STRATEGIC INVESTMENT AS A GEO-STRATEGIC RUSE

American positioning in South and Southern Africa

Andre Zaaiman | 21 May 2026

Abstract

This paper argues that the contemporary pattern of United States investment in South and Southern Africa is not adequately explained by commercial logic. It is shaped by three compounding facts. First, the United States is positioning to dominate South Africa's ***digital infrastructure****, energy, and financial strategic infrastructure, as the investment pattern of the past decade shows. Second, that positioning is designed to deny China the same access. Third, the South African economy is neither securitised nor secured, even as the West has firmly settled into a logic of war, driven by anxiety about its civilisational decline and the unravelling of a global order built on four centuries of Western-Christian primacy. The digital infrastructure question is doubly weighted: in contemporary political economy, AI compute, data, cloud, payments rails, and platform systems constitute what is now termed the New Productive Forces – the principal engines of 21st-century growth and competitiveness. Vulnerability at this layer therefore severely restricts current and future economic development. Drawing on the public language of the U.S. International Development Finance Corporation (DFC), which describes its work as economic statecraft aimed at strategic competition with China, and on the empirical record of U.S. capital flows into South African digital infrastructure, energy, critical minerals, logistics, and financial systems, the paper develops the case that these investments function as instruments of geo-strategic positioning. The framework draws on FARRELL and NEWMAN's theory of weaponised interdependence, BUCHANAN's analysis of cyber operations as instruments of state competition, and DENARDIS's account of infrastructure as political architecture. The Denel PMP overture by the Texas-based firm Omusha, reported by DefenceWeb in May 2026, is read as a symptomatic case rather than an anomaly. The paper then presents a case study of how control over digital infrastructure has historically created vulnerabilities exploited by the United States and Israel to surveil, destabilise, and shape political outcomes in third states.*

1. Introduction: The Denel PMP Overture and the Three Frames

On 18 May 2026, DefenceWeb reported that Omusha, a Texas-based defence and security firm, was pursuing a hundreds-of-millions-of-rand investment in Denel PMP to 'restore production, create jobs, modernise operations, and ultimately export ammunition' (MARTIN, 2026). The proposal was framed to disarm scepticism: a fixed-term lease-and-operate arrangement; Black Economic Empowerment treated as a structural requirement; a majority South African executive team; and continued oversight by Denel, the Ministry of Defence, and the National Conventional Arms Control Committee. The Managing Director, Daniel SERRALDE, acknowledged critics directly: South Africa, he said, has every reason to guard its sovereign capabilities carefully and should reject any arrangement that turns local assets into market-access vehicles while value, skills, and decision-making move elsewhere – but, he insisted, 'that is not this proposal' (MARTIN, 2026).

The framing is careful. It anticipates every standard South African objection and concedes each in advance. That carefulness is itself the analytical entry point. South African ammunition manufacture is not ordinary commerce. The question this paper poses is what this proposal exemplifies. The argument is that it exemplifies a wider pattern in which strategic investment functions as a geo-strategic ruse: a vehicle through which a foreign state, working through private actors and public finance instruments, acquires structural positions in the host state's critical infrastructure that would not be ceded if the request were made openly.

Three claims frame the paper and are returned to in the conclusion:

- **First**, the United States is positioning to **dominate the digital infrastructure, energy, and financial strategic infrastructure** of South Africa, with the digital layer the most advanced front. The contest is no longer over factories and bases; it is over cloud regions, subsea cable landings, data centres, AI compute, payment plumbing, mining finance, and ESG pricing.
- **Second**, the purpose of this positioning is to **deny China** the same access, in line with the explicit doctrine articulated by the DFC and U.S. national security agencies (DFC, 2026a, 2026b, 2026c, 2026e).
- **Third**, the South African economy is **neither securitised nor secured**. This creates a major strategic and national-security vulnerability at the moment when the West is firmly in a logic of war, driven by anxiety about its civilisational decline and the unravelling of a global order based on four centuries of Western-Christian domination. That order has been pushed over the brink by Western entanglement with the apartheid Israeli regime now charged before the International Court of Justice, by the dynastic and ostentatious Trump family regime in Washington, and by the duplicitous Western role in the Ukrainian misadventure that is dragging the United States and Europe toward direct conflict with Russia.

Digital infrastructure is the leading edge, and it carries a weight beyond what its name suggests. In contemporary political economy, the cloud, AI compute, data, platform, and payments layers are what the Chinese strategic literature names the New Productive Forces and what Western policy documents increasingly describe as the 'critical and emerging technologies' base: the principal engines of 21st-century productivity, innovation, and competitiveness. A host state without

sovereign control over these layers is a host state whose current and future economic development is capped from outside. The U.S. footprint already concentrates in cloud, AI, subsea cable, and cybersecurity layers (DFC, 2026d; Carnegie Endowment, 2022). The informational and entertainment layer of the South African public sphere has, in parallel, been penetrated by France: in September 2025 Canal+ completed its $3 billion acquisition of MultiChoice, owner of DStv, GOtv, Showmax, and SuperSport, taking effective control of Africa's largest pay-television group, with the delisting of MultiChoice from the Johannesburg Stock Exchange completed in December 2025 (Daily Post Nigeria, 2025; BusinessTech, 2025; Daily Investor, 2026). The combined entity now serves more than 40 million subscribers across about 70 countries. The architecture of foreign control over the South African public sphere – data, narrative, and pay-television – is being consolidated on multiple fronts at the same time.

An accompanying analytical reference is the Drop Site News piece circulated on 19 May 2026, 'From Mutual Suspicion to Political Embrace: How the U.S. learned to stop worrying and embrace Pakistan' by Waqas AHMED, Murtaza HUSSAIN, and Ryan GRIM (AHMED, HUSSAIN & GRIM, 2026). That piece documents how the United States, having identified a convergence of interests, can rapidly transform a strained bilateral relationship into one of deep structural embedding, with investment flows and strategic access running ahead of any public acknowledgement of the shift. The South African case follows a comparable grammar: investments arrive first, the strategic logic is disclosed only afterwards, and only partially.

