CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

AUGUST 2023

Brazil's Cyber Strategy Under Lula: Not a Priority, but Progress Is Possible

Joe Devanny and Russell Buchan

Brazil's Cyber Strategy Under Lula: Not a Priority, but Progress Is Possible

Joe Devanny and Russell Buchan

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

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

Contents

Introduction

Since coming to office in January 2023, Brazilian President Luiz Inácio Lula da Silva (more commonly known as Lula) and his administration have not treated cyber strategy as a top political priority. So far, no single institution or senior figure in the administration has played a decisive role in driving forward a comprehensive cyber strategy. The administration seems to have settled into a pattern of relative continuity with its predecessors. Its approach to cyber diplomacy continues to mirror Brazil's established approach, and the administration is unlikely to try to challenge the significant role of the country's military in cyber defense.

Overall, progress in improving Brazil's cyber strategy is likely to be slow. In April, the Lula administration passed the mark of one hundred days in office, and it is now over halfway through its first year, so it is still in a relatively early phase of governing.[1] The administration does not appear to prioritize wider cyber strategy politically, but it released an ambitious consultation paper in May to stimulate discussion about reforming domestic cybersecurity governance.[2] This blueprint needs further refinement, but the real test of the administration's commitment will be how it approaches the process of securing congressional and wider approval and, if it achieves this, whether it devotes sufficient resources and political backing to the blueprint. Of greater political significance to the administration is countering online disinformation and extremism. This will be a domestic and foreign policy priority—as such, it is likely to be a productive issue for bilateral engagement.

The Armed Forces, Politics, and Brazil's Cyber Strategy

Like many countries, Brazil started to develop aspects of a national cyber defense strategy in the 2000s. Its 2008 National Defence Strategy identified cyber as one of three strategic priorities, alongside nuclear and space. The early 2010s saw the institutional development of cyber defense, leading to its first national cyber defense doctrine in 2014 and a joint operational command in 2016. These developments occurred during two Workers' Party (*Partido dos Trabalhadores*, or PT) presidencies: those of Lula and his successor, Dilma Rousseff. They were driven by the threat of cyber attacks against the 2014 FIFA World Cup and the 2016 Olympic Games, both hosted by Brazil.

These developments should not be interpreted as a deliberate political prioritization by the Workers' Party of the military aspects of cyber strategy at the expense of the civilian aspects. They rather reflect the broader facts that defense investment increased during Lula's first two terms and that, like in other countries over the last fifteen years, the Brazilian military began to intensify cyber defense structural reforms and capability development.[3]

The Armed Forces' Role in Cyber Defense

Tracking with its status as a leading regional actor, Brazil's cyber defense capabilities are generally considered among the best in Latin America, even though they are not as sophisticated as the capabilities of many Western states or as well organized as Chile's, its neighbor.[4] Brazil has used its expertise collaboratively by providing, for example, cyber defense assistance to neighboring states during major regional events. However, the administration of former president Jair Bolsonaro did not prioritize regional leadership. Moreover, Brazil's relative strength compared with neighboring states is belied by the reality that Brazil faces significant challenges in addressing cyber threats, particularly cyber crime. In recent years, threats have escalated from cyber crimes to cyber attacks against critical national infrastructure. In 2020, for example, Brazil's Superior Court of Justice fell victim to a massive ransomware attack,[5] and in 2021, a cyber attack was launched against the COVID-19 pass app Conect SUS.[6]

One significant shortcoming highlighted by these incidents is the immaturity of the Brazilian institutions that should govern a national cyber defense strategy.[7] There is also a lack of clarity and complementarity between its cybersecurity and cyber defense efforts. This raises questions about how the Armed Forces should contribute to Brazil's cyber strategy.

Managing civil-military relations has been a long-running challenge for the executive since Brazil returned to democracy following the 1964–1985 period of military rule. While Article 142 of Brazil's constitution grants the president "supreme authority" over the Armed

Forces,[8] the military maintains significant influence in the governance of national defense. This influence persists despite the creation of a civilian Defense Ministry in 1999, which replaced the single-service ministries. The military therefore enjoys entrenched privileges and a preeminent position vis-à-vis civilians in the defense establishment, including for the country's cyber defense strategy.[9]

