CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

JANUARY 2024

South Africa's Cyber Strategy Under Ramaphosa: Limited Progress, Low Priority

Russell Buchan and Joe Devanny

South Africa's Cyber Strategy Under Ramaphosa: Limited Progress, Low Priority

Russell Buchan and Joe Devanny

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Summary

During the decades of apartheid, South Africa was an international pariah. Since the country transitioned to majority rule in 1994, the African National Congress (ANC) has dominated politics, and the ANC has itself transitioned from a national liberation movement to a party of government. Domestically, South African cyber strategy should be seen as part of the ANC's wider political challenge of trying to deliver economic growth, development, and prosperity. Over thirty years, the ANC has struggled to deliver on this agenda in a profoundly unequal society with infrastructure and institutions that have weakened particularly over the past fifteen years.

Alongside confronting domestic challenges, the ANC has also tried to reshape South Africa's global role. This was perhaps most visible under its first president, Nelson Mandela (1994–1999), but it was arguably pursued most systematically under Mandela's successor, Thabo Mbeki (1999–2008). This reorientation of South Africa in the world was an ambitious and complex project, the foundations of which were the country's leading role in its region and continent as well as its ties within the wider Global South. The project entailed tensions between the progressive promotion of human rights and freedoms, on the one hand, and the cultivation of instrumental relations with authoritarian and repressive states, on the other. These tensions continue to affect South African foreign policy, including its cyber diplomacy.

South Africa identifies cybersecurity as a key national priority and has to this end adopted a national cybersecurity strategy and established a military Cyber Command. The reality, however, is that other issues have been consistently ranked above cybersecurity, such as addressing corruption, poverty, racial and social injustice, and the HIV/AIDS epidemic.

Cybersecurity has therefore not been seen as a high priority by successive South African governments. This has left Cyber Command underresourced and unmotivated. This deprioritization means that South Africa is unlikely to emerge as a prominent military or intelligence cyber power anytime soon. The wider lack of national prioritization will also make it harder for so-called like-minded states—which are bound together by a mutual respect for democracy, human rights, and the rule of law—to form an effective partnership with South Africa on the topic of cybersecurity.

South Africa's approach to international cyber governance debates has been cautious and noncommittal, reflecting cyber diplomacy's relatively low priority in its national strategy. What position South Africa takes in cyber debates is, however, of keen interest to the international community. An important question is whether South Africa will support the existing multistakeholder approach to cyber governance that is championed by like-minded states or join China and Russia in their efforts to recalibrate this approach and push for greater state control over cyberspace. Indeed, under President Cyril Ramaphosa, South Africa has not yet published its national position explaining how international law applies to cyberspace. A related question is whether South Africa will join like-minded states in elaborating how existing international law applies to cyberspace or side with China and Russia to campaign for new, bespoke international law (for example, treaties) to regulate this domain.

When examining these questions, it is important to recognize the context of the ANC's long-standing ties with Russia, both during its thirty years in government and in its previous decades struggling for national liberation. This is helpful for understanding South Africa's interactions with Brazil, Russia, India, and China (which form the BRICS bloc with South Africa) and forecasting its future positions in cyber governance debates. For example, South Africa has been reluctant to unambiguously condemn Russia's invasion of Ukraine in 2022, and it appears to have supported Moscow by covertly supplying it with weapons. In the longer term, South Africa's positions in cyber diplomacy debates will likely be shaped by trends in both domestic politics—such as the ANC's waning electoral performance—and the success of digital development. In this context, it is perhaps advisable for like-minded states, such as the United States, to focus on cyber capacity-building assistance and ensure that these efforts play into the wider development agenda in South Africa.

Introduction

This paper addresses the domestic politics, foreign policy, and international legal dimensions of South Africa's cyber strategy under President Cyril Ramaphosa. It draws out the relevant policy implications for like-minded states—which are bound together by a mutual respect for democracy, human rights, and the rule of law—of South Africa's challenging journey toward developing a coherent national cyber strategy. Understanding South Africa's cyber strategy is important because of its membership in the BRICS bloc (along with Brazil, Russia, India, and China, and several invitees). It is also important because of South Africa's prominent role in Africa as well as its wider ties within the Global South. South Africa is widely perceived as one of the pivotal middle-ground states—which liberal, like-minded states and authoritarian states compete to influence in contemporary cyber diplomacy.

The paper proceeds in two parts. It first identifies the cyber threats faced by South Africa and moves on to measure the country's cyber power by exploring the extent of its cyber capabilities. The paper then unpacks South Africa's cyber strategy, identifies the institutions and agencies responsible for maintaining cybersecurity in South Africa as well as the regulatory frameworks governing them, and analyzes South Africa's approach to cyber diplomacy and cyber governance at the international level.

South Africa's Cyber Threats in Context

In 1994, the African National Congress (ANC) won South Africa's first democratic election after the country transitioned to majority rule. The party has continued to dominate national politics, remaining the party of government ever since.[1] Although the end of apartheid and the triumph of democracy brought hope, the social and economic reality that the ANC inherited was bleak—and profoundly unequal.[2] In government, the ANC has pursued economic growth alongside efforts to reduce poverty, increase access to public services, and address inequalities of income, wealth, and power. It has struggled to prevent the hope of democratic transition from turning into anger, as the economy has stagnated, institutions have weakened, and its transformational agenda has faltered.[3] The party has itself become increasingly associated with systemic corruption (state capture) and neglect, particularly under the presidency of Jacob Zuma (2009–2018).[4]

As the dominant political actor in post-apartheid South Africa, the ANC and its intraparty factionalism have shaped the country's governance. The deployment of ANC party cadres into senior governmental and parastatal leadership positions blurs the lines between party and state. Particularly during the Zuma presidency, this phenomenon became associated with deteriorating public infrastructure, weakening institutions, and economic stagnation.[5] This represents a very challenging national political context for South Africa to make progress on the domestic implementation of cyber strategy. It is also a context in which the successful implementation of cyber and digital development policies could act as a force multiplier for the government's agenda of poverty reduction and inclusion.[6] Notwithstanding this fact, the reality is that in the rank order of strategic priorities, cybersecurity is rated lower than other objectives. As a leading South African cyber researcher has noted, "We tend to put a higher priority on our socio-economic challenges than on our technological challenges, and we should. We don't have as much money and capacity to focus on technological challenges and cyber security."[7]

Cyber Threats in South Africa

Despite South Africa's various political, economic, and social challenges, it has "leapfrogged into the digital age" and cyberspace has been woven into the fabric of everyday life.[8] With a digital penetration rate of 72 percent, South Africa has been referred to as "the world's most internet-addicted country."[9] That said, the rate is far higher in urban than in rural areas, the latter comprising over 30 percent of the population.[10] The World Bank has identified connectivity and digital skills shortcomings as factors likely to hold back South Africa's pursuit of economic growth and poverty reduction.[11]

As with most states, as digital access has expanded in South Africa, so too has the attack surface for criminals to exploit. There has been a dramatic increase in cyber crime in the country since the COVID-19 pandemic emerged. This is particularly evident in

the incidence of ransomware-related crimes. South Africa reportedly suffers the most ransomware and business email compromise incidents in Africa.[12] According to the information technology (IT) security company Sophos, over half of South African businesses were affected by a ransomware incident in 2021.[13] And according to a 2023 briefing by the South African Council for Scientific and Industrial Research, South Africa is the eighth most targeted country in the world for ransomware.[14] According to that briefing, the impact of cyber crime on the South African economy is currently estimated at 2.2 billion South African rand ($120 million) per year.