2. The DFC and the Public Doctrine of Economic Statecraft

The most important institutional actor in this pattern is the U.S. International Development Finance Corporation (DFC), the international investment arm of the U.S. government, established by the BUILD Act of 2018 and reauthorised in 2025 with an investment ceiling raised from US$60 billion to US$205 billion (Congressional Research Service, 2025; DFC, 2026b). The DFC has been candid in describing its mission. Its CEO, Ben BLACK, told the Council on Foreign Relations in April 2026 that the agency had been tasked with 'resurrecting American economic statecraft' (DFC, 2026a). At the Milken Institute in March 2026, BLACK framed the agency's priorities as energy, critical minerals, and information technology and communications, and described DFC investments as filling a 'shopping list' for the U.S. government covering rare earths and other critical mineral inputs (DFC, 2026b). At the Hill & Valley Forum in March 2026, BLACK described economic statecraft as part of 'the new arsenal of influence' (DFC, 2026c).

The DFC's self-description is explicit. Investments are framed as instruments of:

- supply-chain security;
- energy resilience;
- strategic competition with China; and
- economic statecraft as the 'new arsenal of influence'.

The strategic domains repeatedly named by the agency are:

- critical minerals;
- energy;
- technology and telecommunications;
- infrastructure and logistics; and
- digital infrastructure.

The agency's public materials describe its Sub-Saharan Africa priority as 'strengthening strategic competition through investments in Africa's digital economy' (DFC, 2026d). These domains map closely onto the sectors in which American capital has concentrated in South Africa over the past decade.

Two observations follow. First, the DFC does not present its mandate in the language of development assistance. It presents it in the language of statecraft, with investment as the primary instrument. Second, the public framing of countering China provides a doctrinal cover under which the operational requirement is structural embedding in the host state's infrastructure. This is what FARRELL and NEWMAN (2019, pp. 54–57) call the construction of network 'chokepoints' and 'panopticons': positions of asymmetric jurisdictional control from which a state can subsequently surveil or coerce others transiting the network.

3. The Economic Domain as the Decisive Theatre

Classical strategic studies treated the economy as the base for military power. Contemporary U.S. doctrine treats it as the primary theatre of competition. BLACK's remark at the Tulane Corporate Law Institute is the canonical statement: economic security is national security, and resilient supply chains free from adversary chokepoints are crucial (DFC, 2026e). This inversion is not rhetorical. It reflects the recognition that the economic rise of China is the principal long-term threat to U.S. primacy, and that the contest will be decided in supply chains, standards, financial plumbing, compute capacity, and data architecture before it is decided in any kinetic theatre.

This decisive economic theatre is now organised around what the Chinese strategic literature calls the New Productive Forces (xin zhi shengchanli): AI compute, data, cloud, advanced biotechnology, advanced manufacturing, green energy, and the platform economy. Whichever state controls the New Productive Forces at the layer of digital infrastructure controls the rate at which other states can grow, innovate, and develop. A host state whose digital infrastructure sits under foreign jurisdiction does not merely face a surveillance problem. It faces a development ceiling. Its ability to absorb AI productivity gains, build sovereign data assets, run independent industrial policy, or compete in the next generation of tradable services is set abroad. Vulnerability at the New Productive Forces layer is therefore a direct constraint on current and future economic growth.

Economic security on this account requires the securitisation of the national economy:

- its developmental potential;

- its critical infrastructure;
- its competitive-advantage clusters;
- its intellectual property; and
- its resource base – including critical minerals and bio-information such as seed banks and germplasm.

FARRELL and NEWMAN's (2019) theoretical contribution is that states which already occupy hub positions in global financial, informational, and communications networks – the United States being the paradigmatic case – possess two distinct mechanisms of coercive leverage. The first is the panopticon effect, in which jurisdictional control over a hub permits comprehensive surveillance of all traffic transiting it. The second is the chokepoint effect, in which the same control permits selective denial of access (FARRELL & NEWMAN, 2019, pp. 54–57). Both were demonstrated in the operationalisation of SWIFT against Iran and Russia and in the export-control architecture targeting Chinese semiconductors.

The geo-economic dimension is not confined to the United States. As argued in ZAAIMAN (2026b), France is repositioning across the Eastern Rim of Africa – through the Djibouti naval footprint, the Mozambique Channel, the Mayotte and Réunion perimeter, and the Africa Forward Summit hosted in Nairobi on 11–12 May 2026 – to occupy chokepoint positions on the Indian Ocean trade routes carrying critical minerals, hydrocarbons, and digital traffic out of the African interior. France's Canal+ acquisition of MultiChoice forms one tine of a broader European chokepoint strategy that complements rather than competes with the American economic statecraft model. The combined pressure on Southern Africa from American digital and financial positioning, French informational and chokepoint positioning, and Israeli cyber and narrative positioning is the geo-economic context within which the Denel PMP overture must be read.

The doctrinal frame for France's digital push was set out by President MACRON at the Nairobi summit. Speaking alongside President RUTO at the University of Nairobi on 12 May 2026, MACRON called for stronger technology and energy cooperation between Africa and Europe and urged both continents to reduce their dependence on American and Chinese technologies (Anadolu Agency, 2026; The Standard, 2026). The principal operational vehicle announced was the expansion of the Orange Digital Centres network from 50 to 100 sites across Africa and the Middle East, with a stated target of training more than three million young people by 2030 in artificial intelligence, cybersecurity, cloud computing, and digital entrepreneurship, and supporting more than 500 startups across healthcare, agriculture, fintech, education, and e-commerce (Developing Telecoms, 2026; iAfrica, 2026). A bilateral Kenya–France pact on digital skills and youth empowerment was concluded at the summit, including a new University of Nairobi Science and Engineering Complex partnership presented as a regional research hub (The Standard, 2026). A comparable engagement template is being extended to Ethiopia through Orange-anchored training and innovation infrastructure on the Horn of Africa flank.

Two analytical points follow. First, the training programme is not skills assistance in isolation. It is jurisdictional positioning: a French-domiciled telecommunications operator becomes the

standard-setting interface between African youth and the AI, cloud, and cybersecurity stacks they enter their working lives on, with curricula, certifications, platform partnerships, and downstream employer relationships routed through Paris. The panopticon and chokepoint logic that FARRELL and NEWMAN (2019) identify in financial and informational networks applies equally to skills and certification networks at scale. Second, MACRON's explicit framing – reducing African dependence on American and Chinese technologies – is a competitive bid against both blocs, not a complementary one. It establishes France, with the European Union behind it, as a third claimant on African **digital infrastructure** sovereignty, with the same instruments – training, platform, finance, and ecosystem – deployed against the same host states.

