

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

NOVEMBER 2026

Cyber Statecraft and the Middle Ground

Joe Devanny
Arthur P.B. Laudrain

Technology and International Affairs Program

Cyber Statecraft and the Middle Ground

Joe Devanny
Arthur P.B. Laudrain

November 2026

About the Carnegie Endowment for International Peace

In a complex, changing, and increasingly contested world, the Carnegie Endowment generates strategic ideas, supports diplomacy, and trains the next generation of international scholar-practitioners to help countries and institutions take on the most difficult global problems and advance peace. With a global network of more than 200 scholars across twenty countries, Carnegie is renowned for its independent analysis of major global problems and understanding of regional contexts.

© 2026 Carnegie Endowment for International Peace.
All rights reserved.

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Carnegie Endowment for International Peace. Please direct inquiries to:

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.

TABLE OF CONTENTS

Introduction 1

The Complexity of Statecraft 2

Unpacking the Cyber Middle Ground 6

Politics and Middle Ground Cyber Statecraft 12

Engaging and Influencing the Middle Ground 19

Conclusion 21

Notes 23

Acknowledgments

The authors would like to thank the Defence Science and Technology Laboratory (Dstl) for funding this research through the Engineering and Physical Sciences Research Council (EPSRC) as part of the project on Cyber Statecraft in an Era of Systemic Competition. We are also grateful to the Carnegie Endowment for International Peace's Technology and International Affairs Program, including the editorial team and very helpful reviewers. The paper does not reflect the views of Dstl, EPSRC, Carnegie, or King's College London. The authors benefited greatly from a range of conversations with other researchers and experts, including two roundtable discussions: one in December 2024 at King's College London, and another in July 2025 at the Escola de Comando e Estado-Maior do Exército (ECEME) in Rio de Janeiro. All errors and omissions are the sole responsibility of the authors.

About the Authors

Joe Devanny is a senior lecturer in the Department of War Studies at King's College London, and deputy director of the Centre for Defence Studies at King's. He was a 2023–25 project fellow at the Research Institute for Sociotechnical Cyber Security. He was also a 2022–23 British Academy Innovation Fellow at the UK Foreign, Commonwealth and Development Office. He writes here in a personal capacity.

Arthur P.B. Laudrain is the team lead and a senior researcher in cybersecurity at the Centre for Security Studies (CSS) at ETH Zurich. Previously, he was the Richard Lounsbery US-France Security Fellow at Stanford CISAC, and a research associate in cyber diplomacy at the Department of War Studies at King's College London. He obtained his doctorate from the University of Oxford (Wolfson College), and holds an MA (London) and an LLM (Leiden).

Technology and International Affairs Program

The Technology and International Affairs Program develops insights to address the governance challenges and large-scale risks of new technologies. Our experts identify actionable best practices and incentives for industry and government leaders on artificial intelligence, cyber threats, cloud security, countering influence operations, reducing the risk of biotechnologies, and ensuring global digital inclusion.

Introduction

As foreign actors threaten national governments and private companies through cyberspace daily, cybersecurity highlights the overlap of domestic and international policies perhaps better than any other contemporary security issue. Domestically, improved cybersecurity and resilience are imperative, and, because much of the attack surface is privately owned and operated, private companies are key stakeholders. Internationally, the cyber diplomacy agenda sees states negotiating and implementing nonbinding standards of responsible behavior in the domain. At the same time, many states are operationally active in cyberspace, pursuing their national strategic objectives through espionage, cyber operations, and sometimes cyber crime. As all these practices mature, they have come to be interpreted through the lens of statecraft.

"Cyber statecraft" is a relatively new term, but it draws on a much longer pedigree of statecraft theory and practice.[1] Recent interest in understanding competitive cyber statecraft has been motivated by the recognition that various states are pursuing both diplomatic and operational lines of effort to achieve their respective national strategic objectives in and through cyberspace.

In the field of cyber diplomacy, it has become common to refer to a dividing line between two camps: liberal, like-minded states and authoritarian states.[2] Beyond these two camps, another larger group is often described as a so-called "middle ground." These middle ground states—such as Brazil, India, Qatar, South Africa, and the United Arab Emirates—are grouped together because they neither fit into nor self-define as being part of either camp.[3] The middle ground states are seen as a pivotal constituency,[4] whose approval could tip the balance for either camp and shape the future of global cyber diplomacy.[5] This conception of the middle ground can also be seen as a function of an increasingly decentered global order, indicating the impact of rising powers.[6]

Yet applying one label, "middle ground," to a group of very different states raises the question of how these middle ground states conduct cyber statecraft. Is there more uniting them than their nonmembership in the like-minded or authoritarian camps?[7] This paper argues that there is and illustrates middle ground cyber statecraft with three examples: Brazil, India, and South Africa. These states are among the most frequently labeled middle ground states in cyber diplomacy. They are also perceived as influential in their respective regions and, in different ways, as rising global powers. Despite several important differences among the three, not least their relational power, their approaches to cyber statecraft share broad similarities: Each state's approach is best understood in reference to its particular domestic politics, geopolitical context, relational power, and elite role conception. What might be called a neoclassical realist perspective, combined with insights from the bureaucratic analysis of foreign policy, offers a good guide to what drives cyber statecraft in these states.[8] Each of these states is also involved in the BRICS+ group and is a diplomatically prominent

country in the so-called Global South. Their cyber statecraft is therefore impossible to disaggregate from the wider geopolitical context of great power competition and global disorder.

This leads to a second question: How should states firmly within the two camps approach these middle ground states in their own cyber statecraft? Is the middle ground a so-called diplomatic battleground in which the two camps compete for influence, while the middle ground states consider how best to react or exploit this competition for their own national advantage?[9]

To successfully engage with middle ground states, officials in like-minded states must interpret their statecraft as based on their respective strategies, rather than defining and addressing those strategies as a function of where they sit on an imagined spectrum between the two poles of like-minded and authoritarian states.[10] This paper advocates an approach to like-minded cyber statecraft that navigates the commonalities and specificities of the middle ground:

- Like-minded states should principally offer mutual benefits to middle ground states, rather than seek their normative alignment.
- Developmental goals are integral to middle ground cyber statecraft, meaning that cyber capacity–building assistance is a key tool for like-minded statecraft. Cutting this assistance is likely to be detrimental to like-minded strategies and could strengthen the hand of competing, authoritarian cyber statecraft.
- Given the prioritization of domestic cybersecurity and resilience by middle ground states, like-minded states should privilege bilateral, minilateral, and regional forums for cooperation and assistance, prioritizing this over the existing multilateral process under the United Nations.

The paper proceeds in four parts, beginning with an explanation of how the concept of statecraft is applied to cyberspace. The next section introduces the concept of the middle ground. Then the paper outlines the cyber statecraft of Brazil, India, and South Africa. Finally, the paper explores the implications of a competitive statecraft approach for how like-minded states should engage with the three selected middle ground states.

The Complexity of Statecraft

In light of current debates about the future of international order, the statecraft approach is particularly attractive because it implicitly recognizes the complexity of international relations. The practice of statecraft is competitive, making for an uncertain and volatile system.[11]

Statecraft theory also captures the degree of complexity and competition involved in devising and implementing national policies. Each state's deliberations and positions reflect the contributions and interests of a plurality of actors within a given national system.[12]

This is a compelling approach to analyzing cyber statecraft because it situates cyber diplomacy in a wider-than-cyber geopolitical context, which is particularly important when cyber issues might not command high priority among national decisionmakers.[13] As David A. Baldwin noted about economic statecraft, when states pursue their policies, they rarely have a single objective in mind.[14] For analysts of cyber diplomacy, this is especially evident in the cyber capacity–building consequences of a turn toward reduced like-minded national aid budgets.[15] The complexity of interstate interactions can also complicate interpretations of what goals or values are being pursued in specific instances of disagreement in cyber statecraft.[16] And the wider structural context should never be ignored, including varying degrees of power, the interplay between states and global markets, and the consequences of potential misperception and wider system effects.[17]

The Art of Cyber Statecraft

Cyber-related issues are rarely at the top of the in-tray for elite decisionmakers; today, even those who are tech-savvy are more likely to focus on artificial intelligence (AI).[18] Furthermore, the more technical a decision, the less intelligible it is likely to be for bureaucratic generalists. It can be difficult for states not only to recruit and retain subject matter experts but also to configure and implement systems which make best use of what expertise is available to support decisionmakers. This is as true for deep technical expertise as it is for deep country-level expertise—cyber statecraft requires both of these to inform decisions. Prudent decisionmakers will configure national systems to ensure that this expertise is available. Then they will use it. In states where resources are limited and expertise is scarce, this problem is exacerbated, and there is likely even more of a premium on successful efforts to cultivate allies and stakeholders outside government to reach national positions.[19]

Of course, none of these complicating factors is unique to the cyber dimensions of contemporary statecraft. But the ways in which cyber diplomacy and cyber operations (think the Stuxnet malware, the SolarWinds hack, or the various Typhoon threat actors) have inserted themselves into the toolkits of elite decisionmakers over the past twenty years create a new context to explore how national governments compete with each other and the extent to which their competitive positions are determined by the relative well-functioning of their national systems.[20]

This paper advances the understanding of cyber statecraft in and toward the so-called middle ground states. It argues that the idea of a middle ground is conceptually undeveloped and generally used by diplomats from like-minded states as shorthand for states perceived as being potentially open to influence and persuasion to follow initiatives, norms, or proposals

advanced by their camp. This use of the phrase is near inevitable for busy officials tasked to provide and execute a coherent strategy for cyber diplomacy, but it also risks denying the diversity and agency of states grouped together in the middle ground. Viewed in this way, the middle ground is a situational, reflexive concept, saying as much about those who coined and use it as it does about those it is intended to describe. There is no evidence that any state self-defines as being part of the middle ground, although such self-definition is hardly necessary for the phrase to be a useful guide. Instead, practitioners and academics offer a variety of alternative descriptions, such as "multi-vector" expressions of "strategic autonomy" or "active non-alignment," that collectively imply more agency and purpose.[21] Rather than sitting passively in the middle of two camps, actively nonaligned states might perceive great power competition over their attention as something that "expands policy options."[22]

Like-minded diplomats might continue to think profitably about the middle ground and use the term internally (in intra-government or intra-like-minded communications) as concise shorthand to denote a specific group of states. However, it would be prudent to refrain from using the term in public communications. Just as the past decade saw the rise of "cyber power" as a trope of national cyber strategies, rather than use of the more widely accepted—though diversely interpreted[23]—diplomatic concept of "responsible state behavior in cyberspace," so too might "middle ground" be better retired in public statements and replaced by more amenable alternatives.[24]

Practicing Cyber Statecraft

Drawing explicitly on Baldwin's concise definition of the practice of statecraft, we describe cyber statecraft as comprising the instruments used by policymakers in their attempt to exercise power *in, through, and regarding cyberspace* to get others to do what they would not otherwise do.[25] This capacious definition highlights the concept's flexibility. Cyber statecraft encompasses diplomacy, including the coercive diplomacy of sanctions, as well as capacity-building and the operational dimensions of statecraft.

This definition also reflects the plurality of possible interpretations of the practice: Cyber statecraft could reasonably describe the use of cyber tools to achieve non-cyber ends, as well as the use of non-cyber tools to achieve ends in or regarding cyberspace. A digital information operation aimed at achieving changes in human sentiment "in real life" is an example of using cyber means to achieve a non-cyber end.[26] Bombing an adversary's hackers would be an extreme example of using non-cyber means to pursue a cyber-related end.[27]

Cyber statecraft also encompasses diplomacy. Although early uses of the term "cyber diplomacy" applied to diplomats' use of digital media, today it is more common to distinguish between "digital diplomacy" (such as diplomats on social media) and "cyber diplomacy" (diplomatic engagement on issues substantively related to cyberspace).[28] On this distinction,

cyber diplomacy includes discussing norms of responsible state behavior in cyberspace, negotiating a global cybercrime treaty, managing cyber capacity–building programs, and shaping future standards at the International Telecommunication Union.[29]

Developing operational cyber capabilities, convening a cohort of specialist cyber diplomats, or pursuing a long-term effort to improve domestic cybersecurity and resilience are all aspects of cyber statecraft that can only be sensibly thought of within the context of an international system of states. Moreover, cyber strategy is widely described as "whole-of-nation" because governments do not have a monopoly (or even a majority) of the necessary skills or resources within a state.[30] Beyond this domestic level, states also conduct cyber statecraft internationally: They must cooperate or compete, and sometimes come into conflict, with each other. All acts of cyber statecraft are, in some way, efforts to influence other actors' behavior.[31] Some influence efforts are unilateral, while others require collaboration. Some involve soft power, others hard power, and some a combination of both.