There have been several notable national incidents highlighting this upward trend that, according to one estimate, equated to an 18 percent rise in cyber crime in 2022.[15] For example, in 2019, a ransomware incident was reported at City Power (Johannesburg's electricity utility) and disrupted power supplies.[16] In 2020, South Africa's second-largest private hospital (Life Healthcare Group) was subjected to a cyber attack that affected admissions, processing systems, and email servers.[17] Also that year, a South African credit agency suffered a massive data breach, compromising the information of 24 million people.[18] Then, in 2021, a cyber attack against Transnet—a state-owned rail, port, and pipeline company—caused significant disruption to transportation and extensive economic harm.[19] Also in 2021, ransomware incidents were reported in the Department of Justice and Constitutional Development; the perpetrators encrypted the department's systems and rendered them unavailable to employees and members of the public.[20] In August 2023, it was reported that the South African National Defence Force (SANDF) had suffered a potentially massive data breach by apparent hacktivists, including the theft of highly classified information.[21] Ominously, cybersecurity experts forecast that cyber crime incidents will continue to rise given South Africa's weak cybersecurity and poor cyber hygiene.[22]

South Africa's Cyber Capabilities

Like many other governments over the last decade, the South African government has stated its commitment to develop cyber capabilities for defensive and offensive purposes. In 2015, the cabinet approved the creation of a military Cyber Command. However, as ETH Zurich's Max Smeets has argued, not all military cyber commands are equal.[23] Due largely to the deprioritization of defense expenditure, including on cyber defense, in favor of other spending priorities, the SANDF Cyber Command is, according to its commanding officer, underresourced and has not been able to develop sophisticated cyber capabilities or procure all the capabilities it requires from the private sector.[24]

The serious breach of defense networks reportedly suffered by South Africa in 2023 also suggests significant shortcomings in cyber maturity. South Africa might possess some of the most sophisticated cyber capabilities in Africa,[25] but these are unlikely to compare favorably with those of the states with the most cyber power, such as China, Russia, the United Kingdom (UK), and the United States. For example, the Belfer Center's National Cyber Power Index has never ranked South Africa in its top ten states for cyber power, and South Africa does not feature in any of the metrics it uses to measure cyber power (such as leadership in cyber norms, surveillance, finance, and defense).[26]

Another important instrument of cyber power is digital espionage. In this capacity, South Africa is both a protagonist and a victim, as is the case for many states engaged in intelligence competition. South African politicians have apparently been targeted with commercially available spyware; for example, Ramaphosa was reportedly targeted for surveillance by the Rwandan government using the Pegasus spyware.[27] Meanwhile, there is some evidence to suggest that the South African government has been a customer for domestic spyware services in the past.[28]

Domestic surveillance has also been a sensitive political issue in South Africa for decades.[29] Revelations by Edward Snowden in 2013—for example, that the UK cyber intelligence agency, the Government Communications Headquarters (GCHQ), spied on South African diplomats during a G20 summit—further raised public awareness about digital surveillance.[30] This prompted reflection on the extent to which such practices can be constrained in South Africa.[31] More recently, the Constitutional Court has required the government to reform legislation regulating the use of surveillance capabilities.[32]

The Ramaphosa government's proposals to undertake significant national intelligence reforms under the General Intelligence Laws Amendment Bill (GILAB) have sparked heated debates.[33] The bill's critics, including the prominent Congress of South African Trade Unions (COSATU), say it would dangerously expand the definition of national security and the remit of South African intelligence authorities to spy on individuals involved in lawful political activities.[34] The bill would subject private security companies, nongovernmental organizations, and religious institutions to security checks—ostensibly motivated by the need to improve anti–money laundering powers, but also potentially motivated by a desire to reduce the risk of subversion undermining the integrity of South African democracy or enable the South African government to exert controls over the freedom of political expression. The apparent lack of robust oversight and accountability arrangements in the GILAB has caused concern among researchers and civil society campaigners.[35]

Notwithstanding these criticisms of the GILAB, it has been clear for several years that broad reform of the intelligence community—and specific revision of surveillance legislation—has been necessary in South Africa.[36] The relatively slow pace of government efforts to effect change in this area, together with the apparent trend of the Ramaphosa administration's proposals to further privilege the executive vis-à-vis citizens, suggests a disconnect in both urgency and substance between the government's agenda and the recommendations of two independent commissions. Reforms were urgently recommended in both the final report of South Africa's Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector including Organs of State[37] (better known as the Zondo Commission, after its chair, then deputy chief justice Raymond Zondo) and the 2018 High-Level Review Panel on the State Security Agency, which reported on the politicization and abuse of power and resources at the State Security Agency (SSA) under the Zuma administration.[38] This context suggests it is imperative that the Ramaphosa administration's legislative agenda for intelligence reform receive robust parliamentary scrutiny and public challenge. There is real substance to the public scrutiny of these proposals outside the parliament, but it is not yet clear whether the legislative process is sufficiently open to constructive challenge and feedback to incorporate these perspectives as the draft legislation proceeds.

In one sense, the Ramaphosa administration is simply responding to a contemporary dilemma faced by many liberal democratic states. It is trying to effectively balance the need for limits, accountability, and oversight against the executive's legitimate need to maintain effective cyber and other intelligence capabilities. In another sense, however, the apartheid and post-apartheid history of political abuse of intelligence capabilities in South Africa is cause for concern. Doubt remains about the ability of South Africa to reform its intelligence sector and surveillance capabilities in a manner that upholds the liberal democratic values of the country's constitution.

Cybersecurity Strategy and Responsible Agencies

South Africa has publicly identified cybersecurity as a "central national priority."[39] The reality, however, is that successive governments have not ranked cybersecurity as a top priority. Instead, their priorities have been ending poverty, racial and social injustice, and the HIV/AIDS epidemic. With the ANC dogged by corruption allegations in recent years, ending political corruption has also become a declared focus of the government. In this context, the deprioritization of cybersecurity will make it difficult for like-minded states to gain traction and forge effective partnerships with South Africa on this topic.[40] The optimum engagement would be to explicitly tie cyber capacity-building assistance to the government's agenda of promoting sustainable development, increasing economic growth, and reducing poverty and inequality.