BUCHANAN (2020) extends the argument in the digital domain. He theorises the 'home-field advantage' the United States enjoys due to its jurisdictional control over the internet's physical and logical infrastructure, and shows how Washington has used this structural position for espionage, sabotage, and political shaping below the threshold of war. DENARDIS (2014) provides the architectural theory underneath both: power in the digital domain is exercised at the layers of technical standards, routing protocols, domain name systems, interconnection agreements, and physical cable landings. Whoever controls these layers controls more than data flows; they control the conditions under which political, economic, and social life is conducted. NYE (2010) supplies the conceptual anchor that physical control over the infrastructure layer retains decisive importance even as cyberspace appears to diffuse power.

The implication for a host state such as South Africa is significant. Once foreign capital has constructed or acquired the chokepoint nodes of the South African digital economy, energy system, minerals processing chain, and financial plumbing, the panopticon and chokepoint capacities described by FARRELL and NEWMAN become structurally available to the jurisdiction in which the parent companies are domiciled. The leverage need never be exercised to be effective; its mere availability conditions political and policy choices.

4. The Pattern of U.S. Investment in South Africa, 2015–2024

Before the empirical pattern is set out, a definitional clarification is necessary. 'Investment' in this paper is not limited to financial capital. It encompasses the full repertoire through which a foreign actor acquires structural position in a host economy: equity stakes and capital expenditure, but also supplier and maintenance relationships, training and liaison programmes embedded inside host-state agencies, platform integrations, route and service operations, advisory and consulting mandates, civic and legal funding pipelines, and ecosystem-anchoring transactions such as agency acquisitions and data-centre siting. Each of these is a vehicle through which jurisdictional, operational, and informational dependency is constructed. Financial investment is the most visible vehicle; the others are typically more durable.

According to Wesgro and Financial Times fDi Markets data, American firms invested approximately US$10 billion in cumulative capital expenditure across roughly 250 projects in South Africa between 2015 and 2024 (ZAAIMAN, 2026a). The composition is the point. The largest concentration is no longer in classical industrial sectors but in **digital infrastructure**. Microsoft,

Amazon Web Services, Google, Equinix, Oracle, and Cloudflare together represent the dominant theme. Microsoft alone has announced approximately R20.4 billion invested over three years in enterprise data centres, an additional R5.4 billion in AI and cloud expansion through 2027, and a further R1.3 billion in skills and SMME programmes (ZAAIMAN, 2026a). These are not peripheral commercial investments; they constitute the operating layer of what is now the principal engine of South African productivity growth.

The framing has shifted accordingly. The language of recent investment announcements is no longer the language of outsourcing or ICT services. It is the language of:

- the AI economy and hyperscale infrastructure;
- digital sovereignty and cloud regions;
- cybersecurity and workforce digitisation;
- submarine-cable landing ecosystems; and
- regional AI and data processing for the African market.

South Africa is increasingly positioned as the African cloud hub, a submarine cable landing ecosystem, a regional AI and data processing centre, and a gateway into broader African digital markets. Automotive manufacturing – Ford's Silverton plant and its supplier ecosystem – remains substantial but is no longer the centre of gravity of the American footprint. The automotive presence has its own strategic logic, examined in section 9: it is one of the classical instruments by which a foreign industrial actor forecloses the emergence of an indigenous rival.

Layered on top of corporate investment is U.S. government strategic finance. The DFC's regional engagement intersects with the Mozambique LNG complex led by TotalEnergies with support from the U.S. Export-Import Bank; with projects in critical minerals across the Southern African manganese, platinum group metals, vanadium, rare earths, and chrome sectors; and with regional digital economy investments framed under the DFC's Sub-Saharan Africa priority of strategic competition in the digital economy (DFC, 2026d). Even where the project is regional rather than domestic, South Africa functions as the financial gateway, legal-services hub, logistics node, insurance centre, and digital backbone, so that U.S.-backed regional projects flow through Johannesburg, Cape Town, Durban, and Richards Bay.

A third layer is financial-sector exposure through BlackRock, JPMorgan Chase, Goldman Sachs, Citigroup, and Morgan Stanley, expressed through bond markets, mining finance, ESG-linked infrastructure finance, insurance markets, and renewable-energy financing. Sovereign bond spreads, insurance pricing, maritime-risk pricing, and ESG access all condition South African macroeconomic and policy space. A fourth layer is the **defence-adjacent** civilian presence of Boeing, Lockheed Martin, RTX Corporation, and Honeywell in civil aviation systems, surveillance technologies, aerospace maintenance, and **dual-use** industrial partnerships. The Denel PMP approach by Omusha sits, on this reading, not as a stand-alone proposal but as the visible edge of a much broader pattern in which the strategic-industrial layer is now being approached.

Defence-adjacent dual-use positioning is a hallmark of this model and deserves emphasis. The investment vehicles do not announce themselves as military. They are framed as commercial aviation, civil cybersecurity, AI-enabled productivity, ESG analytics, or critical mineral beneficiation. The **dual-use** character is structural: the same Microsoft platforms that run the South African banking core and government enterprise systems also run U.S. Department of Defense secure cloud workloads; the same Palantir tooling marketed for fraud detection is embedded in NATO intelligence analytics; the same AWS infrastructure that anchors the South African telco backbone hosts U.S. intelligence-community classified workloads. The stealth lies in the **dual-use** shell, not in the underlying integration.

The cumulative shape of the American footprint in South Africa is therefore not the Cold War model of bases, troops, and defence factories. It is the modern model of infrastructural and platform power: cloud infrastructure, digital ecosystems, cyber architecture, critical mineral chains, energy corridors, insurance systems, AI infrastructure, and financial flows. The U.S. government itself describes this as economic statecraft, strategic competition, and the securing of critical supply chains (DFC, 2026a, 2026b). The naive narrative – that this is ordinary commerce and that South Africa is simply attractive to investors – obscures the motive, the intention, and the agenda that the investors themselves now describe in plain language.

4.1 Training, Liaison, and Operational Partnerships with SANDF, SAPS, and the Hawks

Alongside capital flows, a less visible but structurally consequential layer of the U.S. footprint runs through training, liaison, and operational partnerships embedded inside South African defence, policing, financial-intelligence, and prosecutorial institutions. These engagements are typically presented as technical cooperation, capacity building, or counter-criminal assistance. Each transfers institutional knowledge, doctrinal templates, data flows, and operational dependencies that condition future autonomy.