> **All acts of cyber statecraft are, in some way, efforts to influence other actors' behavior.**

Cyber statecraft is, therefore, a capacious concept, encompassing a variety of tools and objectives. Like other aspects of statecraft, some states will excel in the use of certain cyber tools more than others, or they will rely to a different extent than others on cyber tools, depending on strategic culture, doctrine, or perceived necessity. Various efforts have been made to compile indices, matrices, and models to rank states according to their "cyber power," "cyber readiness," or "cyber maturity," which respectively capture different aspects of this diversity of experience of cyber statecraft.[32]

In that sense, although conceptual debates will likely continue to explore and elaborate the definition of cyber statecraft, it might be more useful for policymakers to think instead in terms of how the cyber toolkit and cyberspace-related policy issues can be integrated into the use of the techniques of statecraft as traditionally understood, which Baldwin defines as propaganda, diplomacy, economic, and military techniques, but which are perhaps better known acronymically as diplomatic, informational, military, and economic (DIME).[33]

All this underlines the obvious points that some states have more power than others, some perceive and define their national interests and strategic objectives more sharply than others, and some pursue these objectives more successfully (or more efficiently, or with better governance) than others. Analysis of cyber statecraft and the middle ground inevitably involves considerations of relational power and the interactions of states pursuing different strategic objectives, whether through cooperation, competition, or conflict. Wider regional contexts and global trends therefore shape how the cyber-related elements of statecraft are framed and enacted. Cyber statecraft does not take place in a vacuum.[34]

Unpacking the Cyber Middle Ground

In the diplomatic, more than the operational, aspects of cyber statecraft, the term middle ground offers a useful guide to some similarities among the countries it is used to identify. Brazil, India, and South Africa are not consistently aligned with like-minded or authoritarian positions in multilateral cyber diplomacy debates; this broad fact encompasses considerable nuance and differences in the states' policymaking processes and strategic outlooks. When assessing the operational dimension of their cyber statecraft, each state faces sharply divergent realities.[35] This is true for their wider statecraft, which includes considerable overlap and cooperation, but also reflects different threat perceptions and national strategic objectives.

The Middle Ground and Multipolarity

The different combinations in which these three countries participate in diplomacy, both trilaterally and as part of wider groups, reflect a shared belief in the fact and value of increasingly multipolar international relations. In wider foreign policy, Brazil, India, and South Africa are not only members of BRICS+,[36] but they also have a more long-standing association through their India-Brazil-South Africa (IBSA) Dialogue Forum.[37] IBSA has provided a loose (but fitfully used[38]) device for South–South cooperation, policy consultation, and coordination for over two decades.[39] Recently, there has been a flurry of interest in whether IBSA can reemerge from the shadow of BRICS+ as a useful forum.[40] IBSA will succeed or fail as a forum depending on the level of engagement and priority afforded to it by each member state's political leadership. The national strategic priorities that led each state to join both associations, and the elite political shifts that shaped the extent to which each state engaged within them, account for the layers of complexity and difference that lie beneath the apparent similarity accorded by their shared membership of these groups. Each of these states perceives increasing multipolarity as in its strategic interest, even if, as some argue, this is a misperception.[41]

While all three countries are regional powers, Brazil and India are more powerful and possess a more plausible aspiration to greater global influence.[42] This power imbalance, particularly in economic cooperation, will continue to drive bilateral initiatives between Brazil and India, outside of the trilateral IBSA framework.[43] All three, however, aspire to redress perceived imbalances in the existing international order; both IBSA and BRICS+ have been seen as potential vehicles for pursuing this objective.[44] Oliver Stuenkel argues that this effort to rebalance influence over "global agenda-setting" is part of a wider trend toward "competitive multilateralism." In this conjuncture, Stuenkel argues, emerging powers in the Global South will hedge, both embracing institutional elements of the existing order and pursuing new institutions that better reflect their ambition to enhance their autonomy and influence.[45] As the September 2026 BRICS+ summit in India demonstrated, despite the increased

complexity and potential for intragroup disagreement implicit in its expanded membership, BRICS+ arguably offers the constitutive flexibility to maintain this shared agenda, given its "loosely institutionalised, consensus-based" approach.[46]

While these various movements and groupings share some common outlooks and analyses of the shortcomings of the global status quo, it would be wrong to interpret the BRICS+ or the wider Global South as monolithic actors.[47] As Stuenkel has argued, the challenge for emerging powers in trying to shape a "post-Western world" is that it is difficult to generate a consensus position or "common project" within the Global South to focus shared efforts.[48] This was a persistent criticism of the BRICS group during its first decade.[49] It has extended into the present with questions about the strained coherence and ideological orientation of the recently enlarged BRICS+, though the group appears to have weathered geopolitical storms with relative cohesion to date.[50] Tensions between China and India, in particular, have undermined the extent to which BRICS+ can be a coherent vehicle for deeper cybersecurity cooperation, but the range of cyber-related initiatives in the BRICS+ September 2026 summit's New Delhi Declaration, while individually modest, collectively suggest a more substantial direction of travel.[51] Still, India has more opportunities to actively influence the Global South agenda outside BRICS+.[52]

Further complexity is added by the recent trend toward "minilateral" initiatives, such as the Quadrilateral Security Dialogue (called the Quad), which connects India with the United States, Australia, and Japan and aims to improve security cooperation in the Indo-Pacific in the context of rising Chinese power and influence.[53] Another, more issue-specific example is the Hague Group, which includes South Africa and eight other states and was formed in 2025 to pursue an agenda-setting role regarding international law and the war in Gaza.[54] The middle ground is, therefore, a capacious concept with a variety of different and sometimes diverging connotations. This must be recognized when applying it to analysis of cyber diplomacy.

Cyber Diplomacy in the Middle Ground

Given that cyber diplomacy is not conceived in a vacuum and is ultimately a tool of wider statecraft, it should be expected that wider geopolitical trends will be reflected within it. Andre Barrinha and Arindrajit Basu argue that both the rise of the Global South and the emergence of cyber diplomacy are part of a trend toward a "post-liberal" international order.[55] They also note uncertainty about the future of Global South influence over the agenda of cyber diplomacy. This reflects, to a great extent, wider and deeper uncertainty about the current situation and medium-term prospects for cyber diplomacy in the context of sharpened geopolitical competition and,[56] potentially, reduced funding for cyber capacity–building programs in light of significant aid cuts by major donors such as the United Kingdom and the United States.[57]

Multilateral discussion of norms of responsible state behavior in cyberspace has spanned most of this century. The formal mechanism for this discussion has shifted over time, from a relatively small group of governmental experts (GGE)[58] to a larger and more inclusive open-ended working group (OEWG).[59] The story of this shift was itself political and reflected, in part, a view still held today by many states, namely that the influence of a small number of more powerful states had a disproportionate impact on setting the global cyber diplomacy agenda.[60] Tensions between great powers—predominantly between the United States and Russia, but increasingly also China—have animated the lifespan of multilateral cyber diplomacy from the late 1990s until the present.[61] The stark differences of opinion between these more powerful states largely explain the relatively modest outcome from over fifteen years of active multilateral cyber diplomacy.[62]

The next phase of this process, under a notionally more permanent forum for interstate dialogue—originally discussed as a Programme of Action (PoA), but now styled as a "Global Mechanism" on cybersecurity and responsible state behavior in cyberspace—was subject to tense, yearslong negotiation among states, reflecting disagreement between the great powers, particularly about the modalities of including non-state stakeholders.[63] The debate about whether, under the Global Mechanism's rules of procedure, states should continue to enjoy an unconstrained veto over non-state stakeholder participation could seem esoteric to outsiders. For example, it was difficult to see what would have been lost by conceding the retention of the veto and simply re-committing, as a single state or group of like-minded states, to fund and orchestrate a wraparound shadow program of wider stakeholder engagements on the margins of each Global Mechanism meeting. Not being in *the* room for formal Global Mechanism discussions does not preclude stakeholders from being in *a* room with all the states that would be receptive to listening.[64]

The Global Mechanism held the first substantive meetings of its initial two-year cycle in July 2026, in which it was clear that the stakeholder issue would continue to be a point of tension.[65] Given the prominence of capacity-building in these discussions, reported reductions in like-minded states' capacity-building budgets will likely create acute challenges for the Global Mechanism's forward agenda.[66] This will foreground the prospect for further geopolitical competition in the provision of capacity-building from China, for instance, or from middle ground states themselves.[67]

> **Reported reductions in like-minded states' capacity-building budgets will likely create acute challenges for the Global Mechanism's forward agenda.**

Particularly over the past fifteen years, the UN process has elaborated a shared understanding across states that existing international law applies in cyberspace (albeit with disagreement about precisely how it does so), that states endorse eleven nonbinding norms of responsible state behavior in cyberspace, and that states recognize the importance of confidence- and capacity-building measures to promote international security and stability.[68]

While there are still proponents for a binding, treaty-based series of commitments, or for the elaboration of specific new cyber norms, the majority of states agree on the current approach of recognizing the applicability of existing law to cyberspace and implementing the eleven nonbinding norms.[69] However, continued agreement is not a given. The 2017 UN GGE's failure to reach consensus after elaborating the eleven norms in 2015 is a reminder that backsliding is always possible.[70]

It is possible to adopt a glass half full or glass half empty view of what has been achieved in two decades of UN cyber diplomacy. On the one hand, more than half of states have pronounced their interpretation of how international law applies to cyberspace, improving shared understanding, which itself is a positive development for stability. Similarly, an increasing number of states—and of non-state stakeholders within them—are engaging in a dialogue about the meaning of responsible behavior in cyberspace. This diplomatic dialogue is noticeably more gender-balanced than other UN discussions, attributable in part to concerted program support by donors from like-minded states.[71] Indeed, much of this increased dialogue and the development of an increasing number of national and regional positions on law and cyberspace have been made possible by like-minded donors of capacity-building assistance.[72] This again underlines the fact that capacity-building assistance is an important tool of cyber statecraft; significantly reduced capacity-building funding could lead to reversals.[73]

On the other hand, the pessimistic argument is that existing progress in global cyber diplomacy is both low-hanging fruit and consists of nonbinding commitments that are either perfunctory or, in the worst cases, routinely ignored. The cyber norms consist of eight prescriptive principles that enjoin "responsible" behavior (such as sharing information, protecting national infrastructure, safeguarding human rights, and reporting vulnerabilities so they can be remediated) and three proscriptive principles that prohibit "irresponsible" behavior (not allowing cyber attacks to emanate from your sovereign territory and not attacking another state's critical infrastructure or its computer emergency response teams).[74] Clearly, the salience of cyber crime alone as a severe global threat enabled by permissive, so-called safe-harbor jurisdictions indicates that some states are either unable or (much more likely, simply) unwilling to actively uphold their notional commitments to the prohibitive norms.[75] In this light, it is difficult to avoid the impression of hyperbole in any practitioner statement that the OEWG's agreement in principle of the Global Mechanism was a "historic" achievement.[76]

There is a sense in which states that know how to behave responsibly already do so and do not really need the norms to be enumerated repeatedly in an institutionalized dialogue, while those who do not behave responsibly are undermining the integrity of the normative process and calling the very utility of such a dialogue into doubt. The prognosis for the UN's cyber normative process is therefore contestable. This arguably aligns with Martha Finnemore's early (2011) assessment that any global cyber norms process would be similar to dealing with a "chronic condition that must be constantly managed rather than a single problem to be solved and put to rest."[77] Accepting this diagnosis does not commit one to a specific way of measuring cyber normative success in the future.

Pessimism about cyber capacity building is less radical than that regarding cyber norms because there is more widespread agreement about the value of capacity building, as reflected by its salience in the July 2025 final OEWG report and in the Global Mechanism's initial agenda. Improving the cybersecurity capacity of poorer and less capable states serves a developmental purpose, a global security purpose, and arguably a bilateral purpose (assuming donors perceive capacity building as being, in part, an influential tool of statecraft).[78] The main criticisms of capacity building in recent years have been about the need for better coordination among donors; improved professionalism and collaboration among donors, providers, and recipients in designing capacity-building interventions; and more recently, the potential implications of large reductions in development assistance in some donor states.[79] In light of this, the January 2026 decision by U.S. President Donald Trump's administration to withdraw from the Global Forum on Cyber Expertise (GFCE) suggests that improvements in collaboration and delivery are going to be even harder to achieve in the short term.[80]

The above makes clear the unsatisfactory nature of a shorthand description of cyber diplomacy as simply a contest between liberal, like-minded and authoritarian states. The like-minded bloc has been relatively cohesive over time—albeit with open questions about U.S. cyber diplomacy under the second Trump administration and about the ability of like-minded states to make good on their capacity-building commitments in times of straitened finances. Similarly, Russia and China often outright align or pursue similar proposals. But this leaves considerable variation. Middle ground states, including influential ones such as Brazil, India, and South Africa, participate in this process in ways consistent with the shaping effects of their different national interests, threat perceptions, and capacity constraints.

Constraints on Effective Cyber Diplomacy in the Middle Ground

As Stuenkel has noted more generally, there are input costs and capacity constraints on the ability of Global South states to exercise a role in setting the global agenda. Exercising this role requires thought-leadership expertise, political leadership willing to prioritize this advocacy, and sufficient international credibility to act as an interlocutor.[81] Expertise in cyber diplomacy has been slowly cultivated and unevenly distributed across the world's foreign ministries.