The wider political context has not completely prevented South Africa from developing some aspects of a national approach to cybersecurity. The Zuma government approved the National Cybersecurity Policy Framework (NCPF) in 2012, though it was not officially published by the minister of state security until 2015.[41] The NCPF is seen as South Africa's national cybersecurity strategy and was developed "to ensure a focussed [*sic*] and an all-embracing safety and security response in respect of the cybersecurity environment" and create an "information society which takes into account the fundamental rights of every South African citizen to privacy, security, dignity, access to information, the right to communication and freedom of expression."[42]

The NCPF explains that the SSA has overall responsibility and accountability for the coordination, development, and implementation of cybersecurity measures in the country, all of which make up an integral part of its national security mandate.[43] The SSA established its Computer Security Incident Response Team (CSIRT) in 2003, more than a decade before the national CSIRT was formed by the Department of Telecommunications and Postal Services in 2015.[44] This suggests that institutional cyber maturity is likely more advanced in the security sector than in the wider public-service departments. Under the Ramaphosa government, the SSA was brought into the Office of the Presidency, suggesting closer oversight by the center of government.

As in many countries, institutional separation is also evident in South Africa's cyber defense. An integral part of the Department of Defence and Military Veterans' national defense mandate is to oversee the coordination, accountability, and implementation of cyber

defense measures in South Africa.[45] The Department of Science and Innovation (formerly the Department of Science and Technology) was made responsible for the development, coordination, and implementation of the national capacity development program for cybersecurity under the NCPF.[46] There has been skepticism about how much the department has achieved in this remit over the last decade.[47]

The Justice, Crime Prevention and Security Cluster (JCPS) oversees the implementation of the NCPF. A dedicated cybersecurity response committee has been established in the JCPS to coordinate cybersecurity efforts. This committee is chaired by a member of the SSA and is supported operationally by the Cybersecurity Centre, which is situated in the SSA.[48]

The 2015 Cybercrimes and Cybersecurity Bill mandated the development of defensive and offensive cyber capabilities as part of the defense mandate of the SANDF.[49] The NCPF envisioned the creation of a unified SANDF Cyber Command to lead on the protection of critical national infrastructure, and it was established by the Department of Defence in 2015.[50] As already noted, due to the fact that neither cybersecurity nor wider defense is a top spending priority, Cyber Command is reportedly underresourced and does not possess the necessary equipment, funding, technological expertise, or facilities to enable it to proactively and effectively defend the country's critical infrastructure.[51] Lamenting the lack of resources, Cyber Command's commanding officer explained that it was "able to function, however, not optimally."[52] The aforementioned report of a major data breach of South African defense networks suggests that this might be an understatement. It indicates that the South African government's cyber defense aspirations need to be reviewed, given the apparent misalignment of ends, ways, and means.

How South Africa's Cyber Strategy Fits Into Its Foreign Policy

The ANC's Broader Foreign Policy

Given the transnational nature of cybersecurity, cyber strategy has both domestic and international dimensions. To situate South African cyber diplomacy in context, it is first necessary to establish the wider framework of South African foreign policy under the ANC. Under Mandela, South Africa's first democratically elected president, the ANC developed a post-apartheid foreign policy based on the promotion of fundamental human rights, democracy, justice, and the sovereign equality of states.[53] It should be noted that there is an emerging revisionist view of South African foreign policy under Mandela, one that points to greater continuity with Mandela's successors.[54] During the 1990s and 2000s, South Africa nonetheless maintained a relatively principled approach to foreign policy and became a global defender of international peace and justice, prompting the *Economist* to describe it as a

"diplomatic heavyweight" on the international stage.[55] In short, post-apartheid South Africa positioned itself as a nonaligned, neutral state that was more concerned with the pursuit of normative ideals than with forging strategic power alliances.[56]

There is a critique—evident in both South African and foreign commentaries—that South Africa has been in "diplomatic descent" since Mandela left office.[57] This argument suggests that presidents Thabo Mbeki (1999–2008) and Zuma lost sight of the principles and values proclaimed by the Mandela administration, with South Africa particularly under Zuma losing its "reputation as a principled member of the global community."[58] Critics argue that this trend has continued under Ramaphosa since he assumed office in 2018. However, this argument reflects both a slow recalibration of Western perceptions of South African foreign policy and the shifting modalities of the ANC's foreign policy. The view also obscures the extent to which Mbeki played an influential foreign policy role under the Mandela presidency. Arguably, the surprise is that it took so long for the West to realize that South African foreign policy has been relatively consistent throughout the post-apartheid period.[59] This reflects, perhaps, the relatively low global salience of established South African diplomatic positions on issues such as Zimbabwe,[60] the ANC's long-running ambivalence about South Africa's obligations under and continued membership of the International Criminal Court (ICC),[61] or the party's historic relationship with Russia.[62]

South African foreign policy under the ANC does emphasize human rights and freedoms, but it also exhibits characteristics common in other liberation movements that have transitioned to become parties of government.[63] Regionally, that is evident in its consistent policy toward Zimbabwe during the last twenty years of president Robert Mugabe's rule. Although most closely associated with then president Mbeki, the extent of the broader ANC's opposition to Western sanctions and targeted measures on Zimbabwe should not be discounted. The ANC does not like to see the world's more powerful nations interfere in the sovereign affairs of less powerful states, especially African states.

A similar sentiment motivates ANC criticisms of perceived bias against African states in international institutions such as the ICC. South African diplomatic investment in forums such as the India–Brazil–South Africa (IBSA) forum and the BRICS bloc is evidence of a commitment to reshape the distribution of international influence. While this commitment is a consistent, deeply embedded sentiment within the ANC, it has not always been associated with astute diplomacy, as demonstrated by South Africa's support in 2011 for (and retrospective regret for supporting) United Nations (UN) Security Council Resolution 1973, which authorized military intervention in Libya and led to the overthrow of ruler Muammar Gaddhafi.[64] This support led some Western observers to misinterpret the ideological currents that shape South African foreign policy.

Increasingly in recent years, Western critics have recognized this trend of South Africa adopting positions at odds with the Western view of intervention in the sovereign affairs of other states. South Africa has also exhibited sympathy and support for authoritarian states such as China and Russia. As a result, Western perceptions of South Africa's neutral, nonaligned status, as well as its reputation as a defender of international peace and justice, have been recalibrated.