The U.S.–South Africa Defense Committee (DEFCOM) is the formal bilateral instrument. The November 2024 readout from the U.S. Department of Defense records agreement covering policy and strategy, operations, training and development, acquisition and technology, with a commitment to continue the process and reconvene in the United States in 2025 (U.S. Department of Defense, 2024). The committee is the institutional anchor for U.S. engagement with SANDF doctrine, training, and acquisition processes.

At the industrial layer, the Honeywell–Denel Aviation collaboration agreement signed in October 2015 established a U.S. aerospace and avionics maintenance presence supporting more than 1,500 military and commercial platforms across the region, anchored in the Tshwane aerospace cluster (DefenceWeb, 2015). The arrangement integrates the South African **defence-adjacent** maintenance, repair, and overhaul ecosystem into U.S. supplier and support chains.

Policing and prosecutorial cooperation runs through liaison arrangements between U.S. agencies – principally the FBI, the Drug Enforcement Administration, and Homeland Security Investigations – and South African counterparts including the South African Police Service (SAPS), the Hawks

(Directorate for Priority Crime Investigation, DPCI), the National Prosecuting Authority (NPA), the South African Revenue Service (SARS), and the Financial Intelligence Centre (FIC). The cooperation domains are narcotics interdiction, cybercrime investigation, illicit financial flows, trafficking, and extradition/mutual-legal-assistance work (Financial Intelligence Centre, 2023). The operational consequence is the embedding of U.S.-defined case templates, evidentiary standards, and risk frameworks inside South African investigative and prosecutorial agencies.

A high-visibility instance was the January 2023 visit by U.S. Treasury Secretary Janet Yellen to Dinokeng Game Reserve in Gauteng, at which a U.S.–South African task force approach was announced on financial flows behind wildlife trafficking, with expanded information sharing between the FIC and U.S. financial-intelligence counterparts (Associated Press, 2023; Financial Intelligence Centre, 2023). The choice of a wildlife reserve as the launch site tied wildlife crime to anti-money-laundering, financial intelligence, and corruption networks rather than to conservation alone. The same logic extended to Operation Thunder 2025, an INTERPOL- and WCO-led operation across 134 countries in which U.S. and South African enforcement agencies participated and which produced 24 arrests in South Africa (Reuters, 2025).

Two structural features of this layer matter. First, the cooperation is concentrated at the operational nodes where U.S. liaison capability is most consequential: customs, airports, ports, banking compliance, and telecoms intercepts at Johannesburg, Durban, Cape Town, and the OR Tambo, King Shaka, and Cape Town International airport perimeters. Second, the channel is reciprocal in form but asymmetric in substance: South African agencies receive training, tooling, and intelligence inputs, while U.S. agencies acquire access to South African case data, banking-compliance reporting, and investigative intelligence. The leverage that accumulates on the U.S. side is the same weaponised-interdependence leverage that FARRELL and NEWMAN (2019) identify in financial and informational networks, applied here to law-enforcement and defence cooperation.

5. Big Tech as Dual-Use Strategic Infrastructure

The largest American investments in South Africa are effectively **dual-use** strategic infrastructure. Microsoft's South African investments exceed US$1 billion when aggregating Azure cloud regions, AI infrastructure, cybersecurity systems, enterprise government systems, and digital backbone infrastructure. Microsoft is also deeply integrated into U.S. defence, intelligence, and secure cloud systems, and markets secure defence cloud platforms, battlefield AI, intelligence fusion, and cyber-defence integration for U.S. national security agencies. The South African Microsoft footprint is not commercial IT in isolation; it forms part of broader Western cloud architecture, cyber ecosystems, AI compute infrastructure, and strategic data systems (ZAAIMAN, 2026a).

AWS occupies a structurally similar position. Its South African region represents digital sovereignty infrastructure, regional data dominance, and a strategic node in the African cloud ecosystem. Google's investments in cloud systems, AI compute, and subsea cable systems – including the Equiano cable landed at Melkbosstrand – raise the same questions of data routing, cyber control, AI compute access, and informational sovereignty that are now central to geopolitical competition

over the physical layer of the internet. The Carnegie Endowment's mapping establishes that more than ninety-five per cent of international data – financial transactions, military communications, internet traffic – transits undersea cables, and that the contest over their construction and landing points is now part of strategic competition between the United States and China (Carnegie Endowment, 2022).

American cyber firms also dominate high-end enterprise and state cybersecurity globally. Palantir Technologies, CrowdStrike, Palo Alto Networks, Fortinet, and the Microsoft security platforms are the central reference points (KLIMBURG, 2017). Palantir is deeply integrated with U.S. defence, NATO intelligence analytics, battlefield data fusion, and AI-enabled operational systems. South African banks, telecoms, logistics firms, mining houses, and elements of government increasingly depend on these American cyber ecosystems. KLIMBURG's (2017) framework treats cyberspace as a contested strategic domain whose civilian infrastructure has become a battlespace. CLARKE and KNAKE (2019) make a related point: critical digital infrastructure – power grids, financial systems, healthcare networks – remains exposed because governance has not caught up with the pace of dependence. GOLDSMITH and WU (2006) had already established the foundational point that geography, jurisdiction, and sovereignty continuously reassert themselves over digital networks, against the libertarian thesis of a borderless internet.

ZUBOFF (2019) supplies a complementary analytical layer. Her argument is that the dominant logic of contemporary digital infrastructure is not merely surveillance but behavioural modification at scale. Platform architecture is designed to predict and shape behaviour through continuous feedback. Control over the platform layer therefore translates into the capacity to produce social and political outcomes without coercion.

6. The Narrative Layer: Media, Entertainment, and the FDD Front

Control of the data and compute layers is necessary but not sufficient. Strategic positioning in a contested host state also requires shaping the narrative and public-opinion layer. In South Africa, that layer is being approached from three convergent directions.

The first is the pay-television and entertainment infrastructure. The French Canal+ acquisition of MultiChoice, completed in September 2025 with delisting from the JSE in December 2025, places DStv, GOtv, Showmax, and SuperSport under foreign control, with a 'super app' integration roadmap that will route live TV, streaming, sport, and payments through a single platform under European editorial direction (Daily Post Nigeria, 2025; BusinessTech, 2025; Daily Investor, 2026). This is the largest single shift in the South African media landscape since the unbundling of Naspers, and it has occurred largely without public strategic debate.