Over the past decade, Brazil and India, and to a lesser extent South Africa, have cultivated cyber diplomacy expertise and, at times, exercised prominent roles in multilateral forums. Brazilian diplomats participated in five of the six GGEs, chairing two iterations (Carlos Luís Dantas Coutinho Perez in 2014–2015 and Guilherme de Aguiar Patriota in 2019–2021).[82] India was the fifth host of the Global Conference on Cyber Space (2017), continuing a process started by the London summit (2011) and emphasizing the connection between cybersecurity and development, and further elaborating the principles underpinning cyber capacity–building.[83] South Africa was a member of several iterations of the GGE, but,

consistent with its wider diplomacy, has tended to concert its position on cyber diplomacy within the African Union, as it did with the common African position on the applicability of international law to cyberspace.[84] This is consistent with the bedrock principles of South African foreign policy, but potentially also indicates that collaborative processes are a shared mitigation of individual, sovereign capacity gaps.[85]

> **Analysis of cyber statecraft in Brazil, India, and South Africa suggests that cyber diplomacy is not a top priority for any of them.**

While these states engage in global cyber diplomacy, they each do so within the context of wider national strategy. Analysis of cyber statecraft in each of these countries suggests that cyber diplomacy is not a top priority for any of them.[86] This is not surprising, given the range of other pressing priorities each government faces. Even within technology diplomacy, many states are increasingly focused on the implications of AI, presenting a risk that, with finite diplomatic budgets and workforce, states will struggle to devote sufficient bandwidth and resources to cyber diplomacy.[87]

Arindrajit Basu and Karthik Nachiappan have argued persuasively that India's investment of diplomatic resources tracks its national strategy: Where India perceives the greatest strategic interest in so doing, Indian diplomacy will be proactively engaged.[88] This is a plausible explanation for India's more circumspect engagement with different aspects of global cyber diplomacy, including its reserve about multilateral efforts to constrain the commercial spyware/surveillance market (in which the Indian private sector is globally competitive) and its cautious engagement with the multilateral effort to devise and spread norms of responsible state behavior in cyberspace.[89] A strategic perception of India as a rising power might motivate a diplomatic strategy of reducing future constraints on India's sovereign exercise of cyber power. Conversely, India's reported experience of cyber attacks from Pakistan and China might understandably reduce its confidence in the efficacy of the cyber normative process.[90]

India's wider statecraft under Prime Minister Narendra Modi displays a focus on developing hard power capabilities and addressing defense and security threats, particularly from Pakistan and China. In this context, particularly if India contemplates the use of cyber operations against infrastructure in adversary states, it is unsurprising that India's engagement in cyber norms diplomacy exists—as it does in other cyber-capable states—in some degree of tension with its development of cyber capabilities and the doctrine underpinning their use.[91] In contrast, neither Brazil nor South Africa face such sharp security threats from other states. This more benign environment regarding "state threats" provides the context for both states' cyber diplomacy to endorse normative commitments in cyberspace as positive and implying no adverse impact on their sovereign ability to respond to cyber threats. Even more so for South Africa, which has fewer resources than the other two states to invest in developing its sovereign cyber capabilities, there is a prudential imperative to use normative

diplomacy to at least try to constrain the actions of more powerful states in this domain.[92] There is also the issue of interagency coordination and the distinct equities that operational and policy actors have within each national system, which is a "known unknown" of bureaucratic politics in the case of the coherence of Brazilian cyber statecraft.[93]

Politics and Middle Ground Cyber Statecraft

The international dimension of cyber statecraft has risen in salience over the past fifteen years, as more governments have invested in building cyber expertise in their foreign ministries, engaged in multilateral cyber normative discussions, negotiated the global cybercrime treaty, and interacted in the process of cyber capacity–building. These increasing diplomatic efforts track, and ultimately are a response to, an increase in the cyber threat environment, particularly in the debilitating impact of cybercrime, but also to the reality that an increasing number of states are exploring the use of cyber operations to pursue national strategic objectives.[94]

In some states, such as the United Kingdom and the United States, diplomatic and foreign policy institutions have become more prominent in developing and executing cyber statecraft. Recent iterations of UK and U.S. cyber strategy have included more extensive elaboration of the international dimensions of cyber statecraft.[95] But this should not imply that foreign ministries will inevitably hold and build on this gain in institutional status over time. Reversals are possible. This is particularly the case with administration changes, budgetary realities, departmental restructuring and workforce reductions, or rebalancing by other institutional actors to dial down the emphasis on cyber diplomacy and capacity building, for example (as in the case of the UK) by reemphasizing the importance of domestic resilience and cybersecurity.[96]

Over the same period, Brazil, India, and South Africa have improved their foreign ministries' capacities to engage in bilateral, regional, minilateral, and multilateral cyber discussions. But none of these states built a foreign policy bureau as big as the U.S. Department of State's Bureau of Cyberspace and Digital Policy, or the UK Foreign, Commonwealth and Development Office's Cyber Policy Department. This is mostly a question of different scales in the size of respective foreign ministries. But it also reflects decisions about the prioritization of available resources.[97] Such decisions are ultimately political in every state, notwithstanding the fact that nowhere has cyber statecraft been a polarizing or high-salience issue in domestic political partisanship.[98]

The relatively low *political* salience of cybersecurity applies in countries that have not experienced a major national cyber incident of the kind that has affected Costa Rica or Estonia.[99]

Absent such a compelling imperative, it is difficult to imagine what would prompt any state to sharply elevate the political priority of cybersecurity.[100] The impact of domestic politics on cyber statecraft is therefore more likely to be indirect.

The Politics of Cyber Statecraft in Brazil

In Brazil, the presidency has pursued an ambitious agenda to improve national governance of cybersecurity.[101] It has been able to do so, to some extent, because cybersecurity is less politicized than other aspects of its domestic agenda, but this has its own limiting effect. These reforms have suffered from the wider difficulty of making progress through Congress, and, because 2026 was a presidential election year, further delays were near inevitable as the year progressed. As the 2026 election was proceeding to a run-off as this paper went to press, we can assess Brazil's cyber statecraft during President Luiz Inácio Lula da Silva's third term in office, which was won by a slim margin in 2022. This term was marked by a very difficult relationship with Congress and struggles to advance his program of government. The wider fiscal and political situation circumscribed the government's broader agenda, but it was not clear that this was the sole reason that more was not achieved in advancing the Lula government's ambitious domestic cybersecurity agenda.[102] These structural constraints will persist in Lula's fourth term, following his dramatic October 2026 presidential run-off victory, whereas his defeated competitor—Flavio Bolsonaro—would have enjoyed stronger political support in the recently elected Congress.[103]

The Lula administration's relationship with the Brazilian Armed Forces, in the context of a longer-term trend in civil-military relations since the return to democracy, meant that there were sharp limits to civilian influence over national defense strategy, including cyber defense. This extended to the development of cyber capabilities and the elaboration of relevant doctrine in the armed forces. But given Lula's wider foreign policy approach, his party's historical and political stance on intelligence and security operations, and the strategic and cultural constraints on the external operations of the Brazilian Armed Forces, it was always unlikely that he would task the armed forces to conduct disruptive or destructive cyber operations overseas.[104]

Separately, given both the political history and the more recent domestic spyware scandal involving his predecessor's administration, it is probably reasonable to assume that there are few, if any, nasty surprises to be uncovered about misuse of domestic surveillance tools under Lula.[105] That said, it was somewhat interesting that Brazil, like South Africa and India, did not join the UK-France Pall Mall Process to counter the proliferation and irresponsible use of commercial cyber intrusion capabilities.[106] In Brazil's case, given its prioritization of the multilateral process in foreign policy, it is highly likely that its decision not to embrace the Pall Mall Process was because the process stood outside of the formal multilateral auspices of the United Nations.[107] Brazil might also have been concerned to preserve nonalignment, as the Pall Mall Process could be interpreted as criticizing the behavior of states with which Brazil has good bilateral relations.

The overall impression of the politics of Brazilian cyber statecraft under Lula was that, beyond domestic issues, there was little political momentum being supplied by Lula's government. In the absence of such impetus from the political side of the executive branch, individual lines of official effort were pursued, either progressively (domestic governance reforms), in continuity with past practice (cyber diplomacy and cyber defense), or in direct response to politically charged digital policy issues, such as countering online disinformation and extremism.[108] The transition between President Jair Bolsonaro and Lula demonstrated the potential impact of presidential elections on the principles guiding Brazil's foreign relations.[109] This was particularly evident in the case of the bilateral relationship between Brazil and the United States under Lula and Trump, which could be characterized as strained and transactional.

For six months, between Trump's January 2025 inauguration and mid-July, Lula and Trump coexisted without a major blow up in bilateral relations, contrary to some expectations. Commentators reflected on a variety of factors to explain why this was the case, including Brazil's careful diplomacy, even while cultivating relations and positions that were not in sync with the Trump administration, and Brazil's lower strategic visibility in Washington than, say, Mexico.[110]

However, the bilateral relationship took a sharp turn for the worse when Trump announced in July 2025 that he would impose an additional 50 percent tariff on Brazilian products, citing concern about the legal proceedings against former president Bolsonaro and criticizing the Brazilian approach to regulating digital expression.[111] Coming soon after the completion of the Rio de Janeiro BRICS summit meeting, it was also assumed that the move was partly motivated by Trump's perception of BRICS as pursuing an anti-U.S. agenda.[112]

Trump's tariff decision was widely interpreted in Brazil as an act of foreign interference in domestic politics. This was not an interpretation without foundation: Trump explained his decision in light of what he regarded as a "witch hunt" against Bolsonaro by the Brazilian legal system. Given the potential for a strong negative public reaction against Trump,[113] this episode created a political problem for Brazil's right wing and exposed the different agendas within it.[114] The Bolsonaro family portrayed the situation as requiring an amnesty for Bolsonaro for Brazil to avoid the tariff increase. In contrast, the wider political right, including likely presidential candidates, sought to portray the crisis as caused by Lula's diplomacy and requiring resolution via an effective negotiating response.[115] For the Lula government, while this was a major policy crisis, it offered a potential political opportunity for an administration that had been struggling and would face a tight contest for reelection. The Lula government successfully pursued a negotiated solution, and it benefited instrumentally from public anger at Trump's tariffs and was able to rebuild a wider constituency of support among the electorate.[116] Separately, the January 2026 U.S. military operation in Venezuela, leading to the capture of President Nicolás Maduro, was similarly interpreted as a regional threat by Lula's chief international adviser, Celso Amorim.[117]

Given the relatively low political salience of cyber issues in Brazil's wider statecraft, it was not simply the case that the outcome of the 2026 presidential run-off—Bolsonaro or Lula—would determine whether or not Brazil closely aligned with U.S. positions in cyber diplomacy. This has been visible at the intragovernmental level, where one important research question regarding Brazilian cyber statecraft is the coherence of separate efforts pursued by Brazil's Ministry of Foreign Affairs (normative cyber diplomacy) and the Brazilian Armed Forces (cyber defense and cyber operations). The coherence conundrum is whether long-term efforts by the Brazilian Armed Forces to develop operational cyber capabilities are closely coordinated with national red lines implicit in Brazil's cyber normative engagements in international multilateral forums. Apart from questions about the political and resource constraints on Brazil's cyber hard power, the opacity surrounding this relationship at the heart of Brazil's cyber statecraft renders it difficult for outsiders to interpret the medium-term future of Brazil's development of cyber power. The inter-institutional politics of Brazil's cyber statecraft therefore complicate any effort to simply read across from affinity or tension between heads of state in Brasilia and Washington.

This is the bureaucratic and institutional context within which to interpret the significance of Lula's 2026 presidential run-off victory for the next four years of Brazil's cyber statecraft. Forecasts of Brazil's next steps should factor in the relatively low level of political salience (and leadership appetite) for cyber statecraft. If Flavio Bolsonaro had won the run-off, there would have been greater political alignment between his administration and that of Donald Trump in Washington. A Bolsonaro administration would have inherited the same structural position of Brazil in the international system but would have approached it with a different ideological viewpoint, especially regarding bilateral relations with the United States and China.[118]

In contrast, Lula's fourth term begins with additional complications in the Brazil-U.S. bilateral relationship brought on by Bolsonaro's flight to Miami to avoid a money laundering investigation and the apparent acquiescence of the Trump White House to this development, amid Trump himself initially floating doubts about Lula's victory as looking like "another rigged election."[119] None of this makes the elite personality politics any easier in the short term, but the most plausible forecast of cyber statecraft in Lula's fourth term is one of continuity: slow, incremental institutionalization under the ongoing constraints on Lula's wider governing project, namely acutely contested political prioritization, limits on resource allocation, and indeed the limits to Lula's own power in a system of coalitional presidentialism.[120]

The Politics of Cyber Statecraft in India

India's cyber statecraft mirrors trends in Modi's diplomatic and political strategy, together with the longer-term impact of issues such as national development, strategic culture, and challenges in military modernization.[121] In interagency terms, India's cyber statecraft

resembles many other states in comprising nuanced interaction among actors with different equities—all ultimately under the aegis of Modi's decisionmaking. The central security apparatus, under Indian National Security Advisor Ajit Doval, understandably plays a key role on pivotal files such as China and Pakistan, and this extends to the domestic security and operational elements of cyber statecraft.