This has been evident in several episodes in the past five years. In 2018, then commander of the Brazilian Army General Eduardo Villas Boas tweeted remarks widely seen as hostile to Lula on the eve of a Supreme Court decision that ultimately exhausted Lula's appeals against his criminal conviction.[10] There was speculation before the 2022 presidential election about whether the Armed Forces would be complicit in any effort to steal the election and prevent Lula from taking office.[11] The military has also been criticized for its response to the January 8, 2023, political unrest in Brasília, including the invasion and vandalization of government buildings by pro-Bolsonaro protesters. In the wake of the unrest in Brasília, Lula replaced the commander of the Brazilian Army in what was widely seen as an effort to publicly reassert his control of the military.[12] The appointment of a new army chief (General Tomás Ribeiro Paiva) precipitated the usual round of moves, retirements, and promotions during the first half of 2023. Current indications are that these senior personnel decisions conformed to the army's natural order of promotion, rather than a more politicized clear out.[13] Early reporting indicates that Tomás intends to improve the army's image as an "apolitical" and "nonpartisan" institution.[14] While it is unclear if the administration will succeed in legislating to constrain the political activities of active-duty personnel, it does seem clear that the leadership of the Armed Forces is collectively keen to neutralize this potential issue of tension with Lula.[15] In this context, it is very difficult to see cyber strategy becoming a point of contention between the presidency and the Armed Forces.

The Role of the Institutional Security Cabinet and Other Institutions

In addition to the army, navy, and air force, another significant actor in Brazil's cyber strategy is the Institutional Security Cabinet (GSI), an institution long associated with and populated by the Armed Forces.[16] The GSI advises the president on security and military affairs, including civilian aspects of cybersecurity and cyber defense. The GSI proposes guidelines and strategies for cybersecurity through the Department of Information and Communication Security. Since 2018, the GSI has been expected to bring forward a new national cyber policy, which to the GSI's considerable credit, particularly given the intra-institutional turmoil generated by the presidential transition, has finally been proposed under Lula's government.

Under Bolsonaro, the GSI was led by retired general Augusto Heleno, and many of its posts including the top cyber portfolio were filled by retired and active-duty military officers. Some of these military personnel deployed in the GSI have reportedly been implicated in supporting the January 8 protesters in Brasília.[17] Lula reportedly removed most of the military personnel detailed to the GSI under Bolsonaro. Notably, however, Lula initially

replaced Heleno with another retired general, Marcos Edson Gonçalves Dias, with whom he had worked closely in the past.[18] In April, Gonçalves Dias was himself dismissed following the emergence of video footage of him in the presidential offices during the events on January 8. This reportedly renewed debate within the administration about whether to appoint a civilian to lead the GSI or to abolish the institution altogether. Having initially installed a civilian interim replacement, Lula quickly replaced Gonçalves Dias by formally appointing another retired army general, Marcos Antônio Amaro dos Santos.[19] Lula was ultimately persuaded to maintain the tradition of appointing a senior military officer, albeit to a GSI that is now reduced in size and remit following the events of January 8.[20]

The controversy surrounding the leadership of the GSI has not affected the administration's broader agenda for digital policies. These are managed out of civilian-led secretariats and departments, reflecting their greater political priority under the administration. The president's Social Communications Secretariat (Secom) will reportedly lead the coordination of the administration's efforts to counter disinformation and misinformation.[21] Another early decision with possible implications for cyber policy is the creation of a new management ministry under Esther Dweck, whose portfolio reportedly includes digital aspects of public service delivery and transformation.[22] Similarly, the Human Rights Ministry recently established a working group on countering disinformation and online extremism, indicating that the ministry and group will also be potential points of engagement on those salient issues.[23] It remains unclear how or if this busy institutional landscape will be actively coordinated and managed. The absence of coordination is a recipe for suboptimal outcomes.

It is too early to speculate on the ways in which changes in senior personnel and the distribution of policy responsibilities might change the overall balance between the institutional actors in Brazil's cyber strategy. The evidence suggests, however, that Lula perceives cyber strategy as less politically sensitive than responsibility for overseeing Brazil's Intelligence Agency (ABIN).[24] When Lula removed responsibility for ABIN from the GSI, he placed it under the Casa Civil, the powerful, cabinet-ranked presidential chief of staff who is a senior minister from Lula's Workers' Party.[25] He retained cybersecurity within the GSI's remit.[26] Although both the Casa Civil and the GSI are parts of the presidency, the move is a clear signal that Lula is placing ABIN more explicitly under civilian political control, while he is content for the more security-oriented institution, the GSI, to retain its cyber remit.[27] However, the removal of so many officials from the GSI is likely to reduce its short-term effectiveness as an institutional actor, compounded by Gonçalves Dias's departure in April. As previously mentioned, the GSI had been expected to bring forward a new national cyber policy. The appointment of cyber entrepreneur and scholar Marcelo Malagutti as its senior cyber adviser means that the GSI's cybersecurity portfolio has now been rejuvenated, just as its top leadership descended into controversy and rapid turnover.