The second is the legacy and digital-native press. Major South African titles – including Daily Maverick, News24, and other digital outlets – operate within an ecosystem heavily shaped by American-linked philanthropic funding, training pipelines, and technology platforms. American advertising holding companies have direct municipal presence: Omnicom Media South Africa and TBWA South Africa run offices in Sandton, Woodstock, and Durban; Interpublic Group's FCB Africa

network was restructured in 2015; Accenture acquired the King James Group in 2021; and Park Advertising operates as the South African tier of the IPG global network (ZAAIMAN, 2026a). The point is not that any individual title is captured. The point is that the editorial, advertising, training, and platform infrastructure of the South African press now sits substantially within American-routed circuits, and the 'independent media' layer is structurally exposed to the same weaponised-interdependence logic as the financial and digital layers.

The third is the explicit Israeli-American policy-and-narrative front. The Foundation for Defense of Democracies (FDD), a Washington-based think tank long documented by the Institute for Policy Studies as a central node in the United States Israel lobby (Militarist Monitor, 2020), has in the past two years made South Africa a direct campaign target. The FDD has published reports calling for U.S. Treasury sanctions against named South African civil society figures and organisations including Gift of the Givers, the Al-Quds Foundation of South Africa, Mandla Mandela, and the Media Review Network (SA Jewish Report, 2025); attacked the South African government's ICJ proceedings against Israel as 'meritless' (FDD, 2024); campaigned against South African parliamentary moves it has framed as criminalising pro-Israel speech (FDD, 2025); and used the expulsion of an Israeli chargé d'affaires in January 2026 as the occasion for a wider public campaign against the South African government's foreign policy (FDD, 2026). The FDD's self-described mission is 'to promote pluralism, defend democratic values, and combat terrorism'; its operational behaviour in the South African theatre is the construction of a sanctions, narrative, and lobbying front against a state whose foreign policy positions are inconvenient to Washington and Tel Aviv. This is the Israeli-American media, narrative, and cyber shaping capability arriving in Southern Africa with explicit policy targets and a published playbook.

Read together, the pay-TV layer, the legacy and digital press layer, and the policy-and-narrative front constitute the informational counterpart to the digital and financial infrastructure layers. The classic configuration of Anglo-American, Franco-German, and Israeli-American non-linear hybrid warfare (NLHW) – investment, narrative shaping, civil-society funding, cyber capability, legal-procedural attack, and sanctions threat – is now visibly present in the South African theatre. NLHW operates in the grey zone between war and peace, and its instruments are tuned for electoral manipulation, regime change, and societal destabilisation, as the case record reviewed in section 8 below establishes.

7. The Regional Frame: U.S. Positioning Across Southern Africa, 2015–2026

The South African case cannot be read in isolation. The American footprint extends across Southern Africa through energy, mining, digital, military, and intelligence vectors. The regional picture from 2015 onwards is the necessary frame.

Mozambique hosts the largest single U.S.-linked strategic exposure in the region: the Mozambique LNG complex in Cabo Delgado, led by TotalEnergies with heavy U.S. Export-Import Bank financing and U.S. private security and counterinsurgency support after the 2021 insurgent attack at Palma. The project converted a commercial gas play into a maritime-security, counterinsurgency, and

strategic energy-security project tied directly to Richards Bay logistics, South African port systems, and regional gas demand (ZAAIMAN, 2026a).

Angola sits at the centre of the Lobito Corridor, the flagship U.S.-EU rail and logistics initiative announced at the 2023 G20 and underwritten by DFC and EXIM finance to carry Democratic Republic of Congo and Zambian copper and cobalt to the Atlantic. The corridor is the most explicit U.S. critical-minerals chokepoint project in Africa to date and is framed in official documents as a counter to Chinese Belt and Road infrastructure on the same routes.

Democratic Republic of Congo is the upstream end of the same corridor and the single largest cobalt and a major copper, tantalum, and tin source for the global energy transition. American mining finance, DFC engagement, and U.S. State Department diplomatic activity around DRC mineral concessions intensified through 2024–2026. The Archimedes Group, a Tel Aviv-based political consultancy, was banned by Facebook in 2019 for running coordinated inauthentic networks targeting elections in the DRC, Nigeria, Senegal, Togo, Angola, Niger, and Tunisia (ZAAIMAN, 2026a). This is the documented entry-point of Israeli-linked political influence operations into Southern and Central African electoral processes.

Zambia is integrated into the Lobito Corridor on the eastern end and is the principal regional partner for U.S. critical-mineral diplomacy. The 2024 U.S. AFRICOM engagement schedule with Zambia, the World Bank's Lobito-linked finance, and DFC mineral exposure all concentrate here.

Tanzania hosts the eastern terminus of the East African Crude Oil Pipeline (EACOP), Indian Ocean port infrastructure at Dar es Salaam and Bagamoyo, and a growing U.S. naval engagement footprint. It is the eastern hinge of the chokepoint geography described by ZAAIMAN (2026b) on French repositioning, and a competitive theatre between U.S., French, Indian, and Chinese influence.

Botswana, Lesotho, and Eswatini are tied to South Africa through SACU, monetary union, and labour migration, and are exposed to the same U.S. financial and digital architecture. Botswana's diamond industry, its sovereign wealth management, and its growing data-centre ambitions place it inside the same hyperscaler footprint. Lesotho's textile sector, exposed in 2025 to the unilateral U.S. tariff regime, illustrates the chokepoint vulnerability of small states tied to single-market export dependence under shifting U.S. policy. Eswatini, the last absolute monarchy in the region, has retained close Taiwanese and U.S. policy ties and serves as a counter-China holdout.

Across all of these states the pattern is consistent. American positioning combines:

- DFC and EXIM-financed energy and minerals projects that anchor U.S. supply-chain claims;
- U.S. AFRICOM and special-operations engagements packaged as training, counter-terrorism, and maritime-security cooperation;
- private military and security company presence, often subcontracted through U.S. and allied firms around energy and mining sites;

- hyperscaler cloud and subsea cable infrastructure that bind regional digital economies to U.S. jurisdiction;
- Israeli-linked cyber and influence vendors operating across electoral and civil-society spaces; and
- USAID, Ford Foundation, OSF, and U.S.-routed philanthropic flows shaping civil society, legal training, and media development.

The **defence-adjacent** and **dual-use** stealth character of this regional positioning is the hallmark feature. Each individual project can be defended in commercial, humanitarian, or counter-terrorism terms. The strategic effect is cumulative and structural: a Southern African space increasingly integrated into U.S. jurisdictional reach across energy, minerals, digital, financial, narrative, and security domains.