As in other countries, none of these issues is deeply partisan politically, but both domestic and international aspects of Modi's cyber statecraft are inherently part of his national security approach. For example, the border clash with China in 2020 reportedly led to intensified effort to improve the cyber capabilities of the Indian Armed Forces and its intelligence agencies, especially the National Technical Research Organisation.[122] India's public communication about its emerging cyber doctrine has traditionally been cautious, most likely to preserve ambiguity, but over time, there could be a prudential argument to consider more public statements to reduce misperception risks and enhance deterrence.[123]

Regarding the international dimensions of India's cyber statecraft, its cyber diplomacy displays commitment to the UN processes (GGE, OEWG, and negotiation of the cybercrime treaty) and, like Brazil, a related reluctance to join ad hoc initiatives outside the multilateral context, such as the Summits for Democracy hosted by former U.S. president Joe Biden (including the summits' cyber provisions) and the Pall Mall Process. While Indian civil society groups are active in cyber diplomacy, there is little sense that this has crystalized into a meaningful political constraint or shaping factor on India's cyber diplomacy. The nuances and ambiguities of the country's cyber statecraft are therefore more attributable to the wider mechanics of Modi's foreign policy and interagency decisionmaking about the highest priority national security files. India's positions, including supporting norms of responsible state behavior in cyberspace and constraining the global spyware market, are shaped by the Modi government's perception of national interest and the need to avoid constraining India's current and future freedom of action as a rising global power.[124]

Of the three middle ground states profiled in this paper, India exhibits some starkly different cyber statecraft challenges and opportunities. China presents a diplomatic and operational challenge unlike any facing Brazil or South Africa. The bilateral relationship has improved since the 2020 border clash, with a cautious "managed rivalry" emerging to navigate security risks amid continuing economic interdependency.[125] There are realistic prospects for further confidence-building measures; however, it will take time to restore bilateral trust, raising the question of whether and how like-minded states can rejuvenate cooperation with India, for instance, under the auspices of the Quad.[126]

Similarly, how India manages U.S. frustrations over its continued ties to Russia—perceived as a necessity for India, given its strategy for the China threat[127]—situates India's cyber statecraft in a more nuanced and awkward relationship with great power competition.[128] There are some signs, for example regarding India reducing oil imports from Russia, of it being responsive to U.S. pressure.[129] Alongside these challenges, India's latent and rising cyber power also creates opportunities on a scale outmatching its middle ground counterparts.

There is simultaneously an urgent imperative for India to rapidly improve its domestic cybersecurity and resilience and shepherd the institutional development of operational cyber capabilities among civilian, military, and private sector actors, and, on the more optimistic side, real potential for India to achieve progress in both national missions. While India will continue to engage in multilateral cyber diplomacy, including active participation in the Global Mechanism, in a manner consistent with its approach to multilateralism and leading the promotion of the Global South's shared interests, the success or failure of India's cyber statecraft will be measured by its ability to rapidly improve its defenses and its capacity to undertake (or credibly threaten the use of) offensive cyber operations.[130]

The Politics of Cyber Statecraft in South Africa

Post-apartheid South African statecraft has been dominated by the African National Congress (ANC), the political party with the largest vote share at every national election since 1994, which was the first election with universal suffrage. Over its first decade, the ANC increased its electoral dominance, securing a two-thirds majority in the National Assembly.[131] From this zenith, the ANC's electoral fortunes waned gradually, until it finally lost its outright majority in 2024—albeit remaining the largest party and continuing in government with coalition partners.[132] This decline continued in the November 2026 local elections, with the ANC suffering its worst ever results.[133]

The ANC's waning electoral fortunes are attributable to significant splits within its political movement. The electoral performance in 2024 of two parties led by former ANC politicians, the Economic Freedom Fighters and *uMkhonto weSizwe* is one example. The South African Communist Party's decision to assert its independence of the ANC and contest the November 2026 local elections is another.[134] Moreover, corruption scandals and voter disillusionment based on a sense that, notwithstanding the enormous challenges it inherited in 1994, the ANC has struggled to deliver the growth, poverty reduction, economic development, and quality public services have also contributed.[135]

The domestic security and defense-related aspects of South African cyber statecraft face sharp resource and capacity constraints. This is consistent with the wider defense and security sector across the ANC's period in government.[136] Successive ANC governments prioritized domestic socioeconomic expenditure, consistent with their strategic objectives to grow the economy and improve the circumstances and opportunities of the majority of South Africans who had been so systemically exploited during the apartheid era.[137]

Given the magnitude of socioeconomic problems facing the ANC in government and the relatively benign state threat environment in Southern Africa, such an orientation of public expenditure is understandable, even though it comes at the cost of South Africa's ability to effectively deploy its armed forces for national defense and missions such as peacekeeping in the Democratic Republic of the Congo. The situation of cyber defense reportedly mirrors this reality, with significant questions about the adequacy of resources available to South Africa's Cyber Command.[138]

The relatively low strategic priority afforded to cybersecurity by the ANC also reflects its relatively low political salience in South Africa. As noted above, this is an experience shared with Brazil, India, and many other countries. Cybersecurity is simply not a major issue in South African multi-stakeholder engagement in public policy, notwithstanding criticism of specific issues, such as surveillance legislation or controversies over the domestic use of commercial spyware.[139]

Internationally, South African cyber diplomacy is consistent with the leading principles of South African foreign policy. A pan-African approach has long been a key feature of South Africa's diplomacy under the ANC, and it is a cornerstone of its cyber diplomacy. For instance, South Africa has followed the common African position on the applicability of international law to cyberspace. Regarding principles to regulate the global commercial cyber intrusion market through the Pall Mall Process, South African participation was explicitly under the auspices of the African Union. Beyond that, as expected from a state lacking significant cyber capabilities of its own and generally supportive of multilateral processes promoting international security, South Africa has been a persistent participant in the UN cyber norms process and similarly in the negotiation of the global cybercrime treaty. South Africa also conforms with the wider IBSA and BRICS commitment to pursue "digital sovereignty" and digital development.[140]

South African cyber statecraft shares several common features with those of Brazil and India, both in terms of commitment to multilateralism and membership in overlapping forums such as IBSA and BRICS. But South Africa confronts many of the same issues from a position of relational weakness. It carries the weight of neither Brazil nor India in international forums. It cannot match the investment in cybersecurity, resilience, or operational capabilities that is being made in Brazil and India. The bilateral U.S.-South Africa tensions experienced under the second Trump administration similarly highlight South Africa's greater exposure to contemporary geopolitical turbulence.[141]

> **While Brazil and India appear capable of managing their dependencies and retaining strategic autonomy, the constraints on South Africa are greater.**

All this pushes South Africa to embrace even further the strategy of partnerships it has pursued for several decades, continentally through the African Union and economically and geopolitically through engaging with China and the BRICS+, including Brazil and India.[142] While the recent tensions in South African relations with the United States have a new element of volatility—for example, over tariffs—the long-term strategy of South African foreign policy has been consistently to deepen its relationship to China, and wider via BRICS+, to better position itself in a changing international order.[143] Twenty years ago, like-minded diplomats might have instinctively expected South Africa to row behind most of their positions in multilateral forums, but the reality over time has seen South Africa shift

toward China. While Brazil and India appear capable of managing their dependencies and retaining strategic autonomy, the constraints on South Africa are greater. This truth is clearly wider than cyber statecraft, but, in light of the contextual factors shaping South African cyber statecraft outlined above, it applies equally to it.

Engaging and Influencing the Middle Ground

There is a broad commonality of experiences shared by the countries described as being in the middle ground. They adopt similar positions in multilateral cyber diplomacy and face similar challenges in principle from the great power competition shaping international politics. While the expansion of BRICS suggests an effort by several middle ground countries to concert their positions in new forums, this does not contradict a key argument of this paper, namely that each state maintains its own sovereign agency over its national cyber statecraft. If like-minded states want to engage and influence these middle ground states more effectively than China and Russia, they need to do so by focusing on each state's sovereign interests and decisionmaking processes. Any strategy for the middle ground requires tailored implementation plans for each country, or else it will be filtered through a layer of unnecessary and possibly counterproductive abstraction. At a time of foreign ministry retrenchment, this will require ever closer collaboration between cyber offices and in-country representatives. Reductions in cyber capacity–building funding will likely make these strategies even harder to implement effectively. In fact, the risk is that China in particular will selectively prioritize its engagement, for example in South Africa, to entrench its ties further.

The necessary starting point for like-minded states is to clarify first, for themselves, what it is that they want to achieve by engaging and influencing middle ground states. This is not always as discernible, nor as sharply conceived, as it should be in like-minded cyber statecraft. In 2022, the then director of the UK cyber and signals intelligence agency, Government Communications Headquarters (GCHQ), argued that like-minded states needed to establish a "persuasive and coherent" "counteroffer" to Chinese influence with those states "who haven't yet decided which way they should jump," noting that "too often" like-minded offers were not sufficiently persuasive or coherent.[144] One example is the difficulty of finding a price-competitive challenger to China's telecommunications infrastructure. But part of the problem could be to some extent self-inflicted: The attractiveness of a digital sovereignty agenda to middle ground states should not be a surprise, not least because all states care about sovereignty and national capability. The challenge for like-minded states is how to navigate different national interpretations of how states should exercise sovereignty in and through cyberspace, and ultimately to decide how much they prioritize the issue in the context of each bilateral relationship.

Likewise, on the contribution of nongovernmental stakeholders in the future UN multilateral cyber dialogue process, it appears that the like-minded states have accepted that the most feasible grounds for agreement lay in the de facto maintenance of the veto on stakeholder participation. The compromise, involving up to three months of consultation to explore whether a veto might be waived, seems very thin. Whether this outcome was worth the effort of arguing the point is open to question, particularly as like-minded states can continue to organize shadow programs of multistakeholder participation alongside meetings of the Global Mechanism. They can ensure that these are well organized, properly funded, and facilitate broadly balanced global stakeholder representation. This was always likely to be the simplest option, playing to the existing soft power strengths of like-minded cyber diplomacy and demonstrating their commitment to capacity building—a theme of rising prominence in the final OEWG draft report, but a goal that the Global Mechanism will struggle to pursue due to funding reprioritization.

Where appropriate, and shaped for specific national context, further intensification of cyber defense cooperation should also be a part of like-minded cyber statecraft toward middle ground states. Elements such as "hunt forward" operations might not be well-received in all cases, but there are many other ways for bilateral or minilateral military-to-military or intelligence agency-to-agency ties to improve cooperative cyber defense, as there are from the involvement of the private sector. As noted above, it is crucial for such efforts to be persuasive and coherent—both within a national approach to cyber statecraft and in coordination across like-minded states. This does not happen by accident and requires significant collaboration and active management. It requires leadership from senior career officials, as well as the explicit buy-in and resource commitment of political leaders. There is also explicit competition: The September 2026 New Delhi Declaration indicated that BRICS+, however loosely institutionalized the group may be, is advancing a range of cooperative cybersecurity initiatives. Like-minded states need to think carefully about how to navigate this ongoing development.

> **A more direct focus on capacity building, technical cooperation, and actively cultivating roles for like-minded states' private companies is likely to be a more constructive framework for cyber statecraft.**

Geopolitically, it is unsurprising that of the three middle ground states compared in this paper, India has enjoyed more of such attention, mostly due to its size and proximity to China. But the logic is the same for Brazil, South Africa, and other influential middle ground states, such as Indonesia, Saudi Arabia, and the other Gulf Arab states. The best ways for like-minded states to engage with them will vary from state to state, and some like-minded states will be better placed than others to engage on specific issues. Notwithstanding this context dependence, a more direct focus on capacity building, technical cooperation, and actively cultivating roles for like-minded states' private companies, is likely to be a more

constructive framework for cyber statecraft toward these states than more like-minded engagement regarding the tortuous fate and questionable value of the future multilateral cyber normative process.

In the current context of geopolitical competition, it is strategically prudent for like-minded states to calibrate their cyber statecraft more directly toward these security and prosperity objectives than toward the normative aspects of cyber diplomacy, particularly as they apply to sovereign decisions over the domestic internet in different states. This has long been the approach pursued by China.[145] This does not mean that such priorities disappear from the agenda, but it does reflect an already discernible trend in particularly UK and U.S. statecraft in general: to focus more narrowly on the security and prosperity elements of the strategic triad of security, prosperity, and values. Viewed competitively with respect to Russian and Chinese cyber statecraft, there are also likely to be obvious wedge issues to emphasize and address, such as the global impact of Russia-originated cyber crime and the perceived threat of China's military and cyber power in the Indo-Pacific region.