Lessons From South Africa's Response to the Russia-Ukraine War

South Africa's so-called diplomatic descent was particularly noted in its response to Russia's invasion of Ukraine in February 2022. That year, the UN General Assembly characterized the invasion as an act of aggression,[65] and in 2023 it demanded Russia's complete withdrawal from Ukrainian territory.[66] South Africa abstained from both resolutions—unlike Brazil, another nonaligned BRICS member, which voted in favor of both. South Africa also abstained from a vote in the General Assembly to suspend Russia from the UN Human Rights Council.[67] In January 2023, South Africa hosted Russian Foreign Minister Sergei Lavrov in Pretoria and the following month held naval exercises with China and Russia in its territorial sea.[68] Furthermore, in May 2022, the United States alleged that South Africa allowed a Russian vessel to collect weapons from a naval base near Cape Town, calling it a "serious issue."[69]

Additionally, South Africa hosted the annual BRICS conference in August 2023. There was uncertainty ahead of the summit about whether Russian President Vladimir Putin would attend. His potential in-person participation sparked international furor given that South Africa is a member of the ICC and the court's chief prosecutor had issued an arrest warrant for Putin.[70] Under Zuma, South Africa had refused to arrest then Sudanese president Omar al-Bashir—who was the subject of an ICC arrest warrant—when he visited South Africa in 2015.[71] Despite that history, South Africa ultimately hosted the 2023 BRICS event, with Lavrov attending in person and Putin participating online. Although this allowed South Africa to avoid breaching its obligations under the ICC statute, its efforts to accommodate Putin were viewed by some in the West as "cosying up" to the Kremlin.[72]

South Africa has refuted claims that it has aligned with Russia. In particular, it has sought to present itself as a neutral and impartial advocate of international law and the principles that stand behind it (including respect for sovereignty and the inviolability of territorial integrity).[73] For example, South Africa explained that it abstained from the UN General Assembly votes on the basis that the assembly should be a forum for constructive dialogue aimed at creating a sustainable peace, rather than be used to assign political or legal blame for international incidents and potentially fan the flames of instability and conflict.[74] Outside the General Assembly, South Africa maintained that "our non-aligned position does not mean that we condone Russia's intervention in Ukraine, which has violated international law."[75] South African officials further explained that the "territorial integrity of States, including that of Ukraine, [is] sacrosanct and we reject all actions that undermine the Purposes and Principles of the UN Charter, and International Law."[76] Moreover, in May 2023, Ramaphosa responded to U.S. allegations that a South African naval base had been used to supply a Russian vessel with weapons by expressing concern at the alleged incident and setting up an independent inquiry to investigate it.[77] That inquiry reportedly refuted the U.S. allegations, according to a published executive summary, but the Ramaphosa government said it does not intend to publish the inquiry's findings in full.[78]

What conclusions can be drawn from South Africa's response to the Russian invasion of Ukraine? Is South Africa continuing its diplomatic descent and, by doing so, abandoning its neutral status and aligning with Russia? Or is South Africa genuinely seeking to tread the line of neutrality and nonalignment as an impartial advocate for international law in a complex, volatile, and increasingly polarized world? The evidence over time indicates that South Africa has aligned with positions shared by Russia. Indeed, South Africa has long-standing ties with Russia, which South African International Relations and Cooperation Minister Naledi Pandor referred to in March 2023 as an "old, historical friend" that "we cannot become sudden enemies [with] on the demand of others."[79] This was a reference to the Soviet Union and its political and military support for South Africa's national liberation struggle during apartheid.

Additionally, South Africa's solidarity with Russia seems to be a product of what a significant current of opinion within the ANC perceives as Western hypocrisy. On this argument, while the West was quick to condemn Russia's actions as a breach of Ukrainian sovereignty and put significant pressure on other states to denounce Russia's invasion, it has also itself intervened militarily in states such as Afghanistan, Iraq, and Libya and failed to support effectively Palestinian sovereignty.[80] Ramaphosa himself also seemed to support Russia's argument that invading Ukraine was justified because of attempts by the North Atlantic Treaty Organization (NATO) to expand eastward into Russia's so-called sphere of influence.[81] The persuasiveness of these arguments within the ANC stems from the party's liberation struggle, its ideological opposition to Western imperialism, and the entrenched power of Western states in the international system.

Even if South Africa's drift toward Russia continues, it is important to recognize that the two states will make "uncomfortable bedfellows."[82] The values of human rights, justice, democracy, and sovereign equality are forever ingrained in the psyche of South Africa due to its experience of apartheid; yet, as the Russia-Ukraine war exemplifies, Russia demonstrates little respect for these principles and values in practice, even if it makes grand proclamations in their favor. This means South Africa and Russia are likely to experience a difficult and turbulent relationship going forward, which is indicated by the fact that South African officials have referred to Russia's invasion of Ukraine as a violation of international law.

There is still a window of opportunity for like-minded states to draw South Africa away from Russia. That South Africa has greater economic ties with the West than it does with Russia could be an important lever of influence for like-minded states, though South Africa also has significant trade and investment ties to China.[83] The reality of at least the past decade of diplomacy is that Western states have struggled to identify and act effectively on productive instrumentalities in their respective bilateral or collective relations with South Africa. The limits of like-minded states' influence on South Africa, particularly for cyber diplomacy, therefore should not be ignored.

South African Cyber Diplomacy and Cyber Governance

The tension in South Africa's foreign policy between neutrality and nonalignment, on the one hand, and its support for the BRICS bloc, on the other, provides important context when evaluating its approach to cyber diplomacy and cyber governance. Viewed from the perspective of a competition for influence between like-minded states and Russia and China, South Africa has been seen as a pivotal "swing state" or "digital decider" in debates about global cyber governance and norms of responsible state behavior in cyberspace.[84] It should be emphasized that these labels have been applied to South Africa by others; they are not labels that the ANC government has appropriated to articulate its own agenda. Indeed, it is not clear from twenty years of South African engagement in cyber diplomacy that there *is* a distinctive, consistent South African agenda.

Exacerbated by wider geopolitical tensions, the diplomatic debate over the future structure of cyber governance has fractured into two opposing camps. In one camp, like-minded states are campaigning to maintain the existing multistakeholder approach to cyber governance, which is based on openness, inclusion, collaboration, and consensual decisionmaking by private industry, international technical governance institutions, governments, and civil society.[85] This model pushes for a free and open cyberspace in which human rights are protected and governmental control is limited. These states also see the existing rules of international law as sufficient to regulate cyberspace, with the immediate task being to better understand how these rules apply to cyberspace rather than to create new rules.

In the other camp are the so-called sovereigntists, with its most prominent advocates being China and Russia. These states are looking to rewrite the rules on cyber governance and create a new structure that confers greater authority and control on governments at the expense of other stakeholders. Moreover, this camp argues that existing rules of international law do not apply to cyberspace or are so woefully inadequate that new, bespoke rules and regimes are needed, ideally crafted through international treaties. Like-minded states are concerned by these developments, fearing these initiatives may be used by states to clamp down on fundamental human rights and establish rules that bind Western states but which they would not abide by themselves.