8. Case Studies: Digital Infrastructure as Vector of Coercion

This section assembles the case record on how control over digital infrastructure produces the vulnerabilities described above. The cases are drawn from the documented public record and are presented to establish that the capacities at stake are not theoretical.

8.1 Stuxnet and the precedent of digital sabotage. ZETTER's (2014) reconstruction of Operation Olympic Games is the foundational case. The joint U.S.–Israeli covert cyber operation physically destroyed centrifuges at Iran's Natanz nuclear facility using the Stuxnet worm, seeded into the air-gapped facility through industrial control system dependencies. The significance is the precedent: digital infrastructure can be used as an instrument of regime-directed coercion and physical sabotage, with deniability. SANGER's (2018) *The Perfect Weapon* extends the precedent across SWIFT, election systems, power grids, and the Sony hack.

8.2 Election interference and political shaping. LEVIN's PEIG dataset (LEVIN, 2019, 2020) establishes the quantitative baseline. Between 1946 and 2000, the United States and the Soviet Union/Russia intervened in one in nine national executive elections across the international system, with the United States the more frequent actor. Documented case studies include Serbia, Ukraine, Kenya, and multiple Latin American states. LEVIN's PEIG 2.0 (LEVIN, 2025) extends the coverage to 2014 and shows a thirty-seven per cent increase in the total number of intervention cases. The structural conclusion is that electoral interference is not exceptional but routine for great powers, and that cyber-enabled vote-tally manipulation and large-scale information operations represent an extension rather than a break.

The Associated Press investigation of USAID's ZunZuneo programme (GILLUM, ARCE & WEISSENSTEIN, 2014) provides a clear platform-based case: USAID covertly built a Cuban social media platform designed to harvest mobile numbers, map political networks, and push politically mobilising content when the platform reached critical mass. The grammar of the operation – an apparently civilian digital service that is in fact an instrument of political destabilisation – is precisely the grammar that becomes available wherever a foreign actor controls the underlying platform layer. TUFEKCI (2017) provides the sociological complement: digitally-enabled protest in

the Arab Spring, Euromaidan, Gezi Park, and Latin American mobilisations appears spontaneous but is deeply conditioned by platform architecture, funding flows, and external coordination. RID (2020) traces the genealogy of disinformation as a state instrument from Soviet active measures to contemporary Russian and Western operations; BRADSHAW and HOWARD (2019) document that state-run computational propaganda operations now exist across more than seventy countries; VOSOUGHI, ROY and ARAL (2018) supply the empirical mechanics, showing that false news travels faster, further, and deeper than true news.

8.3 Commercial spyware and the suppression of accountability. The Citizen Lab body of forensic investigation has mapped the use of commercial spyware – predominantly Israeli-developed – against journalists, human rights defenders, opposition politicians, judges, and prosecutors in at least forty-five countries (MARCZAK et al., 2018). The Pegasus Project, anchored on Amnesty International's Security Lab forensic methodology (Amnesty International, 2021), documented infections on the devices of human rights lawyers, judges, prosecutors, and activists across Morocco, Azerbaijan, India, Mexico, Rwanda, and Hungary. The European Parliament's PEGA Committee Inquiry (European Parliament, 2023) extended the record across Hungary, Spain, Poland, and Greece.

Two cases concretise the dynamic. In Mexico, the joint investigation by R3D, Article 19, SocialTIC, and Citizen Lab (Article 19, 2022) documented that the Secretariat of National Defence had secretly contracted Pegasus and operated it against human rights defender Raymundo Ramos and journalists, including during the period in which Ramos was assisting the families of civilians killed in a suspected extrajudicial execution by the Army. In Greece, the Predator surveillance scandal – Predator being produced by Intellexa, founded by former Israeli military intelligence officer Tal Dilian – documented the simultaneous targeting of the leader of the opposition PASOK, the Chief of the Hellenic National Defence General Staff, multiple cabinet ministers, and journalists. In February 2026 a Greek court convicted four Intellexa executives and referred the case for further investigation of unidentified third parties (European Parliament, 2023).

The Venice Commission (Council of Europe, 2024) concluded that the deployment of NSO Group spyware by state police and intelligence services against judges, lawyers, opposition politicians, and journalists, in most cases without judicial authorisation, represents a systemic subversion of the institutional independence of judiciaries. DEIBERT (2020) synthesises the convergence of the Israeli defence-intelligence industry with authoritarian-leaning governments across Africa, Latin America, Southwest Asia, and Eastern Europe. HEVER (2018) frames this structurally: the export of occupation-tested surveillance and policing technology is integral to the Israeli state's political economy, not incidental to it.

8.4 Project Raven and the U.S.–Israeli cyber ecosystem. The DarkMatter / Project Raven case is analytically decisive. From approximately 2009 the UAE's National Electronic Security Authority contracted the U.S. firm CyberPoint and from late 2015 the UAE-based DarkMatter to build an offensive cyber unit staffed by former NSA and U.S. intelligence personnel. Its operational record included hacking the Emir of Qatar, the former Deputy Prime Minister of Turkey, Yemeni Nobel Peace laureate Tawakkol Karman, journalists, human rights activists, and U.S. persons (BING &

SCHECTMAN, 2019). In September 2021 the U.S. Department of Justice secured a Deferred Prosecution Agreement against three former NSA officers for violations of the Arms Export Control Act and computer fraud statutes (SOESANTO, 2021).

8.5 What the cases collectively show. Control over digital infrastructure produces vulnerabilities that are exploited:

- to surveil opposition figures, journalists, judges, prosecutors, and military commanders;
- to interfere in elections and shape public opinion;
- to destabilise governments through the digital seeding of mobilisation;
- to compromise economic and industrial infrastructure; and
- at the extreme, to enable physical violence against individuals identified through the same surveillance.

The infrastructure does not have to be owned by a foreign state for these capacities to be available. It has to be operated under a jurisdiction in which the foreign state can compel cooperation, or be accessed by tools sold under that jurisdiction's export licensing regime. The South African digital footprint is now substantially in that condition.

9. Strategic Risk: Non-Linear Hybrid Warfare in an Unsecuritised Economy

The strategic risk in an economy that is neither securitised nor secured is political-economic in character. Where critical infrastructure is operated under foreign jurisdiction, where developmental potential is blocked, and where the public sphere is exposed to externally-shaped narrative and platform layers, the social conditions for political instability are produced from outside the country's own decision space.