Conclusion

The middle ground is more than a convenient bureaucratic shorthand phrase; however, as an analytical concept to inform cyber statecraft strategies, it must be handled carefully, with recognition of the context dependence of cyber statecraft across states. Any term denoting a group of states as different as Brazil, India, and South Africa, is going to struggle for definitional precision or one-size-fits-all policy insights. While there is a clear need for like-minded states to recognize that they are in a competition to influence the middle ground states, their engagements must tailor to fit each case bilaterally and, where appropriate, through regional organizations and existing (or new) forms of minilateralism.

There is a broad commonality within the so-called middle ground in its approach to multipolarity and embrace of the fluidity of bilateral and minilateral relations. But the breadth and depth of strategic autonomy enjoyed by these states, in the development and use of the tools of cyber statecraft, varies considerably according to differences in relational power, strategic culture, threat perception, and the impact of domestic factors such as governance and developmental issues.

The capacity and inclination of each such state to instrumentalize the return of competition as a theme of great power grand strategy clearly differs, but that does not change the fact that like-minded states develop and implement cyber statecraft strategy in a competitive environment. This is most true with respect to Chinese cyber statecraft and the need for like-minded states to think carefully about what each can best do, individually and collectively, to counter growing Chinese influence in these states. Like other areas of like-minded cooperation, the diversity of national interests within the like-minded group could

potentially affect the coherence of engagements with middle ground states, particularly when they are framed as selective bilateral engagements. And where the like-minded objectives are relatively consistent—for example, persuading middle ground states to reduce dependence on Chinese technology or to behave responsibly in cyberspace or as customers for commercial cyber capabilities—it needs to be recognized that the domestic political and strategic structural factors driving middle ground statecraft will shape what is possible in each case.

Over the past decade, like-minded cyber statecraft has been neither as urgently nor as coherently pursued as it might have been. It is possible for like-minded states to do better, but this will require a degree of patient, sustained, and well-resourced effort, underpinned by political commitment, that is not readily discernible across the like-minded group. The general resource constraints and range of political factors that impede progress in democratic cyber statecraft will not make improvement easy to deliver. As all this is a dynamic and not a passive process, like-minded states must also be attuned to (and be ready to counter) what is happening in competitor states, and to the interests of those states with which the like-minded states wish to engage and influence.

Notes

1 In the United Kingdom, at least, "statecraft" appears to be enjoying a renaissance, as evidenced by the recent creation of research centres in Oxford (Strategy, Statecraft, and Technology) and London (Statecraft and National Security). David A. Baldwin offers a usefully concise definition of the practice of statecraft: "the instruments used by policy makers in their attempt to exercise power, i.e. to get others to do what they would not otherwise do." See David A. Baldwin, *Economic Statecraft (new edition)* (Princeton, New Jersey: Princeton University Press, 2020), 7.

2 Mark Raymond and Justin Sherman, "Authoritarian Multilateralism in the Global Cyber Regime Complex: The Double Transformation of an International Diplomatic Practice," *Contemporary Security Policy* 45, no. 1 (2024): 110–140.

3 See the series of Carnegie papers on "cyber diplomacy in the Middle Ground," Technology and International Affairs Program, "Cyber Diplomacy in the Middle Ground," Carnegie Endowment for International Peace, July 29, 2025, https://carnegieendowment.org/programs/technology-and-international-affairs/collections/cyber-diplomacy-in-the-middle-ground.

4 This pivotal status was captured in two earlier phrases: "swing states" and "digital deciders." See Tim Maurer and Robert Morgus, *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate* (Waterloo, Canada: Centre for International Governance Innovation and Royal Institute for International Affairs, 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no2.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.

5 To see this argument applied to the United Nations' cybercrime treaty negotiation, see Arun Sukumar and Arindrajit Basu, "Back to the Territorial State: China and Russia's Use of UN Cybercrime Negotiations to Challenge the Liberal Cyber Order," *Journal of Cyber Policy* 9, no. 2 (2024): 1–32, https://doi.org/10.1080/23738871.2024.2436591.

6 Amitav Acharya, *The End of American World Order* (Cambridge: Polity, 2014); and Amitav Acharya, "Thinking Beyond a Polarized World: Why Multiplexity Matters," *International Affairs* 102, no. 2 (2026): 503–511.

7 In a non- or wider-than cyber context, John G. Ikenberry noted a lack of cohesion in the group of rising powers in the early twenty-first century: "rising states do not constitute a bloc that seeks to overturn or reorganise the existing international order. China, India, Russia, Brazil, South Africa and others all are seeking new roles and more influence within the global system. But they do not constitute a new coalition of states seeking global transformation." See John G. Ikenberry, "The Liberal International Order and Its Discontents," *Millennium: Journal of International Studies* 38, no. 3 (2010): 515, https://doi.org/10.1177/0305829810366477.

8 For an introduction to the neoclassical realist approach to foreign policy, see Jeffrey W. Taliaferro, Steven E. Lobell, and Norrin M. Ripsman, "Introduction: Neoclassical Realism, the State, and Foreign Policy," in Jeffrey W. Taliaferro, Steven E. Lobell, and Norrin M. Ripsman (eds.), *Neoclassical Realism, the State, and Foreign Policy* (Cambridge: Cambridge University Press, 2009), 1–41.

9 Barry Posen has argued that increasing multipolarity necessitates more active diplomacy in pursuit of "coalition building." See Barry Posen, "Emerging Multipolarity: Why Should We Care?," *Current History* 108, no. 721 (November 2009): 350.

10 The same could be said for states within the like-minded group. Perhaps the sharpest framing by a head of government of the wider, intra-like-minded tensions experienced during the second Trump administration is that of Canadian Prime Minister Mark Carney. See Mark Carney, "Davos 2026: Special Address by Mark Carney, Prime Minister of Canada," World Economic Forum, January 20, 2026, https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada.

11 Jochen Prantl, "Reuniting Strategy and Diplomacy for 21st Century Statecraft," *Contemporary Politics* 28, no. 1 (2021): 8, https://doi.org/10.1080/13569775.2021.1961387.

12 Valerie M. Hudson and Christopher S. Vore, "Foreign Policy Analysis Yesterday, Today, and Tomorrow," *Mershon International Studies Review* 39, no. 2 (October 1995): 210. This complexity also translates to the challenges of cybersecurity at the regional level. See Joe Devanny, "Cyber Threats in Latin America: Cybersecurity Cannot Be Depoliticized," *CEBRI Journal* 5, no. 17 (2026): https://cebri.org/revista/en/artigo/283/cyber-threats-in-latin-america.

13 High priority does not guarantee successful outcomes. For an example of an analysis of the UK government's strategic approach to the 2003 Iraq war, which makes the case that even high priority issues can be pursued unsuccessfully, see William D. James, *British Grand Strategy in the Age of American Hegemony* (Oxford: Oxford University Press, 2024).

14 Baldwin, *Economic Statecraft*.

15 Kevin Poireault, "U.S. to Leave Global Foreign on Cyber Expertise," *Infosecurity Magazine*, January 8, 2026, https://www.infosecurity-magazine.com/news/us-leave-global-forum-on-cyber.

16 Sukhwant S. Bindra, "Analysing Foreign Policy," *World Affairs* 23, no. 3 (2019): 26; and Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, New Jersey: Princeton University Press, 1997).

17 Susan Strange, *The Retreat of the State: The Diffusion of Power in the World Economy* (Cambridge: Cambridge University Press, 1996), 24–29; and Robert Jervis, *Perception and Misperception in International Politics: New edition* (Princeton, New Jersey: Princeton University Press, 2017).

18 This trend is unsurprising but unfortunate. Decisionmakers should certainly address the international security implications of artificial intelligence (AI) but also need to confront the range of contemporary cybersecurity challenges, several of which are interconnected with the impact of AI. See Joe Devanny, *Artificial Intelligence and Cyber Power* (Miami: Jack D. Gordon Institute for Public Policy, Florida International University, 2024), https://digitalcommons.fiu.edu/jgi_research/63. More recently, see Anne Neuberger, "The New Chinese Way of Cyberwar: How Beijing Will Weaponize Digital Chokepoints," *Foreign Affairs*, September 15, 2026, https://www.foreignaffairs.com/china/new-chinese-way-cyberwar-ai.

19 The UK provides an example of this challenge, with its foreign ministry forecast to reduce its workforce by 25 percent over the next four years. See Jim Dunton, "FCDO's Domestic Staff to 'Bear Brunt' of Job Cuts, Perm Sec Says," *Civil Service World*, December 12, 2025, https://www.civilserviceworld.com/professions/article/fcdos-domestic-staff-to-bear-brunt-of-job-cuts-perm-sec-says.

20 For different perspectives on the variety of national organizational arrangements for cyber operations, see Daniel Moore, *Offensive Cyber Operations* (London: Hurst, 2021); and Max Smeets, *No Shortcuts* (London: Hurst, 2021).

21 Subrahmanyam Jaishankar, "S. Jaishankar on India's Growing Global Role," *The Economist*, November 13, 2023, https://www.economist.com/the-world-ahead/2023/11/13/s-jaishankar-on-indias-growing-global-role; Subrahmanyam Jaishankar, *Why Bharat Matters* (New Delhi: Rupa Publications, 2024), 54; and Jorge Heine, "Active Non-Alignment and Global Governance: From Latin America to the Global South," *Global Governance* 30 (2024): 214–224.

22 Heine, "Active Non-Alignment," 220.

23 Louise Marie Hurel, "New Ways to Frame Responsible Cyber Behaviour Beyond the UN," RUSI, May 13, 2025, https://static.rusi.org/new-ways-to-frame-rcb-beyond-un.pdf.

24 It is an open question about the next iteration of UK national cyber strategy, expected to be published later in 2026 under the restyled title "National Cyber Action Plan,", whether it will choose to retire the concept of "Responsible Democratic Cyber Power" and how much it will focus on the international dimensions of cyber statecraft. "Responsible Democratic Cyber Power" does not, for example, appear in the most recent iteration of UK National Security Strategy, published in June 2025. For the origins of this concept in UK strategy, see Joe Devanny and Andrew Dwyer, "From Cyber Security to Cyber Power: Appraising the Emergence of 'Responsible, Democratic Cyber Power' in UK Strategy," in *15th International Conference on Cyber Conflict: Meeting Reality* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2023), 381–398, https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf.

25 Adapted from Baldwin, *Economic Statecraft*, 7.

26 Influence operations can even be competitive, see "More-Troll Kombat: French and Russian Influence Operations Go Head to Head Targeting Audiences in Africa," Graphika and Stanford Internet Observatory Cyber Policy Center, 2020, https://public-assets.graphika.com/reports/graphika_stanford_report_more_troll_kombat.pdf.

27 For reporting of three such operations, see Robert Chesney, "Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility," Lawfare, May 6, 2019, https://www.lawfaremedia.org/article/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility; and Catalin Cimpanu, "Israel Bombed Two Hamas Cyber Targets," *The Record* (blog), Recorded Future News, May 19, 2021, https://therecord.media/israel-bombed-two-hamas-cyber-targets.

28 Evan Potter (ed.), *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century* (Montreal & Kingston: McGill-Queen's University Press, 2002).

29 For wider reading on cyber diplomacy, see Andrea Salvi, Heli Tiirmaa-Klaar, and James Andrew Lewis (eds.), *A Handbook for the Practice of Cyber Diplomacy* (Luxembourg: EU Institute for Security Studies, 2025); and George Christou, Wilhelm Vosse, Joe Burton, and Joachim A. Koops (eds)., *The Palgrave Handbook on Cyber Diplomacy* (London: Palgrave Macmillan, forthcoming).

30 Vice Adm. (Ret.) Ross A. Myers, Embracing a Whole-of-Nation Approach to the 2026 National Cybersecurity Strategy Inspired by the Manhattan Project. *Cyber Defense Review 11(2)*, 2026, 249-254, https://cyberdefensereview.army.mil/Portals/6/Documents/2026-vol11-iss2/CDR_V11_N2_Myers.pdf.

31 This formulation follows Baldwin, *Economic Statecraft*, 118.

32 A non-exhaustive list of different approaches includes Belfer Center for Science and International Affairs, "Cyber

Power Index," Harvard Kennedy School, 2022, https://www.belfercenter.org/publication/national-cyber-power-index-2022; "Cyber Power Matrix," International Institute for Strategic Studies, accessed October 10, 2026, https://www.iiss.org/cyber-power-matrix/overview; "Global Cybersecurity Index," International Telecommunication Union, June 2026, https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx; "Cyber Readiness Index," Potomac Institute for Policy Studies, November 2015, https://www.potomacinstitute.org/about/centers/past-centers/cyber-readiness-index; and Global Cyber Security Capacity Centre, "Cyber Security Capacity Maturity Model for Nations," University of Oxford, 2021, https://gcscc.ox.ac.uk/the-cmm.

33 Baldwin, *Economic Statecraft*, 12.

34 The impact of geopolitical context on the evolving understanding of cyber statecraft is particularly noticeable in the ways in which researchers are responding to increasing number of cyber operations in the context of armed conflict. The earliest theoretical accounts of the utility of cyber operations did not benefit from this number of cases, so the forward agenda of cyber statecraft research will include a focus on how states use cyber capabilities in the context of contest and conflict.