It is currently unclear where South Africa will land on this important cyber governance debate. South Africa has participated constructively in the UN Group of Governmental Experts (GGE) and the UN Open-Ended Working Group (OEWG). It does not, however, appear to have been a prominent voice in these forums, neglecting to push a particular agenda or set of objectives. It is also a party to the Budapest Convention on Cybercrime, which is typically seen as a Western initiative.[86] Moreover, in April 2022, South Africa and the Netherlands issued a joint statement on cyber policy, which emphasized the importance of international mechanisms for ensuring an open, free, stable, and secure cyberspace, such

as the OEWG and the International Telecommunication Union.[87] They also highlighted the need for capacity building in developing countries, including "finance, technology transfer and capacity building, as well as engagement with the multi-stakeholder community." At the same time, South Africa has participated in negotiations for a new cyber crime treaty, which is a Russian initiative, although South Africa appears to be playing a mediating role between the two camps, looking to find a compromise between them on this issue.[88]

South Africa's position on the application of international law to cyberspace is equally unclear. South Africa was a member of the 2019–2021 GGE session, which produced a report confirming the application of international law to cyberspace while leaving open the possibility that new rules may need to be developed over time. South Africa did not, however, contribute to the GGE's compendium on voluntary national positions on the application of international law to cyberspace, which is surprising given that it was a member of the GGE at the time. Moreover, outside the GGE and OEWG processes, South Africa has not produced a national statement on the application of international law to cyberspace, as a number of states have,[89] although reportedly the African Union (of which South Africa is a member) will publish a "Common African Position on Cyber Security in Africa" in 2024.[90]

Given that South Africa has been a strong advocate for sovereignty, human rights, and sovereign equality, one could have reasonably expected it to come out in favor of the application of these principles to cyberspace, as other Global South states have. Fellow BRICS member Brazil, for example, has done so. It remains unclear whether South Africa has refused to issue such a statement because Russia may have called on states to boycott these initiatives and push for new international law on cyberspace,[91] or whether it has not done so simply because it does not regard the issue as a top priority.

Conclusion

Since its democratic transition, South Africa has faced a number of significant political, economic, and social challenges. These challenges have reasonably been prioritized above cybersecurity. While South Africa has adopted a national cyber strategy and established a Cyber Command, the deprioritization of cybersecurity under successive ANC governments has meant that Cyber Command has not received the funds, resources, or political support necessary to enable South Africa to become a heavy-hitting cyber power, a position that is unlikely to change in the coming years. This is neither surprising nor uniquely a cyber issue: the same could be said more generally of South Africa's national defense.

After apartheid ended, South Africa initially presented itself to the world as a neutral and

impartial supporter of human rights, justice, democracy, and the sovereign equality of states. The bedrock of South African foreign policy has been its leading positions in the Southern African Development Community region and in the African Union. But South Africa also aspires to a more global role, particularly in Global South cooperation to redress the asymmetries of the international system. South Africa's membership in the BRICS bloc, set against the broader contestation between the West and China and Russia, is simultaneously an expression of this agenda and an indication of the difficulty of continuing to cultivate a nonaligned status in an increasingly polarized world.

South Africa has increasingly expressed support for China and Russia, irritating the West. South Africa is therefore increasingly seen in the West as walking a delicate line between maintaining neutrality and supporting authoritarianism. Its abstention from UN efforts to condemn Russia's invasion of Ukraine, as well as other acts seen as supportive of Russia since the invasion, indicate to Western critics that South Africa has lost sight of its neutral and nonaligned status and is drifting toward Russia. It should be noted that this view differs from those of the South African presidency in Pretoria and the ANC headquarters in Johannesburg. Ukraine is a more distant issue for South Africa than it is for NATO. This geographic distance, as well as South Africa's deeply entrenched skepticism about the role of the West in the international system, enables the country to adopt a more pragmatic indifference.

Viewed against this backdrop, South Africa can be a partner for like-minded states in cyber diplomacy. But it must be approached on its own terms, and like-minded states must be mindful of the limits of Western influence and of the persistence of historical baggage that the West might not feel it carries but that the ANC has not forgotten. Civil society has some influence on the South African government and contains different currents of opinion, but the issues of cyber diplomacy do not have high salience domestically. In this context, like-minded states should coordinate to pursue a sustained cyber capacity-building agenda across a wide spectrum of activities in South Africa. This could not only elevate South African cybersecurity capacity domestically but also help support the growth of like-minded views on cyber diplomacy within South Africa.

It is unclear whether South Africa's closer association with Russia will spill over into the cyber governance sphere. South Africa has refused to be drawn on whether it will support like-minded states in maintaining the existing, multistakeholder approach to cyber governance or will instead side with the sovereigntist camp advocated by China and Russia. Equally, South Africa has said little about how cyberspace should be regulated going forward: that is, whether existing international law is sufficient (as maintained by like-minded states) or whether new legal initiatives should be developed (as argued by China and Russia). All this implies that there is still time to influence the future shape and direction of South African cyber diplomacy.

About the Authors

Dr. Joe Devanny is a lecturer in the Department of War Studies at King's College London. He was a 2022–2023 British Academy Innovation Fellow at the UK Foreign, Commonwealth and Development Office. He writes here in a personal capacity. Follow him on X, @josephdevanny.

Dr. Russell Buchan is a professor of international law at the University of Reading School of Law. He was a 2022–2023 British Academy Innovation Fellow at the UK Foreign, Commonwealth and Development Office. He writes here in a personal capacity. Follow him on X, @russellbuchan.

Notes

1 Evan Lieberman, *Until We Have Won Our Liberty: South Africa After Apartheid* (Princeton, NJ: Princeton University Press, 2022).

2 Alan Hirsch, *Season of Hope: Economic Reform Under Mandela and Mbeki* (Pietermaritzburg: University of KwaZulu-Natal Press, 2005); and Pippa Green, *Choice, Not Fate: The Life and Times of Trevor Manuel* (Johannesburg: Penguin South Africa, 2008).

3 Brian Levy, Alan Hirsch, Vinothan Naidoo, and Musa Nxele, "South Africa: When Strong Institutions and Massive Inequalities Collide," Carnegie Endowment for International Peace, March 18, 2021, https://carnegieendowment.org/2021/03/18/south-africa-when-strong-institutions-and-massive-inequalities-collide-pub-84063; and Richard Calland and Mabel Sithole, *The Presidents: From Mandela to Ramaphosa, Leadership in the Age of Crisis* (Johannesburg: Penguin South Africa, 2022).

4 Jacques Pauw, *The President's Keepers: Those Keeping Zuma in Power and Out of Prison* (Cape Town: Tafelberg, 2017); and Adriaan Basson and Pieter du Toit, *Enemy of the People: How Jacob Zuma Stole South Africa and How the People Fought Back* (Johannesburg: Jonathan Ball, 2017). Allegations of corruption did not start during Zuma's presidency. See, for example, Andrew Feinstein, *After the Party: A Personal and Political Journey Inside the ANC* (Johannesburg: Jonathan Ball, 2007).

5 "The World Bank in South Africa," World Bank, last updated September 14, 2023, https://www.worldbank.org/en/country/southafrica/overview.

6 This is the rationale for external cyber capacity-building assistance, such as the United Kingdom government's Digital Access Programme in South Africa. See "Leaving No One Behind in a Digital World: The United Kingdom's Digital Access Programme," Organisation for Economic Co-operation and Development, December 20, 2021, https://www.oecd.org/development-cooperation-learning/practices/leaving-no-one-behind-in-a-digital-world-the-united-kingdom-s-digital-access-programme-e8b15982.