Blocking developmental potential is not only a matter of debt, ratings, and ESG pricing, though these are powerful instruments. It is also a matter of industrial structure. A foreign industrial actor that establishes a deeply embedded assembly, distribution, and supplier ecosystem in a host country can foreclose the emergence of an indigenous rival industry without ever exercising overt political pressure. The mechanism is structural. Once final-assembly plants, component supplier networks, dealership and finance systems, skills pipelines, and tariff and rules-of-origin frameworks are organised around the foreign producer, an indigenous entrant has no commercially viable entry path. It cannot compete on unit cost because the foreign producer is amortised across a global platform; it cannot compete on supplier access because the supplier base is locked into the incumbent's specifications; and it cannot compete on capital cost because financial markets price the indigenous entrant as a higher-risk asset. The classical case is automotive: locating a global producer's assembly plant in a developing country secures the domestic and regional market for that producer and makes the emergence of an indigenous national car manufacturer economically impossible without sustained state intervention – the kind of intervention that the same investing jurisdiction can then attack through trade-rule disputes, ESG and ratings actions, and sanctions threats. The same logic now applies, with much greater force, in the digital infrastructure layer: a host state without a sovereign cloud, sovereign AI

compute, and sovereign data architecture cannot grow an indigenous digital industry to compete with the incumbent hyperscaler, and is therefore locked out of the New Productive Forces that drive 21st century growth.

Persistent stagnation, produced by both financial pricing instruments and these structural-industrial mechanisms, creates the constituencies that non-linear hybrid warfare seeks to activate. Domination of the digital, media, and entertainment infrastructure provides the channels through which activation occurs. The two halves of the strategy are mutually reinforcing: foreign positioning at the digital infrastructure and industrial layers produces the developmental constraint; foreign positioning at the narrative and platform layer provides the means to mobilise the discontent that the constraint generates.

Non-linear hybrid warfare (NLHW), in its Anglo-American, Franco-German, and Israeli-American configurations, operates in the grey zone between war and peace through a layered repertoire:

- calibrated economic pressure (tariffs, sanctions threats, ratings actions, ESG exclusion);
- narrative and platform shaping through owned or influenced media, advertising, and entertainment infrastructure;
- civil-society funding pipelines into legal, human-rights, and media-development organisations;
- commercial cyber and surveillance vendors deployable against opposition, judiciary, and security leadership;
- U.S. and allied law-enforcement liaison embedded inside host-state policing, financial intelligence, and judicial systems; and
- the option of escalation to targeted sanctions, designations, and procurement exclusions.

The empirical record in section 8 demonstrates that each of these instruments has been deployed against states whose policy positions conflicted with the dominant Western strategic frame. There is no analytical basis for assuming that a South Africa which sustains positions inconvenient to Washington and Tel Aviv – the ICJ proceedings on Palestine, BRICS expansion, the debate on critical minerals beneficiation, the maintenance of strategic relations with Russia, China, and Iran – will be exempted from the application of these instruments by its strategic-investment partners. The capacities are in place. The doctrinal language is explicit. The political conditions are already activated.

10. Conclusion: Investment as Strategic Position

The Denel PMP overture by Omusha is best read against this broader pattern. It is not the anomaly. It is the strategic-industrial extension of a logic that has already been operating for a decade in South Africa's digital, financial, energy, minerals, and logistics infrastructure. The American footprint in South Africa is no longer organised around bases, troops, or defence factories. It is organised around cloud regions, subsea cable landings, data centres, AI compute, payment plumbing, mining finance, energy corridors, and insurance and ESG pricing. The U.S. government's own primary instrument in this domain, the DFC, describes the project in plain language: economic statecraft, strategic competition with China, the securing of critical supply chains, and the construction of investment ecosystems anchored to U.S. capital markets (DFC, 2026a).

The three claims that opened this paper are returned to here:

- The United States is positioning to dominate South Africa's digital infrastructure, energy, and financial strategic infrastructure. The investment pattern of 2015–2024 shows it directly. The DFC's public doctrine confirms it. Because digital infrastructure is the operating layer of the New Productive Forces, this is also a direct cap on South African economic development.
- The purpose is to deny China geopolitically. The DFC names China as the strategic rival in every major public address of its current CEO; the doctrinal frame is 'the new arsenal of influence'.
- The South African economy is neither securitised nor secured. This is the gravest vulnerability. Critical infrastructure is treated as ordinary commerce. The narrative and entertainment layer is being absorbed by foreign capital. The cyber and surveillance layer is exposed to vendors licensed under jurisdictions hostile to South African foreign policy positions. The state has no operational framework for treating any of this as a national-security question.

The structural consequence is direct. The combination of weaponised-interdependence theory (FARRELL & NEWMAN, 2019), the home-field advantage analysis of U.S. cyber operations (BUCHANAN, 2020), and DENARDIS's (2014) architecture-as-politics framework predicts that the more the digital and financial infrastructure of a host state is operated under foreign jurisdiction, the more the panopticon and chokepoint capacities of that foreign jurisdiction become available against the host. The case record from Mexico, Greece, the Gulf, and the European Union shows that those capacities are used.

The cumulative effect on South Africa is that the country is falling behind in a cluster of sectors that is now central to both national security and economic development, in the present and in the coming decades: the digital, artificial-intelligence, cyber, and electromagnetic-spectrum domains. These are the operating layers of the New Productive Forces and the principal arenas in which the next generation of growth, sovereignty, and deterrence will be decided. The Western strategic posture in these domains is not a neutral race in which African states might catch up at their own

pace. It is an active positioning to block both China and the African continent from acquiring sovereign capability at the same layer, through investment ecosystems, export controls, standard-setting, training architectures, and the licensing regimes that govern cyber, AI, and spectrum-related technologies. The longer this asymmetry holds, the more deeply South Africa's developmental ceiling is set abroad.

South Africa's sovereign developmental potential depends on treating critical infrastructure investments as national-security questions rather than as ordinary commerce. That requires institutional capability the country does not currently possess: an investment-screening regime with national-security teeth; a critical-infrastructure designation framework that covers cloud, subsea cable landings, AI compute, payments, and critical minerals processing; a sovereign-data architecture; a domestic cyber-vendor base; an industrial policy framework that protects the conditions for indigenous competitors to emerge in the New Productive Forces sectors; an export-control regime aligned with South African foreign-policy positions; and a media-ownership framework that recognises the strategic stakes in narrative infrastructure. Building these is the work of the decade. The alternative is the slow consolidation of a shadow architecture of foreign jurisdictional control over the South African public, economic, and political sphere – an architecture whose doctrinal logic is now stated openly by the agencies that build it, and which the Denel PMP overture has simply made visible at the strategic-industrial edge.