35 For background reading on each state's approach to cyber statecraft, see Joe Devanny and Arthur Laudrain, "Interpreting India's Cyber Statecraft," Carnegie Endowment for International Peace, March 27, 2025, https://carnegieendowment.org/research/2025/03/interpreting-indias-cyber-statecraft; Joe Devanny and Russell Buchan, "Brazil's Cyber Strategy Under Lula: Not a Priority, but Progress Is Possible," Carnegie Endowment for International Peace, August 8, 2023, https://carnegieendowment.org/research/2023/08/brazils-cyber-strategy-under-lula-not-a-priority-but-progress-is-possible; and Joe Devanny and Russell Buchan, "South Africa's Cyber Strategy Under Ramaphosa: Limited Progress, Low Priority," Carnegie Endowment for International Peace, January 12, 2024, https://carnegieendowment.org/research/2024/01/south-africas-cyber-strategy-under-ramaphosa-limited-progress-low-priority. For analysis of another middle ground state's cyber strategy, see Joe Devanny and Russell Buchan, "Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO," Carnegie Endowment for International Peace, May 28, 2024, https://carnegieendowment.org/research/2024/05/mexicos-national-cybersecurity-policy-progress-has-stalled-under-amlo.

36 Yu-Shan Wu, "What the BRICS Reflects About International Order," in Aaron McKeil and Stuart Austin (eds.), *International Order Strategies* (London: LSE Ideas, 2024), 44–49; and Sanusha Naidu and Gustavo de Carvalho, *BRICS Expansion: Redefining Global Structural Power in a Changing World Order* (Pretoria: South African Institute of International Affairs, 2025).

37 Anit Mukherjee and Caroline Arkalji, "Revitalizing IBSA: India, Brazil, and South Africa," ORF America, November 7, 2024, https://orfamerica.org/orf-america-comments/revitalizing-india-brazil-south-africa.

38 Oliver Stuenkel, "BRICS Democracies Are Losing Leverage," *Foreign Policy*, May 20, 2025, https://foreignpolicy.com/2025/05/20/india-brazil-south-africa-brics-ibsa-russia-china-trump.

39 Chris Alden and Marco Antonio Vieira, "The New Diplomacy of the South: South Africa, Brazil, India and Trilateralism," *Third World Quarterly* 26, no. 7 (2005): 1,077–1,095.

40 Ash Narain Roy, "Treat IBSA as Good BRICS," *The Diplomat*, June 16, 2025, https://diplomatist.com/treat-ibsa-as-good-brics.

41 Ashley J. Tellis, "India's Great-Power Delusions," *Foreign Affairs*, June 17, 2025, https://www.foreignaffairs.com/india/indias-great-power-delusions.

42 Elizabeth Sidiropoulos, "IBSA: Avoiding Being BRICked Up," *Strategic Analysis* 37, no. 3 (2013): 285–290, https://doi.org/10.1080/09700161.2013.782628.

43 Manoj Kumar and Mayank Bhardwaj, "India, Brazil Sign Mining Pact as Modi Targets $20 Billion Trade in Five Years," Reuters, February 21, 2026, https://www.reuters.com/world/americas/india-brazil-sign-mining-pact-modi-targets-20-billion-trade-five-years-2026-02-21. For the wider agenda of bilateral cooperation, including in defense and cybersecurity, see "India-Brazil Joint Statement: State Visit of President of Brazil to India," Indian Ministry of External Affairs, February 21, 2026, https://www.mea.gov.in/bilateral-documents.htm?dtl/40812.

44 Gladys Lechini, "Middle Powers: IBSA and the New South-South Cooperation," *NACLA Report on the Americas* 40, no. 5 (2007): 28–32, https://doi.org/10.1080/10714839.2007.11725377.

45 Oliver Stuenkel, *Post-Western World* (Cambridge: Polity, 2016), 5, 11.

46 Heena Makhija and Sandra Thachirickal Prathap, "Consensus Amid Contestation: Reading BRICS's New Delhi Declaration," Observer Research Foundation, September 16, 2026, https://www.orfonline.org/expert-speak/consensus-amid-contestation-reading-brics-s-new-delhi-declaration.

47 Sandra Thachirickal Prathap, "From BRICS@15 to BRICS@20: India's Chairship Ahead of the Summit," Observer Research Foundation, September 9, 2026, https://www.orfonline.org/expert-speak/from-brics-15-to-brics-20-india-s-chairmanship-ahead-of-the-summit.

48 Stuenkel, *Post-Western World*, 204–205.

49 Oliver Stuenkel, *The BRICS and the Future of Global Order*, 2nd edition (London: Rowman and Littlefield, 2020), 1–7.

50 Lisandra Paraguassu, "Growing BRICS Group Shows Internal Rifts as Ministers Fall Short of Joint Statement," Reuters, April 29, 2025, https://www.reuters.com/world/brics-ministers-fail-reach-joint-statement-brazil-warns-against-protectionism-2025-04-29/; and Stewart Patrick et al., "BRICS Expansion and the Future of World Order: Perspectives from Member States, Partners, and Aspirants," Carnegie Endowment for International Peace, March 31, 2025, https://carnegieendowment.org/research/2025/03/brics-expansion-and-the-future-of-world-order-perspectives-from-member-states-partners-and-aspirants?lang=en. More recently, see Makhija and Prathap, "Consensus Amid Contestation."

51 On India's pragmatic realism and calculations about its bilateral relationship with China, see Tellis, *India's Great-Power Delusions*. For the cybersecurity aspects of the New Delhi Declaration, see Indian Ministry of External Affairs, "BRICS New Delhi Declaration: Building for Resilience, Innovation, Cooperation and Sustainability," September 12, 2026, https://www.mea.gov.in/bilateral-documents?dtl/41776/BRICS_New_Delhi_Declaration_Building_for_Resilience_Innovation_Cooperation_and_Sustainability_September_12_2026.

52 Kyunghoon Kim, "Supply Chain Resilience: India's Case for Global South Leadership," Observer Research Foundation, September 11, 2026, https://www.orfonline.org/expert-speak/supply-chain-resilience-india-s-case-for-global-south-leadership.

53 For minilateralism and the Quad, see Nick Bisley, "The Quad, AUKUS and Australian Security Minilateralism: China's Rise and New Approaches to Security Cooperation," *Journal of Contemporary China* 34, no. 154 (2024): 564–576, https://doi.org/10.1080/10670564.2024.2365241. Though it is perhaps noteworthy that the Quad is yet to meet at leaders' level since Trump's second inauguration in 2025, after a series of such meetings during the Biden presidency.

54 Patrick Wintour, "South Africa and Malaysia to Launch Campaign to Protect International Justice," *The Guardian*, January 31, 2025, https://www.theguardian.com/law/2025/jan/31/south-africa-and-malaysia-to-launch-campaign-to-protect-justice.

55 Andre Barrinha and Arindrajit Basu, "Cyber Diplomacy and the Rise of the 'Global South,'" E-International Relations, June 10, 2025, https://www.e-ir.info/2025/06/10/cyber-diplomacy-and-the-rise-of-the-global-south/.

56 The latest iteration of UK national security strategy refers to the current moment as one of "radical uncertainty" in the international system. See Cabinet Office, "National Security Strategy: Security for the British People in a Dangerous World," UK Government, June 24, 2025, 4, https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world-html.

57 Clarity about the funding situation for capacity building is a significant topic for Global South cyber diplomacy. The early January 2026 U.S. withdrawal from the GFCE suggested, at a minimum, that the Trump administration intends to channel any remaining funding bilaterally. This is compounded by uncertainty about how cyber-related diplomacy will be affected by the concomitant workforce reductions planned by the U.S. Department of State and the UK Foreign Commonwealth and Development Office—of 15 and up to 25 percent, respectively. It is an open question whether, for example, a reduction in project funding and dedicated diplomatic effort by the like-minded states, would be met by China seeking an opportunity to fill this gap. For the prominence of capacity building as an element in the UK's cyber diplomacy, see Joe Devanny, "United Kingdom," in George Christou, Wilhelm Vosse, Joe Burton, and Joachim A. Koops (eds), *The Palgrave Handbook on Cyber Diplomacy* (London: Palgrave Macmillan, 2025), 435–452.

58 The first GGE in 2004 originally included a group of fifteen governmentally selected experts, including representatives of all five permanent members of the UN Security Council. Over the course of its six successive iterations, the GGE grew to twenty-five experts in its final iteration ending in 2021. For the history of the GGE process, see Heli Tiirmaa-Klaar, *The Evolution of the UN Group of Governmental Experts on Cyber Issues: From a Marginal Group to a Major International Security Norm-Setting Body* (The Hague: The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace, 2021), https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf.

59 Christian Ruhl, Duncan Hollis, Wyatt Hoffman, and Tim Maurer, "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads," Carnegie Endowment for International Peace, February 26, 2020, https://carnegieendowment.org/research/2020/02/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-a-crossroads.

60 For a good example of the diversity of global views on responsible cyber behavior and dissatisfaction with the disparities of influence in that discussion, see Louise Marie Hurel, *New Ways to Frame*

Responsible Cyber Behaviour Beyond the UN (London: Royal United Services Institute, 2025), https://static.rusi.org/new-ways-to-frame-rcb-beyond-un.pdf.

61 Michele Markoff, "The Origins of Cyber Diplomacy: Great Power Cyber Competition and Rapprochement in the United Nations 1998–2021," in Andrea Salvi, Heli Tiirmaa-Klaar, and James Andrew Lewis (eds.), *A Handbook for the Practice of Cyber Diplomacy* (Luxembourg: EU Institute for Security Studies, 2025), 45–57.

62 Joe Devanny, "Two (or Too Many) Cheers for UN Cyber Diplomacy," Carnegie Endowment for International Peace, July 29, 2025, https://carnegieendowment.org/posts/2025/07/un-cyber-diplomacy-oewg-successes-shortcomings?lang=en.

63 For the debate about stakeholder participation, see Pavlina Pavlova, "A Bridge Too Far? UN Dialogue on International Cybersecurity Undecided on Future Mechanism as Stakeholder Participation Hangs in Balance," EU Cyber Direct, May 26, 2025, https://eucyberdirect.eu/blog/a-bridge-too-far-un-dialogue-on-international-cybersecurity-undecided-on-future-mechanism-as-stakeholder-participation-hangs-in-balance.

64 The outcome of the final OEWG, proposing the Global Mechanism, was ultimately to fudge this issue: retaining states' veto of stakeholder participation, but with the provision of some form of process for such a veto to be, itself, vetoed by other states. For the proposed modalities of the Global Mechanism, see: "Draft Final Report," Open-ended working group on security of and in the use of information and communications technologies 2021-2025, July 11, 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_10_July_2025.pdf, 19–21.

65 "UN Global Mechanism on cybersecurity begins work with focus on participation and consensus," Digital Watch Observatory, July 21, 2026, https://dig.watch/updates/un-global-mechanism-cybersecurity-plenary-session.

66 Patryk Pawlak and Chris Painter, "Resetting Cyber Relations With the United States," Carnegie Endowment for International Peace, March 10, 2026, https://carnegieendowment.org/research/2026/03/resetting-cyber-relations-with-the-united-states.

67 "UN Global Mechanism on ICT Security Begins Building Global Capacity Architecture," Digital Watch Observatory, July 24, 2026, https://dig.watch/updates/global-mechanism-on-ict-security-eighth-meeting.

68 For an excellent insider's account of the history of UN cyber diplomacy, see Michele Markoff, "The Origins of Cyber Diplomacy: Great Power Cyber Competition and Rapprochement in the United Nations 1998– 2021," in Andrea Salvi, Heli Tiirmaa-Klaar, and James Andrew Lewis (eds.), *A Handbook for the Practice of Cyber Diplomacy* (Luxembourg: EU Institute for Security Studies, 2025), 45–57.

69 Pavlova, "A Bridge Too Far?"

70 Arun S. Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?," Lawfare, July 4, 2017, https://www.lawfaremedia.org/article/un-gge-failed-international-law-cyberspace-doomed-well; and Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone is Pleased," Council on Foreign Relations, 2018, https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased. The most recent agreement to establish a more permanent mechanism for multilateral dialogue about nonbinding cyber norms—due to meet for the first time in 2026—would surely feel like a hollow achievement if, as seems likely, the trend toward global cyber insecurity continues.

71 Pavlova, "A Bridge Too Far?"

72 Hurel, *New Ways to Frame Responsible Cyber Behaviour*.

73 For an upbeat assessment by an experienced practitioner of the situation of capacity-building within the current phase of multilateral cyber diplomacy, see Robert Collett, "The OEWG's Final Report and CCB," Cyber Capacity, July 11, 2025, https://cybercapacity.org/the-oewgs-final-report-and-ccb.

74 Bart Hogeveen, "The UN Norms of Responsible State Behaviour in Cyberspace: Guidance on Implementation for Member States of ASEAN," Australian Strategic Policy Institute, March 2022, https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.