7 Simnikiwe Mzekandaba, "Cyber Crime's Annual Impact on SA Estimated at R2.2bn," ITWeb, April 4, 2023, https://www.itweb.co.za/content/JN1gPvOAxY3MjL6m.

8 Jaco Hoffman, "'Leapfrog Technology': Locating Older (South) Africans at the ICT Interface" in Vera Roos and Jaco Hoffman (eds), *Age-Inclusive ICT Innovation for Service Delivery in South Africa* (New York: Springer, 2022).

9 Faustine Ngila, "South Africa Is the World's Most Internet-Addicted Country," Quartz, March 29, 2023, https://qz.com/south-africa-the-worlds-most-internet-addicted-country-1850278160.

10 Ngila, "South Africa Is the World's Most Internet-Addicted Country."

11 "The World Bank in South Africa," World Bank.

12 "SA Has Highest Number of Ransomware and Email Attacks in Africa," Seacom, January 20, 2023, https://seacom.co.za/business-insights/sa-has-highest-number-of-ransomware-and-email-attacks-in-africa.

13 "Ransomware Hits More Than Half of SA Companies," IT-Online, May 9, 2022, https://it-online.co.za/2022/05/09/ransomware-hits-more-than-half-of-sa-companies.

14 Mzekandaba, "Cyber Crime's Annual Impact on SA Estimated at R2.2bn."

15 Mandisa Ndlovu, "Spyware Attacks in South Africa Increase by 18.8%," *Mail and Guardian*, May 19, 2023, https://mg.co.za/article/2023-05-19-spyware-attacks-in-south-africa-increase-by-18-8.

16 "Ransomware Hits Johannesburg Electricity Supply," BBC News, July 26, 2019, https://www.bbc.co.uk/news/technology-49125853.

17 "South Africa's Life Healthcare Hit by Cyber Attack," Reuters, June 9, 2020, https://www.reuters.com/article/us-life-healthcare-cyber-idUSKBN23G0MY.

18 Ahmore Burger-Smidt, "Massive Data Breach in SA: Did Experian Do Enough?," Independent Online, September 3, 2020, https://www.iol.co.za/business-report/opinion/massive-data-breach-in-sa-did-experian-do-enough-24426a71-c3d0-44cf-9c00-fbf53f8beb63.

19 "SA Ill-Equipped for Cyberwarfare – With Limited Money, Manpower, and Tech Expertise," News24, September 26, 2022, https://www.news24.com/news24/bi-archive/south-africa-open-to-cyberwarfare-as-defence-force-runs-out-of-money-2022-9.

20 "Justice Department's IT System Brought Down in Ransomware Attack," News24, September 9, 2021, https://www.news24.com/news24/southafrica/news/justice-departments-it-system-brought-down-in-ransomware-attack-20210909.

21 "Answers Sought on Apparent SA Defence Cyber Attack," defenceWeb, August 26, 2023, https://www.defenceweb.co.za/sa-defence/sa-defence-sa-defence/answers-sought-on-apparent-sa-defence-ict-ransomware-attack; and "SNATCHed – SANDF Data Leaked in Cyberattack Appears to Be Authentic, Say Cybersecurity Analysts," *Daily Maverick*, September 6, 2023, https://www.dailymaverick.co.za/article/2023-09-06-snatched-sandf-data-leaked-in-cyberattack-appears-to-be-authentic-say-cybersecurity-analysts.

22 Sibongile Khumalo, "Cybercriminals in 'Concerted Effort' to Target SA's Critical Infrastructure," News24, June 1, 2022, https://www.news24.com/fin24/companies/cybercriminals-in-concerted-effort-to-target-sas-critical-infrastructure-20220601.

23 Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London: Hurst, 2022).

24 "SA Ill-Equipped for Cyberwarfare," News24.

25 Uchenna Jerome Orji, "Interrogating African Position on State Sponsored Cyber Operations: A Review of Regional and National Policies and Legal Responses," *Baltic Yearbook of International Law* 20, no. 1 (2022): 236, https://brill.com/view/journals/byio/20/1/article-p236_12.xml?language=en.

26 "National Cyber Power Index 2022," Belfer Center for Science and International Affairs, 2022, https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

27 Angelique Chrisafis, Dan Sabbagh, Stephanie Kirchgaessner, and Michael Safi, "Emmanuel Macron Identified in Leaked Pegasus Project Data," *Guardian*, July 20, 2021, https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data.

28 Simon Allison, "South African Phones Targeted by Notorious 'Governments Only' Spyware," *Mail and Guardian*, October 2, 2018, https://mg.co.za/article/2018-10-02-south-african-phones-targeted-by-notorious-governments-only-spyware; and Craig Timberg, Michael Birnbaum, Drew Harwell, and Dan Sabbagh, "On the List: Ten Prime Ministers, Three Presidents and a King," *Washington Post*, July 20, 2021, https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware.

29 Staff Reporter, "Zuma's Legal Team 'Has Mbeki, McCarthy on Tape,'" *Mail and Guardian*, March 26, 2009, https://mg.co.za/article/2009-03-26-zumas-legal-team-has-mbeki-mccarthy-on-tape; and "Jacob Zuma 'Spy Tapes' Given to South Africa's Helen Zille," BBC News, September 14, 2014, https://www.bbc.co.uk/news/world-africa-29059479.

30 Ewen MacAskill, Nick Davies, Nick Hopkins, Julian Borger, and James Ball, "GCHQ Intercepted Foreign Politicians' Communications at G20 Summits," *Guardian*, June 17, 2013, https://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits.

31 Jane Duncan, *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa* (Johannesburg: Wits University Press, 2018).

32 Jane Duncan, "South Africa's Surveillance Law Is Changing but Citizens' Privacy Is Still at Risk," *Conversation*, October 8, 2023, https://theconversation.com/south-africas-surveillance-law-is-changing-but-citizens-privacy-is-still-at-risk-214508.

33 Pierre de Vos, "New Intelligence Bill Is Anti-democratic, and a Unique Mix of Malice and Stupidity," *Daily Maverick*, September 7, 2023, https://www.dailymaverick.co.za/article/2023-09-07-new-intelligence-bill-is-a-unique-mix-of-malice-and-stupidity.

34 "COSATU Rejects the General Intelligence Laws Amendment Bill's Shocking Undermining of the Constitution," Congress of South African Trade Unions, August 17, 2023, http://mediadon.co.za/2023/08/17/cosatu-rejects-the-general-intelligence-laws-amendment-bills-shocking-undermining-of-the-constitution; Heidi Swart, "Rica and Gilab – the Two Surveillance Bills Before Parliament That Should Give Every Freedom-Loving South African Pause for Thought," *Daily Maverick*, October 3, 2023, https://www.dailymaverick.co.za/article/2023-10-03-rica-and-gilab-the-two-surveillance-bills-before-parliament-that-should-give-every-freedom-loving-south-african-pause-for-thought; and Paul Hoffman, "The GILA Bill Is Unconstitutional," PoliticsWeb, October 12, 2023, https://www.politicsweb.co.za/opinion/the-general-intelligence-laws-amendment-bill-is-un.