References

Ahmed, W., Hussain, M., & Grim, R. (2026, May 17). From mutual suspicion to political embrace: How the U.S. learned to stop worrying and embrace Pakistan. *Drop Site News*.

Amnesty International. (2021). *Forensic methodology report: How to catch NSO Group's Pegasus*. Amnesty International Security Lab.

Anadolu Agency. (2026, May 12). Macron urges Africa-Europe tech alliance in Nairobi. *Anadolu Agency*.

Article 19. (2022). *Ejército espía*. Article 19, R3D, SocialTIC, and Citizen Lab.

Associated Press. (2023, January 25). Yellen tours wildlife reserve to start South Africa visit. *Associated Press*.

Bing, C., & Schectman, J. (2019, January 30). Exclusive: UAE used cyber super-weapon to spy on iPhones of foes. *Reuters*.

Bradshaw, S., & Howard, P. N. (2019). The global organisation of social media disinformation campaigns. *Journal of Information Technology & Politics*, 16(4), 328–342.

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

BusinessTech. (2025, October 26). New DStv owner already in trouble in South Africa. *BusinessTech*.

Carnegie Endowment for International Peace. (2022). *The geopolitics of submarine cables: The infrastructure of the digital age*. Carnegie Endowment for International Peace.

Clarke, R. A., & Knake, R. K. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press.

Congressional Research Service. (2025). *U.S. International Development Finance Corporation (DFC)* (IF11436). Congressional Research Service.

Council of Europe. (2024). *Report on a rule of law and human rights compliant regulation of targeted surveillance* (CDL-AD(2024)043). Venice Commission.

Daily Investor. (2026, May 13). South Africans kiss DStv goodbye. *Daily Investor*.

Daily Post Nigeria. (2025, July 24). Canal+ finalizes $3bn acquisition of MultiChoice. *Daily Post*.

DefenceWeb. (2015, November 6). Honeywell Aerospace and Denel Aviation sign collaboration agreement. *DefenceWeb*.

Deibert, R. (2020). *Reset: Reclaiming the internet for civil society*. House of Anansi.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Developing Telecoms. (2026, May 13). Orange boosts digital inclusion and job support commitments in Africa. *Developing Telecoms*.

DFC. (2026a, April 22). *DFC CEO Ben Black at Endless Frontiers: American economic statecraft is back* [Press release]. U.S. International Development Finance Corporation.

DFC. (2026b, March 4). *DFC CEO Ben Black discusses U.S. economic statecraft, DFC tools during Milken panel* [Press release]. U.S. International Development Finance Corporation.

DFC. (2026c, March 27). *DFC CEO Ben Black discusses economic statecraft during Hill & Valley Forum* [Press release]. U.S. International Development Finance Corporation.

DFC. (2026d). *Sub-Saharan Africa: Strengthening strategic competition through investments in Africa's digital economy*. U.S. International Development Finance Corporation.

DFC. (2026e, March 19). *DFC CEO Ben Black discusses U.S. economic statecraft, DFC financial tools during Tulane Corporate Law Institute conference* [Press release]. U.S. International Development Finance Corporation.

European Parliament. (2023). *Report of the committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware* (A9-0189/2023). European Parliament PEGA Committee.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351

FDD. (2024, February 16). *ICJ rejects South Africa's new attack against Israel*. Foundation for Defense of Democracies.

FDD. (2025, June 9). *South African MPs seek to criminalize speech defending Israel from apartheid allegations*. Foundation for Defense of Democracies.

FDD. (2026, February 9). *South Africa rejects Israeli water assistance to carry water for Hamas*. Foundation for Defense of Democracies.

Financial Intelligence Centre. (2023). *Experts gather to share global knowledge on combating illegal wildlife trade* [Media release]. Financial Intelligence Centre, Republic of South Africa.

Gillum, J., Arce, A., & Weissenstein, M. (2014, April 3). USAID used secretive program to create a 'Cuban Twitter' to stir unrest. *Associated Press*.

Goldsmith, J., & Wu, T. (2006). *Who controls the internet? Illusions of a borderless world*. Oxford University Press.

Hever, S. (2018). *The privatisation of Israeli security*. Pluto Press.

iAfrica. (2026, May 13). Orange targets 3 million youth and 500 startups with expanded AI and digital skills commitments in Africa. *iAfrica*.

Klimburg, A. (2017). *The darkening web: The war for cyberspace*. Penguin Press.

Levin, D. H. (2019). Partisan electoral interventions by the great powers: Introducing the PEIG dataset. *Conflict Management and Peace Science*, 36(1), 88–106.

Levin, D. H. (2020). *Meddling in the ballot box: The causes and effects of partisan electoral interventions*. Oxford University Press.

Levin, D. H. (2025). Introducing PEIG 2.0: Sixty-nine years of partisan electoral interventions 1946–2014. *Conflict Management and Peace Science*. Advance online publication.

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). *Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries* (Citizen Lab Research Report No. 113). University of Toronto.

Martin, G. (2026, May 18). US company looking to invest in and help revive Denel PMP. *DefenceWeb*.

Militarist Monitor. (2020). *Foundation for Defense of Democracies (FDD)*. Institute for Policy Studies.

Nye, J. S., Jr. (2010). *Cyber power*. Belfer Center for Science and International Affairs, Harvard Kennedy School.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Reuters. (2025, December 11). Interpol-led global wildlife sting makes record seizures of animals, plants, timber. *Reuters*.

SA Jewish Report. (2025, September). Will pro-Hamas-linked South Africans face US sanctions? *SA Jewish Report*.

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. Crown.

Soesanto, S. (2021, September 23). Prosecuting Project Raven: A new frontier for export control enforcement. *Lawfare*.

The Standard. (2026, May 12). Macron, Ruto seal pact on digital skills and youth empowerment. *The Standard* (Kenya).

Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.

U.S. Department of Defense. (2024, November 20). *Readout of Republic of South Africa – United States of America Defense Committee* [Press release]. U.S. Department of Defense.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151.

Zaaiman, A. (2026a). *Strategic investment USA in South Africa: Source compilation*. DefenceWeb compilation, May 2026.

Zaaiman, A. (2026b, May 12). *France repositioning in Africa: African Eastern Rim and the Africa Forward Summit in Kenya, 11–12 May 2026*. Working paper.

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.