75 The spectrum of malign or irresponsible behavior in this instance encompasses states that profit directly from cyber crime (such as North Korea), states that have an unclear but seemingly instrumental relationship with cybercriminals (such as Russia), and states that are de facto permissive of cyber crime but for reasons ranging from lack of capacity to corruption.

76 See two representative examples: Joanna Kulesza, "Breaking Ground: Historic Launch of UN Global Mechanism for Cyberspace Governance," *CircleID*, July 12, 2025, https://circleid.com/posts/breaking-ground-historic-launch-of-un-global-mechanism-for-cyberspace-governance; and Pavlina Pavlova, LinkedIn post, July 11, 2025, https://www.linkedin.com/posts/pavlpavlova_the-permanent-mechanism-for-international-activity-7349452935661031424-u9Yt.

77 Martha Finnemore, "Cultivating International Cyber Norms," in Kristin M. Lord and Travis Sharp (eds.), *America's Cyber Future Security and Prosperity in the Information Age,* volume II (Washington, D.C.: Center for New American Security, 2011), 90, https://www.files.ethz.ch/isn/129907/CNAS_Cyber_Volume%20II_2.pdf#page=89.

78 Patryk Pawlak, "Capacity Building in Cyberspace as an Instrument of Foreign Policy," *Global Policy* 7, no. 1 (2016): 83–92; Zine Homburger, "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace," *Global Society* 33, no. 2 (2019): 224–242; and Nayia Barmpaliou and Patryk Pawlak, *Between Ambition and Pragmatism: The Future of Cyber Capacity-Building in a Fragmented World* (Paris: EU Institute for Security Studies, 2025), https://www.iss.europa.eu/sites/default/files/2025-02/The%20future_of_cyber%20capacity_building_0.pdf.

79 Robert Collett and Nayia Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios," EU

Institute for Security Studies, 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf.

80 Chris Painter, "U.S. Withdrawal from International Cyber Organizations Weakens Global Cooperation Against Cyber Threats," Just Security, February 9, 2026, https://www.justsecurity.org/129944/us-withdrawal-cyber-organizations.

81 Stuenkel, *Post-Western World*, 113.

82 Devanny and Bucha, "Brazil's Cyber Strategy Under Lula," 11; and Ruhl, Hollis, Hoffman, and Maurer, "Cyberspace and Geopolitics," 4.

83 Robert Collett, "Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures," *Journal of Cyber Policy* 6, no. 3 (2021): 308–309, https://doi.org/10.1080/23738871.2021.1948582.

84 Mohamed Helal, "The Common African Position on the Application of International Law in Cyberspace: Reflections on a Collaborative Lawmaking Process," EJIL:Talk!, February 5, 2024, https://www.ejiltalk.org/the-common-african-position-on-the-application-of-international-law-in-cyberspace-reflections-on-a-collaborative-lawmaking-process.

85 On South African foreign policy principles, see Ronald Lamola, "Address by DIRCO Minister Ronald Lamola on SA's Foreign Policy," South African Institute of International Affairs, July 12, 2024, https://saiia.org.za/research/address-by-dirco-minister-ronald-lamola-on-sas-foreign-policy. On capacity-building support to the African Union, see Helal, "The Common African Position."

86 See Devanny and Buchan, "Brazil's Cyber Strategy Under Lula"; Devanny and Buchan, "South Africa's Cyber Strategy Under Ramaphosa"; and Devanny and Laudrain, "Interpreting India's Cyber Statecraft."

87 On the need to pursue AI diplomacy and cyber diplomacy in tandem, see Joe Devanny, *Artificial Intelligence and Cyber Power* (Miami: Jack D. Gordon Institute for Public Policy, Florida International University, 2024), https://digitalcommons.fiu.edu/jgi_research/63.

88 Arindrajit Basu and Karthik Nachiappan, "Will India Negotiate in Cyberspace?," in Fabio

Cristiano and Bibi van den Berg (eds), *Hybridity, Conflict and the Global Politics of Cybersecurity*

(Rowman and Littlefield, 2023), 189–210.

89 For an expansion of this analysis of India's approach to cyber diplomacy, see Devanny and Laudrain, "Interpreting India's Cyber Statecraft," 22–23.

90 On India's experience of state actor cyber threats, see Devanny and Laudrain, "Interpreting India's Cyber Statecraft," 11–12. On Indian and Pakistani cyber activities surrounding Operation Sindoor in May 2025, see Sameer Patil, "Operation Sindoor and India-Pakistan's Escalated Rivalry in Cyberspace," RUSI, June 20, 2025, https://www.rusi.org/explore-our-research/publications/commentary/operation-sindoor-and-india-pakistans-escalated-rivalry-cyberspace.

91 Devanny and Laudrain, "Interpreting India's Cyber Statecraft," 15–17.

92 Devanny and Buchan, "South Africa's Cyber Strategy Under Ramaphosa," 8.

93 Devanny and Buchan, "Brazil's Cyber Strategy Under Lula," 6.

94 As Max Smeets notes, all national cyber commands are not equal. There are more actors, but a significant variation in the nature of the activities being pursued by these different actors. See Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London: Hurst, 2022).

95 For the rising influence of the FCDO on UK cyber statecraft, see Devanny and Dwyer, "From Cyber Security to Cyber Power." For the Biden administration's international cyber strategy, see U.S. Department of State, "United States International Cyberspace and Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future," 2024, https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf.

96 Joe Devanny, "The U.K.'s Cybersecurity Refresh," Lawfare, December 22, 2025, https://www.lawfaremedia.org/article/the-u.k.-s-cybersecurity-refresh; Eric Geller, "State Department Reorganization Could Imperil Cyber Diplomacy," *Cybersecurity Dive*, April 23, 2025, https://www.cybersecuritydive.com/news/state-department-reorganization-could-imperil-cyber-diplomacy/746137/; Jennifer Hansler, Kylie Atwood, and Sean Lyngaas, "Rubio Lays Out Detailed Plan to Restructure State Department to Focus on Trump's Priorities," CNN, May 29, 2025, https://edition.cnn.com/2025/05/29/politics/rubio-lays-out-detailed-plan-to-restructure-state-department-to-focus-on-trumps-priorities; George Parker, "Foreign Office Staff in London Face Major Cull," *Financial Times*, May 25, 2025, https://www.ft.com/content/9bac6ef9-4f6d-41b3-92ec-2a6b235a1722; Lena Cohrs, "The Comprehensive Spending Review – A Disappointing Conclusion for UK ODA After Months of Speculation," *BOND International*, June 12, 2025, https://www.bond.org.uk/news/2025/06/the-comprehensive-spending-review-a-disappointing-conclusion-for-uk-oda-after-months-of-speculation/; and Olivia O'Sullivan and Jerome Puri, "First USAID Closes, Then UK Cuts Aid: What a Western Retreat From Foreign Aid Could Mean," Chatham House, April 16, 2025, https://www.chathamhouse.org/2025/03/first-usaid-closes-then-uk-cuts-aid-what-western-retreat-foreign-aid-could-mean.

97 For a comparative analysis of how a foreign ministry is shaped by its size and national priorities, see Jorge A. Schiavon and Bruno Figueroa, "Foreign Policy Capacities, State Foreign Services, and International Influence: Brazil Versus Mexico," *Diplomacy & Statecraft* 30, no. 4 (2019): 816–828, https://doi.org/10.1080/09592296.2019.1673560.

98 It is worth clarifying that aspects of digital policy are indeed politically contested, such as efforts by states or the European Union to control the operations of global social media platforms. This has led to significant trans-Atlantic tension. For like-minded states, however, domestic digital issues are generally treated as separate from the narrower domain of cyber diplomacy. For Russia and China, animated by a more totalizing conception of cyber or information sovereignty, these issues run together.

99 Eugenia Lostri and Georgia Wood, "The Role of International Assistance in Cyber Incident Response." *Lawfare*, March 30, 2023, https:// www.lawfaremedia.org/article/role-international-assistance-cyber-incident-response; Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security 4(2)*, 2011, pp.49-60, DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3.

100 For a reflection on this issue from a UK political perspective, see Alexander Martin, "UK Election Campaigns Ignore London Hospitals Cyberattack Despite Disruption," *The Record* (blog), Recorded Future News, June 7, 2024, https://therecord.media/uk-election-campaigns-ignore-london-attacks. A more recent example from Brazil is the July 2025 cyber crime targeting financial institutions and whether this might galvanize political leadership to drive forward with cybersecurity reforms. See Pedro Santos Teixeira, "Polícia de São Paulo prende suspeito de participar de ataque hacker a empresa que opera Pix," Folha de São Paulo, July 4, 2025, https://www1.folha.uol.com.br/tec/2025/07/policia-de-sao-paulo-prende-suspeito-de-participar-de-ataque-hacker-a-empresa-que-opera-pix.shtml.

101 Devanny and Buchan, "Brazil's Cyber Strategy Under Lula," 5–6.

102 See Devanny, "Cyber Threats in Latin America."

103 Monica de Bolle, "Brazil's Economic Impasse: Neither Lula nor Bolsonaro Can Solve the Country's Problems," *Foreign Affairs*, October 22, 2026, https://www.foreignaffairs.com/brazil/brazils-economic-impasse; Americas Quarterly, "REACTION: Lula Wins Brazil's Presidency in Historic Comeback," October 26, 2026, https://americasquarterly.org/article/reaction-lula-wins-brazils-presidency-in-historic-comeback/.

104 Devanny and Buchan, "Brazil's Cyber Strategy Under Lula," 2–3. This interpretation has been affirmed more recently in discussions between the authors and Brazilian officials.

105 Tom Phillips, "New Charges Accuse Bolsonaro of Running Spy Ring From Brazil's Presidential Palace, *The Guardian*, June 17, 2025, https://www.theguardian.com/world/2025/jun/17/bolsonaro-spy-ring-brazil.

106 Alexander Martin, "As Spyware Market Continues to Expand, Diplomatic Pall Mall Process Hits a Pivot Point," *The Record* (blog), Recorded Future News, April 9, 2025, https://therecord.media/pall-mall-process-commercial-spyware-hacking-paris-diplomacy.

107 Communication between authors and Brazilian practitioners, July 2025.

108 Devanny and Buchan, "Brazil's Cyber Strategy Under Lula," 7–8; and Patricia Campos Mello, "Big techs terão regime mais duro, ditado pelo STF, após lobby pesado contra leis no Congresso," *Folha de São Paulo*, June 26, 2025, https://www1.folha.uol.com.br/poder/2025/06/big-techs-terao-regime-mais-duro-ditado-pelo-stf-apos-lobby-pesado-contra-leis-no-congresso.shtml.

109 Daniel Buarque, "Upside-Down Diplomacy – Foreign Perceptions About Bolsonaro's Intentions and Initial Transformations of Brazil's Foreign Policy and Status," *Third World Quarterly* 43, no. 10 (2022): 2,450–2,466, https://doi.org/10.1080/01436597.2022.2098103; and Vinicius Guilherme Rodrigues Vieira, "Embedded Nationalism in a Fragmented World: Lula's Brazil," *Washington Quarterly* 46, no. 1 (2023): 45–60, https://doi.org/10.1080/0163660X.2023.2192136.

110 Fernanda Magnotta, "Trump and Lula Think Differently. Will They Find Common Ground?," *Americas Quarterly*, January 22, 2025, https://www.americasquarterly.org/article/trump-and-lula-think-differently-will-they-find-common-ground/; Oliver Stuenkel, "The Risks—and One Major Opportunity—Trump Presents to Brazil," Carnegie Endowment for International Peace, April 28, 2025, https://carnegieendowment.org/emissary/2025/04/brazil-trump-risks-opportunities-brics-trade?lang=en; and Tom Phillips, "Brazil's President Seeks 'Indestructible' Links With China Amid Trump Trade War," *The Guardian*, May 12, 2025, https://www.theguardian.com/world/2025/may/12/brazil-china-trade-lula-da-silva-trump.

111 Ari Hawkins, Eric Basal-Eimil, Daniel Desrochers, and Megan Messerly, "Trump Threatens to Slap Brazil With 50 Percent Tariffs Over Treatment of Bolsonaro, Other Disagreements," *Politico*, July 9, 2025, https://www.politico.com/news/2025/07/09/trump-threatens-to-slap-brazil-with-50-percent-tariffs-over-treatment-of-bolsonaro-other-disagreements-00445401.

112 Megan Messerly, Ari Hawkins, and Eric Bazail-Eimil, "'The President Is Pissed': Trump's Brazil Tariff Threat Is Part of a Bigger Geopolitical Dispute," *Politico*, July 10, 2025, https://www.politico.com/news/2025/07/10/trumps-brics-fueled-anger-sparked-50-percent-tariff-threat-on-brazil-00447814.

113 For the public opinion context of this episode, specifically preexisting skepticism about the United States, see Gustavo Ribeiro, "Lula's Got Mail," *Brazilian Report*, July 10, 2025, https://newsletters.brazilian.report/p/lula-trump-tariffs-bolsonaro.