35 Craig Kotze, "SA's New 'Spy Bill' Lacks Sufficient Checks and Balances, Civilian Oversight – ISS," defenceWeb, October 25, 2023, https://www.defenceweb.co.za/editors-pick/sas-new-spy-bill-lacks-sufficient-checks-and-balances-civilian-oversight-iss; and Murray Hunter, "RICA Bill Misses the Chance for Real Reform," GroundUp, September 20, 2023, https://www.groundup.org.za/article/rica-bill-misses-chance-for-real-reform.

36 High-Level Review Panel on the State Security Agency, "High Level Review Panel Report on the State Security Agency," South African Government, December 2018, https://www.gov.za/sites/default/files/gcis_document/201903/high-level-review-panel-state-security-agency.pdf; and Hunter, "RICA Bill Misses the Chance for Real Reform."

37 "Report V Volume I: State Security Agency and Crime Intelligence," Judicial Commission of Inquiry into State Capture, June 22, 2022, 1–376, https://www.statecapture.org.za/site/files/announcements/667/OCR_version_-_State_Capture_Commission_Report_Part_V_Vol_I_-_SSA.pdf.

38 High-Level Review Panel on the State Security Agency, "High Level Review Panel Report on the State Security Agency."

39 "Department of Defence Strategic Plan for 2020–2025," Parliament of the Republic of South Africa, February 2020, 28, https://www.parliament.gov.za/storage/app/media/Docs/tpap/5a2878b3-e7a0-4568-87d8-776234e41173.pdf.

40 One commentator explains that for South Africa, cybersecurity is seen as "nice to have" rather than a main national security priority. See Karen Allen, "Cyber Diplomacy and Africa's Digital Development," Institute for Security Studies, January 2022, 2, https://issafrica.s3.amazonaws.com/site/uploads/ar-38.pdf.

41 State Security Agency, "National Cybersecurity Policy Framework," South African Government, December 4, 2015, https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf.

42 State Security Agency, "National Cybersecurity Policy Framework," 15.

43 The SSA was responsible for drafting the NCPF.

44 "FIRST Members Around the World," Forum of Incident Response and Security Teams, accessed November 30, 2023, https://www.first.org/members/map#country%3AZA.

45 The NCPF tasked the Department of Defence with formulating a cyber warfare strategy, but this has not yet been submitted to the Justice, Crime Prevention and Security Cluster.

46 State Security Agency, "National Cybersecurity Policy Framework," 94.

47 Elmarie Biermann and Noëlle van der Waag-Cowling, "Mind the Gap: Addressing South Africa's Cybersecurity Skills Shortage," *Daily Maverick*, July 13, 2018, https://www.dailymaverick.co.za/article/2018-07-13-mind-the-gap-addressing-south-africas-cybersecurity-skills-shortage.

48 State Security Agency, "National Cybersecurity Policy Framework," 82.

49 "Cybercrimes and Cybersecurity Bill," Cybercrime.org.za, 2015, section 54(3)(a)(i), https://cybercrime.org.za/docs/Cybercrimes_and_Cybersecurity_Bill_2015.pdf.

50 "Cybercrimes and Cybersecurity Bill," Cybercrime.org.za.

51 "Funding Mars SANDF Cyber Command," *Military Africa*, January 13, 2023, https://www.military.africa/2023/01/funding-mars-sandf-cyber-command.

52 "SANDF Cyber Command Operating in 'Limited Space,'" defenceWeb, January 5, 2023, https://www.defenceweb.co.za/featured/sandf-cyber-command-operating-in-limited-space.

53 For example, Mandela explained that the protection of human rights would be "the light that guides our foreign affairs." See Nelson Mandela, "South Africa's Future Foreign Policy," *Foreign Affairs*, December 1, 1993, https://www.foreignaffairs.com/articles/south-africa/1993-12-01/south-africas-future-foreign-policy.

54 See, for example, Christopher Williams, "Re-Evaluating South African Foreign Policy Decision-Making: Archives, Architects and the Promise of Another Wave," *Politikon* 48, no. 4 (2021): 547–571, https://doi.org/10.1080/02589346.2021.1991658.

55 "South Africa's Diplomatic Descent," *Economist*, February 23, 2023, https://www.economist.com/leaders/2023/02/23/south-africas-diplomatic-descent.

56 "South Africa's Foreign Policy Under Ramaphosa," International Institute for Strategic Studies, April 2021, https://www.iiss.org/publications/strategic-comments/2021/south-africas-foreign-policy-under-ramaphosa.

57 "South Africa's Diplomatic Descent," *Economist.*

58 Jon Temin and Richard Calland, "Can South Africa Return to the Global Stage?," Center for Strategic and International Studies, December 17, 2018, https://www.csis.org/analysis/can-south-africa-return-global-stage. For a more nuanced appraisal of South African foreign policy, particularly from Mbeki onward, see Adekeye Adebajo and Kudrat Virk (eds), *Foreign Policy in Post-Apartheid South Africa: Security, Diplomacy and Trade* (London: IB Tauris, 2017); Adam Habib, "South Africa's Foreign Policy: Hegemonic Aspirations, Neoliberal Orientations and Global Transformation," *South African Journal of International Affairs* 16, no. 2 (2009): 143–159; and Elizabeth Sidiropoulos, "South African Foreign Policy in the Post-Mbeki Period," *South African Journal of International Affairs* 15, no. 2 (2008): 107–120.

59 Sidiropoulos, "South African Foreign Policy in the Post-Mbeki Period."

60 Merle Lipton, "Understanding South Africa's Foreign Policy: The Perplexing Case of Zimbabwe," *South African Journal of International Affairs* 16, no. 3 (2009): 331–346, https://doi.org/10.1080/10220460903495181; and Joe Devanny, "The European Union Has Failed on Zimbabwe — but It's Not Too Late to Change Course," *Mail and Guardian*, February 6, 2019, https://mg.co.za/article/2019-02-06-00-the-european-union-has-failed-on-zimbabwe-but-its-not-too-late-to-change-course.

61 Richard Goldstone and Mark Kersten, "Ramaphosa Has a Rare Chance to Stop SA Withdrawing From the ICC," *Mail and Guardian*, June 12, 2018, https://mg.co.za/article/2018-06-12-ramaphosa-has-a-rare-chance-to-stop-sa-withdrawing-from-the-icc; and Julian Borger, "South Africa's President and ANC Sow Confusion Over Leaving ICC," *Guardian*, April 25, 2023, https://www.theguardian.com/world/2023/apr/25/south-africas-president-and-party-sow-confusion-over-leaving-icc.

