beam Clean Power Down To Earth.' Forbes [online]. Available at: https://www.forbes.com/sites/arielcohen/2021/03/29/space-lasers-the-truth/?sh=6e8e28fc6d46

Donnenfeld, Z. (2019). 'Drone strikes a growing threat to African civilians.' ISS Africa [online]. Available at: https://issafrica.org/iss-today/drone-strikes-a-growing-threat-to-african-civilians

Dyer, J. (2018). 'Defending African maritime sovereignty with fini e resources: the prospects and power of drones and AUVs.' Unpublished paper.

Gwala, S. (2020). 'An analysis of the implementation of the South African National Cybersecurity Policy Framework.' Unpublished PhD, University of the Witwatersrand.

Heitman, H. (2021). 'What to do with Denel?'. DefenceWeb [online]. Available at: https://www.defenceweb.co.za/featured/feature-what-to-do-with-denel/

Joshi, N. (2018). 'The opportunities, challenges, benefits, a d threats of drones.' Allerin.com [online]. Available at: https://www.allerin.com/blog/understanding-the-opportunities-challenges-benefits-a d-threats-of-drones

Khanyile, N. (2019). Fun with a warning. Witness [online]. Available at: https://www.news24.com/witness/news/fun-with-a-warning-20190204-2

Koigi, B. (2019). 'Drones drive development revolution in Africa.' FairPlanet [online]. Available at: https://www.fairplanet.org/story/drones-drive-development-revolution-in-africa/

Krähenmann, S., Call, G. and Dvaladze, G. (2020). 'Humanitarian concerns raised by the use of armed drones.' ReliefWeb [online]. Available at: https://reliefweb.int/report/world/humanitarian-concerns-raised-use-armed-drones

Kristensen, H. and Korda, M. (2021). 'Russian nuclear weapons, 2021.' Tandfonline.com [online]. Available at: https://www.tandfonline.com/doi/pdf/10.1080/00963402.2021.1885869
https://doi.org/10.1080/00963402.2021.1885869

Lutkevich, B. (n.d.) 'What is a Drone?-Definition rom WhatIs.com.' IoT Agenda [online]. Available at: https://internetofthingsagenda.techtarget.com/definition drone

Mills, G. (2020). 'The African security intersection. Discussion paper 1/2020.' Brenthurst Foundation [online]. Available at: http://thebrenthurstfoundation.org/workspace/files discussion-paper-01-2020-the-african-security-intersection-.pdf

Naidoo, S. (2021). 'Transnet cyber-attack confi med: Port terminals division declares force majeure.' MoneyWeb [online]. Available at: https://www.moneyweb.co.za/news/companies-and-deals/transnet-cyber-attack-confi med-port-terminals-division-declares-force-majeure/

Norman, G. (2020). 'The 5 most powerful armies in the world.' Military [online]. Available at: https://www.military.com/daily-news/2020/02/24/5-most-powerful-armies-world.html

Obering, H. (2021). 'Directed Energy Weapons Are Real... And Disruptive.' National Defense University Press [online]. Available at: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Obering_36-46.pdf

Reva, D. (2021). 'Cyber-attacks expose the vulnerability of South Africa's ports.' ISS Today [online]. Available at: https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports

SSA. (2015). 'The National Cybersecurity Policy Framework.' [online] Available at: https://www.gov.za/sites/default/files gcis_document/201512/39475gon609.pdf

Seidel, J. (2020). 'China's secret 'submarine cave' revealed.' News.com.au [online]. Available at: https://www.news.com.au/technology/innovation/military/south-china-sea-photos-reveal-secret-underground-base-off-hainan-island/news-story/b138456800abdb0ea71970465ee8c464

Shamsi, H. (2021). 'Trump's Secret Rules for Drone Strikes and Presidents' Unchecked License to Kill.' Just Security [online]. Available at: https://www.justsecurity.org/75980/trumps-secret-rules-for-drone-strikes-and-presidents-unchecked-license-to-kill/

Sutherland, E. (2017). 'Governance of Cybersecurity-the case of South Africa.' The African Journal of Information and Communication 20. [online] Available at: https://www.researchgate.net/publication/322460472_Governance_of_Cybersecurity_-_The_Case_of_South_Africa
https://doi.org/10.23962/10539/23574

Sutton, H. (2021). 'Chinese Ships Seen Mapping Strategic Seabed In Indian Ocean.' Naval News [online]. Available at: https://www.navalnews.com/naval-news/2021/01/how-china-is-mapping-the-seabed-of-the-indian-ocean/

Van Nieuwkerk, A. (2021). 'Building anticipatory governance in SADC: Post-Covid-19 confli t and defence outlook.' SAIIA Occasional Paper 323. [online] Available at: https://saiia.org.za/research/building-anticipatory-governance-in-sadc-post-covid-19-confli t-and-defence-outlook/

Vergun, D. (2018). 'DOD scaling up effort to develop hypersonics.' Defense [online]. Available at: https://www.defense.gov/Explore/News/Article/Article/1712954/dod-scaling-up-effort-to-develop-hypersonics/

World Economic Forum. (2019). 'The Global Risks Report 2019.' [online] Available at: https://www.weforum.org/reports/the-global-risks-report-2019

World Economic Forum. (2021). 'The Global Risks Report 2021.' [online] Available at: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Williams, D. (2021). 'Israeli lawmaker sees possible export review on NSO spyware scandal.' Reuters [online]. Available at: https://www.reuters.com/article/israel-cyber-nso-idAFL8N2OY1NT
https://doi.org/10.1016/S1353-4858(21)00082-9

Woolf, A. (2020). 'Russia's Nuclear Weapons: Doctrine, Forces and Modernisation.' Congressional Research Service [online]. Available at: https://crsreports.congress.gov/product/pdf/R/R45861

Yaacoub, J., Noura, H., Salman, O. and Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Science Direct.
https://doi.org/10.1016/j.iot.2020.100218

Zysk, K. (2021). 'Defence innovation and the 4th industrial revolution in Russia.' Taylor & Francis [online]. Available at: https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090
https://doi.org/10.4324/9781003268215-5