114 Marianna Holanda, Thaisa Oliveira, and Raphael Di Cunto, "Bolsonaristas admitem desgaste com tarifa de Trump, buscam blindar ex-presidente e culpam Lula," *Folha de São Paulo*, July 10, 2025, https://www1.folha.uol.com.br/poder/2025/07/bolsonaristas-admitem-desgaste-com-tarifa-de-trump-buscam-blindar-ex-presidente-e-culpam-lula.shtml; Juliana Arreguy, "Vice de Tarcísio diz que estratégia de Trump é equivocada na forma e na execução," *Folha de São Paulo*, July 9, 2025, https://www1.folha.uol.com.br/poder/2025/07/vice-de-tarcisio-diz-que-estrategia-de-trump-e-equivocada-na-forma-e-na-execucao.shtml; and "Agressão de Trump dificulta equilibrismo na direita," *Folha de São Paulo*, July 11, 2025, https://www1.folha.uol.com.br/opiniao/2025/07/agressao-de-trump-dificulta-equilibrismo-na-direita.shtml.

115 Joao Gabriel and Raphael Di Cunto, "Camara resiste a pressão bolsonarista por anistia em troca do fim do tarifaco," *Folha de São Paulo*, July 14, 2025, https://www1.folha.uol.com.br/poder/2025/07/camara-resiste-a-pressao-bolsonarista-por-anistia-em-troca-do-fim-do-tarifaco.shtml.

116 Catia Seabra and Raphael Di Cunto, "Lula cria comite para avaliar sobretaxa de Trump e conversara pessoalmente com empresários," *Folha de São Paulo*, July 13, 2025, https://www1.folha.uol.com.br/mercado/2025/07/lula-cria-comite-para-avaliar-sobretaxa-de-trump-e-conversara-pessoalmente-com-empresarios.shtml; Julia Chaib, "Tarifas são sobre Bolsonaro, mas governo não deve ceder integridade institucional, diz ex-embaixador," *Folha de São Paulo*, July 14, 2025, https://www1.folha.uol.com.br/mercado/2025/07/tarifas-sao-sobre-bolsonaro-mas-governo-nao-deve-ceder-integridade-institucional-diz-ex-embaixador.shtml; and Mary Anastasia O'Grady, "Trump's Brazilian Trade War," *Wall Street Journal*, July 13, 2025, https://www.wsj.com/opinion/trumps-brazilian-trade-war-trial-tariffs-south-america-eb4f2203.

117 Gabriela Piva, "Intervenção dos EUA na Venezuela quebra confiança regional, diz Amorim," CNN Brasil, January 26, 2026, https://www.cnnbrasil.com.br/politica/intervencao-dos-eua-na-venezuela-quebra-confianca-regional-diz-amorim.

118 Alberto Maresca, *Brazil's foreign policy at a crossroads*. Heinrich Boll Stiftung, September 29, 2026, https://eu.boell.org/en/2026/09/29/brazils-foreign-policy-crossroads; Catherine Osborn, "How Flávio Bolsonaro Sees the World," *Foreign Policy*, September 21, 2026, https://foreignpolicy.com/2026/09/21/brazil-presidential-election-lula-bolsonaro-china-us-trump/; Tings Chak, "How Brazil's Election Could Reshape Relations with China," *CounterPunch*, October 14, 2026, https://www.counterpunch.org/2026/10/14/how-brazils-election-could-reshape-relations-with-china/.

119 Jose Marques, "Flávio Bolsonaro usou passaporte italiano para entrar na Argentina e não passou por posto de controle brasileiro," *Folha de São Paulo*, October 28, 2026, https://www1.folha.uol.com.br/poder/2026/10/flavio-bolsonaro-usou-passaporte-italiano-para-entrar-na-argentina-e-nao-passou-por-posto-de-controle-brasileiro.shtml; Oliver Griffin and Eduardo Simões, "Trump says Brazil election looked 'rigged,' defeated Bolsonaro's party recognizes Lula win," *Reuters*, October 26, 2026, https://www.reuters.com/world/americas/brazil-heads-back-future-flavio-bolsonaro-refuses-recognize-lula-win-2026-10-26/.

120 Joe Devanny, "Cyber Threats in Latin America," *CEBRI Journal 5(17)*, June 17, 2026, pp.49-50, https://cebri-revista.emnuvens.com.br/revista/article/view/305/514; Octavio Amorim Neto, "Cabinets and Coalitional Presidentialism," in Barry Ames (ed.). *Routledge Handbook of Brazilian Politics* (Abingdon: Routledge, 2019) pp.293-312; André Singer, "Lulismo 3.0: A Mid-Term Diagnosis," *New Left Review II/150*, November–December, 2024, pp. 39–54.

121 Devanny and Laudrain, "Interpreting India's Cyber Statecraft," 17–20.

122 Devanny and Laudrain, "Interpreting India's Cyber Statecraft," 7–9. This view was echoed in a series of conversations between the authors and former Indian officials between October and December 2024.

123 Devanny and Laudrain, "Interpreting India's Cyber Statecraft," 10.

124 Devanny and Laudrain, "Interpreting India's Cyber Statecraft," 5, 19–20.

125 Shantanu Roy-Choudhury, "The Indispensable Adversary: India's Approach to China," War on the Rocks, December 29, 2025, https://warontherocks.com/2025/12/the-indispensable-adversary-indias-approach-to-china; and Nikunj Ohri and Sarina Chaganti Singh, "India Eases Curbs on Chinese Equipment Imports for Power, Coal as Projects Delayed, Sources Say," Reuters, February 18, 2026, https://www.reuters.com/sustainability/climate-energy/india-eases-curbs-chinese-equipment-imports-power-coal-projects-delayed-sources-2026-02-18.

126 Rishi Gupta, "Caution and Calculus: How India Sees China in 2026," Think China, January 20, 2026, https://www.thinkchina.sg/politics/caution-and-calculus-how-india-sees-china-2026. For the connection between the 2025 so-called thaw in China-India relations and the Trump administration, see Ivan Lidarev, "China-India Relations in 2026: Can the Thaw Continue?" *The Diplomat*, January 2, 2026, https://thediplomat.com/2026/01/china-india-relations-in-2026-can-the-thaw-continue.

127 Michael Kugelman and Srujan Palkar, "Dispatch From New Delhi: Another India-China Flare-Up Is Coming," Atlantic

Council, December 10, 2025, https://www.atlanticcouncil.org/dispatches/dispatch-from-new-delhi-another-india-china-flare-up-is-coming.

128 Shanthie Mariet D'Souza explored the role of India-Taiwan relations in this context. See Shanthie Mariet D'Souza, "Leveraging Taiwan: India's Strategic Counterbalance to China," *The Interpreter*, December 16, 2025, https://www.lowyinstitute.org/the-interpreter/leveraging-taiwan-india-s-strategic-counterbalance-china.

129 Nidhi Verma, "Russian Share of India's January Oil Imports Lowest Since Late 2022, Data Shows," Reuters, February 18, 2026, https://www.reuters.com/business/energy/russian-share-indias-january-oil-imports-lowest-since-late-2022-data-shows-2026-02-18.

130 "UN Global Mechanism on ICT Security Begins Building Global Capacity Architecture," Digital Watch Observatory. For a wider consideration of India's cyber statecraft, see Devanny and Laudrain, "Interpreting India's Cyber Statecraft."

131 Buchan and Devanny, "South Africa's Cyber Strategy Under Ramaphosa."

132 Alex Vines, "South Africa's New Coalition Government Heralds Change for the Region and Its Leaders," Chatham House, June 21, 2024, https://www.chathamhouse.org/2024/06/south-africas-new-coalition-government-heralds-change-region-and-its-leaders.

133 Federica Marsi, "What 'catastrophic' South Africa local election results mean for ANC," *Al Jazeera*, November 9, 2026, https://www.aljazeera.com/news/2026/11/9/what-catastrophic-south-africa-local-election-results-mean-for-anc.

134 Ferial Haffajee, "SACP's strong showing signals end of the Tripartite Alliance," *Daily Maverick*, November 8, 2026, https://www.dailymaverick.co.za/article/2026-11-08-sacps-strong-showing-signals-end-of-the-tripartite-alliance.

135 Collette Schulz-Herzenberg and Roger Southall (eds.), *Election 2024, South Africa: Countdown to Coalition* (Johannesburg: Jacana, 2024).

136 Clive Coetzee, "The Depth and Breadth of the Defunding of the SANDF," DefenceWeb, May 16, 2025, https://www.defenceweb.co.za/featured/the-depth-and-breadth-of-the-defunding-of-the-sandf; Helmoed Romer Heitman, "South Africa's Declining Military Capability," *The Round Table*, 2025, 1–3, https://doi.org/10.1080/00358533.2025.2514775; and Kevin Gopaul, Elma van der Lingen, and Rudolph Oosthuizen, "The South African Defence Industry: A Contemporary Comparative Analysis of Its Second Tier Nature," *African Security Review* 34, no. 2 (2024): 168–187, https://doi.org/10.1080/10246029.2024.2429392.

137 For early ANC government economic policies, see 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). For a longer view of the problems that the ANC governments faced, see 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/research/2021/03/south-africa-when-strong-institutions-and-massive-inequalities-collide?lang=en. For wider political context on the ANC in government, see Richard Calland and Mabel Sithole, *The Presidents: From Mandela to Ramaphosa, Leadership in the Age of Crisis* (Johannesburg: Penguin South Africa, 2022); and Evan Lieberman, *Until We Have Won Our Liberty: South Africa After Apartheid* (Princeton, NJ: Princeton University Press, 2022).

138 "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.

139 Hinako Sugiyama, "In This Era of Spyware, Parliament Must Codify Safeguards in Surveillance Law," *Daily Maverick*, June 2, 2025, https://www.dailymaverick.co.za/article/2025-06-02-in-this-era-of-spyware-parliament-must-codify-safeguards-in-surveillance-law/; Heidi Swart, "The Two Surveillance Bills Before Parliament That Should Give Every South African Pause for Thought," IntelWatch, October 3, 2023, https://intelwatch.org.za/2023/10/03/op-ed-the-two-surveillance-bills-before-parliament-that-should-give-every-south-african-pause-for-thought; and Freedom House, "South Africa Key Developments, June 1, 2023 - May 31, 2024," in *Freedom on the Net 2024*, 2024, https://freedomhouse.org/country/south-africa/freedom-net/2024.

140 Luca Belli and Min Jiang, "Digital Sovereignty in the BRICS: Structuring Self-Determination, Cybersecurity, and Control," in Min Jiang and Luca Belli (eds.), *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance* (Cambridge: Cambridge University Press, 2024), 18. As Belli and Jiang note, the expansion of BRICS makes the potential shaping impact of BRICS cyber cooperation even greater—comprising more than 40 percent of the world's population and a growing number of its internet users—but, at the same time, likely makes it harder to reach consensus positions.

141 Kanishka Singh and Bhargav Acharya, "Rubio Announces US Visa Curbs for Some Foreign Nationals From South Africa," Reuters, September 15, 2026, https://www.reuters.com/world/africa/us-announces-visa-curbs-some-foreign-nationals-south-africa-2026-09-15; and Michelle Gavin, "Who Is Really in Charge in South Africa?," Council on Foreign Relations, January 26, 2026, https://www.cfr.org/articles/who-is-really-in-charge-in-south-africa.

142 Adwoa Tenkoramaa Ramena, "South Africa Hunts for New Markets as US Tariffs Bite," Deutsche Welle, February 17, 2026, https://www.dw.com/en/south-africa-hunts-for-new-markets-as-us-tariffs-bite/a-75991451; and Sam Mkokeli and Yinka Adegoke, "Relief, but No Reset: South Africa Recalibrates After US Tariff Ruling," Semafor, February 23, 2026, https://www.semafor.com/article/02/23/2026/relief-but-no-reset-south-africa-recalibrates-after-us-tariff-ruling.

143 Chris Alden and Maxi Schoeman, "Being Africa's BRIC(S): South Africa's Foreign Policy Turn From 'Neo-Liberalism' to the 'New Era,'" *South African Journal of International Affairs* 32, no. 1–2 (2025): 71–90, https://doi.org/10.1080/10220461.2025.2503212.

144 Jeremy Fleming, "Director GCHQ's Speech on Global Security Amid War in Ukraine," GCHQ, March 31, 2022, https://www.gchq.gov.uk/speech/director-gchq-global-security-amid-russia-invasion-of-ukraine.

145 For recent developments in China's wider statecraft approach to Latin America, see Leland Lazarus, "How China Is Seeking Dominance in Latin America," *Americas Quarterly*, June 10, 2025, https://www.americasquarterly.org/article/how-china-is-seeking-dominance-in-latin-america; and "AQ Podcast | BRICS and China's Influence in Latin America," *Americas Quarterly*, June 26, 2025, https://www.americasquarterly.org/article/aq-podcast-brics-and-chinas-influence-in-latin-america.



CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW
Washington, DC 20036
CarnegieEndowment.org