62 See, for example, Vladimir Shubin, *ANC: A View From Moscow* (Johannesburg: Jacana Media, 2017).

63 Habib, "South Africa's Foreign Policy."

64 Sarah Brockmeier, Oliver Stuenkel, and Marcos Tourinho, "The Impact of the Libya Intervention Debates on Norms of Protection," *Global Society* 30, no. 1 (2016): 113–133, https://doi.org/10.1080/13600826.2015.1094029.

65 UN General Assembly, Resolution A/ES-11/1, "Aggression Against Ukraine," March 2, 2022, https://digitallibrary.un.org/record/3965290?ln=en.

66 UN General Assembly, Resolution A/ES-11/L.7, "Principles of the Charter of the United Nations Underlying a Comprehensive, Just and Lasting Peace in Ukraine," February 16, 2023, para. 5, https://digitallibrary.un.org/record/4004933?ln=en.

67 UN General Assembly, Resolution ES-11/3, "Suspension of the Rights of Membership of the Russian Federation in the Human Rights Council," April 7, 2022, https://press.un.org/en/2022/ga12414.doc.htm.

68 Carien du Plessis, "South Africa Defends Planned Drills With Russia and China," Reuters, January 23, 2023, https://www.reuters.com/world/africa/russias-lavrov-visits-ally-south-africa-amid-western-rivalry-2023-01-23.

69 Mark Stone, "It's a Serious Issue: White House Responds to Claims South Africa Passed Weapons to Russia," Sky News, May 12, 2023, https://news.sky.com/story/its-a-serious-issue-white-house-responds-to-claims-south-africa-passed-weapons-to-russia-12879320.

70 Sarah Carter, "South Africa Moves to Let Putin Attend BRICS Summit Despite ICC Arrest Warrant Over Ukraine War," CBS News, May 30, 2023, https://www.cbsnews.com/amp/news/south-africa-vladimir-putin-icc-arrest-warrant-ukraine-war-brics-immunity.

71 Owen Bowcott, "Sudan President Omar al-Bashir Leaves South Africa as Court Considers Arrest," *Guardian*, June 15, 2015, https://www.theguardian.com/world/2015/jun/15/south-africa-to-fight-omar-al-bashirs-arrest-warrant-sudan.

72 "South Africa's Diplomatic Descent," *Economist*.

73 South Africa's foreign minister said that the country is resisting "becoming embroiled in the politics of confrontation and aggression that has been advocated by the powerful countries" and instead asserting its "independent, non-aligned views." See Naledi Pandor, "Statement by the Minister of International Relations and Cooperation, Dr Naledi Pandor, During the Media Briefing on the Russia / Ukraine Conflict," International Relations and Cooperation Department of South Africa, April 8, 2022, https://www.dirco.gov.za/statement-by-the-minister-of-international-relations-and-cooperation-dr-naledi-pandor-during-the-media-briefing-on-the-russia-ukraine-conflict-08-april-2022.

74 Pandor, "Statement by the Minister of International Relations and Cooperation."

75 Pandor, "Statement by the Minister of International Relations and Cooperation."

76 "With 143 Votes in Favour, 5 Against, General Assembly Adopts Resolution Condemning Russian Federation's Annexation of Four Eastern Ukraine Regions," United Nations, October 12, 2022, https://press.un.org/en/2022/ga12458.doc.htm.

77 "South Africa to Investigate US Allegation of Arms Shipment to Russia," Reuters, May 30, 2023, https://www.reuters.com/world/south-africa-investigate-us-allegations-arms-shipment-russia-2023-05-28.

78 John Eligon and Lynsey Chutel, "South African Inquiry Rebuts U.S. Charge on Russian Arms," *New York Times*, September 3, 2023, https://www.nytimes.com/2023/09/03/world/africa/south-african-inquiry-russia-ship.html.

79 Cameron Scheijde, "South Africa's Slow Embrace of Russia Should Cause Alarm for the West," Foreign Policy Centre, May 18, 2023, https://fpc.org.uk/south-africas-slow-embrace-of-russia-should-cause-alarm-for-the-west.

80 Quoted in Scheijde, "South Africa's Slow Embrace of Russia."

81 Ramaphosa said, "The war could have been avoided if NATO had heeded the warnings amongst its own leaders and officials over the years that its eastward expansion would lead to greater, not less, instability in the region." Quoted in Reuters, Gadi Zaig, and *Jerusalem Post* Staff, "South African President Blames NATO for Russia-Ukraine War," *Jerusalem Post*, March 17, 2022, https://www.jpost.com/international/article-701571.

82 Scheijde, "South Africa's Slow Embrace of Russia."

83 Thapelo Tselapedi, "South Africa Walks a Tightrope of International Alliances – It Needs Russia, China and the West," *Conversation*, May 11, 2023, https://theconversation.com/south-africa-walks-a-tightrope-of-international-alliances-it-needs-russia-china-and-the-west-204052; and "China and South Africa Holds Talks on Trade and Investment in Preparation for State Visit by President Xi Jinping," South African Department of Trade, Industry and Competition, August 11, 2023, http://www.thedtic.gov.za/china-and-south-africa-holds-talks-on-trade-and-investment-in-preparation-for-state-visit-by-president-xi-jinping.

84 Tim Maurer and Robert Morgus, "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate," Centre for International Governance Innovation, May 2014, https://web.archive.org/web/20140620172535/http://www.cigionline.org/sites/default/files/no7_2.pdf; and Robert Morgus, Jocelyn Woolbright, and Justin Sherman, "The Digital Deciders," New America, October 23, 2018, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders.

85 Julia Pohle and Thorsten Thiel, "Digital Sovereignty," *Digital Sovereignty* 9 (2020): 1, 5, https://policyreview.info/concepts/digital-sovereignty.

86 Interestingly, South Africa has not signed the African Union Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention.

87 "Joint Statement by South Africa and the Netherlands: Cyber Policy Dialogue," Government of the Netherlands, April 6, 2022, https://www.government.nl/documents/diplomatic-statements/2022/04/06/south-africa-netherlands-cyber-policy-dialogue-joint-statement.

88 "National Statement by the Republic of South Africa," UN Office on Drugs and Crime, February 28–March 11, 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/South_Africa.pdf.

89 Although, as Uchenna Jerome Orji observes, "no African State has clearly stated its position on the applicability of existing international law to State sponsored cyber operations." See Orji, "Interrogating African Position on State Sponsored Cyber Operations," 265.

90 "The African Union Takes Significant Steps Towards Establishing a Common African Position on the Application of International Law to Cyberspace," African Union, June 30, 2023, https://au.int/en/pressreleases/20230630/african-union-takes-significant-steps-towards-establishing-common-african.

91 "Commentary of the Russian Federation on the Initial 'Pre-Draft' of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations, April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers around the world. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Technology and International Affairs

The Carnegie Technology and International Affairs Program (TIA) helps governments and industries reduce large-scale international risks of new technologies and related services. Recognizing that commercial actors control many of the most germane technologies, TIA identifies best practices and incentives that can motivate industry stakeholders to pursue growth by enhancing rather than undermining international relations.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org