New Proposals for Domestic Cyber Policy

Evidence of the GSI's renewed focus on cybersecurity emerged in May, when it published a consultation document for draft legislation to create a new national cybersecurity policy (PNCiber), including the creation of three new institutions: a national cybersecurity agency, a national cybersecurity committee, and a national management office of cyber crises. This document is the Lula administration's boldest, clearest, and most ambitious vision for reforming Brazil's approach to cybersecurity. It proposes a coherent system incorporating every level of government and embraces a networked approach involving government and the private sector. If anything, it is perhaps too ambitious.[28] It will require significant investment and leadership to meet the implementation targets, such as reforming the national cybersecurity profession and creating 800 new government cybersecurity jobs over five years. The draft is also somewhat vague about the boundaries between the new national agency and existing regulators, as it is about the boundaries between cybersecurity and cyber defense. The latter is a consequential blur, given the institutional lead of the Armed Forces in cyber defense.

The consultation draft has so far received a relatively positive, if somewhat guarded, welcome from other government departments, regulators, and nongovernment stakeholders, all of whom agreed that further progress is needed. They have emphasized that they need more time to reflect on the implications of the draft and contribute feedback and suggested revisions to the president.[29] The budget for the proposed agency is also a challenge to secure in the current fiscal and political context. The GSI's lead for cybersecurity, Malagutti, has injected considerable energy into the consultation and reportedly aims to achieve congressional approval to proceed by the end of 2023.[30] It is not clear that the domestic political ground has been prepared to ensure that such an ambitiously reformist draft becomes law. A long road lies ahead, and the National Congress will determine the draft law's fate.[31] The administration will need to spend political capital—and likely also make concessions—to persuade Congress to approve its plans. The outlook for the PNCiber is, therefore, extremely uncertain, notwithstanding energetic efforts from within the GSI to stimulate progress.

More generally, the GSI consultation draft emerged from an administration that appears to lack a senior political figure with a track record of treating cyber strategy as a top priority. This is not the most auspicious context for the consultation and its prospects of achieving congressional approval. Given the difficulties that will face the administration in getting its top, non-cyber priorities through the federal legislature, progress in the development and implementation of cyber strategy, such as that outlined in the GSI blueprint, is likely to be slow unless there is a strong prioritization of cyber and motivating leadership,.

This suggests an emerging answer to a wider question that was raised prior to the 2022 election: namely, whether a Lula administration will try to rebalance institutional governance of Brazil's cyber strategy, reducing the influence of the Armed Forces. At the level of cabinet and senior government appointments, Lula's administration will clearly not

have the same (uniformed) composition as Bolsonaro's. This does not necessarily—and, particularly in light of the early ABIN/GSI decision, probably will not—mean the Armed Forces will lose their ability to influence the aspects of cyber strategy about which they care most. Under Lula's previous presidential terms, the implicit bargain was that the Armed Forces were well funded and quiescent, with Lula not moving to significantly reform the defense sector. It will be harder for Lula to pursue that strategy with less money available than he had previously, but the Armed Forces will undoubtedly benefit from the resource allocation that is such an entrenched feature of Brazil's system of coalitional presidentialism.

Pragmatism and Political Context Shape Lula's Cyber Decisionmaking

Given his narrow margin of victory and the reality of the composition of Congress, Lula needs to lean into his reputation as a pragmatic, transactional negotiator. How Lula handles relations with the Armed Forces will be an important issue particularly for managing his administration's relationship with the more conservative elements of Brazilian society. There is evidence, for example, in Lula's picks of a career diplomat as foreign minister and in his choice of defense and communications ministers from beyond the Workers' Party, that his general approach to balancing his government will continue to be to avoid confrontation. Wherever possible, the administration will try to establish pragmatic working relationships with those parts of the state that are skeptical, if not outright opposed, to Lula's presidency specifically and more generally to the Workers' Party as a political actor.[32] (However, the fallout from the January 8 attacks on Brasília highlight that it will not always be possible to establish such relationships.) Cyber strategy is not yet a political hot potato or source of tension in civil-military relations, so in this difficult context, it is very unlikely that Lula will choose to spend political capital picking a fight about it. Ultimately, higher-priority political issues will determine the way that Lula's relationship with the Armed Forces unfolds during his current term in office. These higher-priority issues include how Lula handles the aftermath of the political violence in Brasília.[33] This is particularly the case if retired or serving military personnel (or their family members) are implicated and face prosecution.

None of these issues is directly about the Armed Forces' role in cyber strategy, but the broader political reality of tense civil-military relations will undoubtedly affect the context in which Brazil's cyber strategy—with its significant military component—is developed and implemented. The Lula administration is, for example, likely to be reluctant to press too hard to improve the institutional coordination of Brazil's cyber strategy, particularly between the Armed Forces (which prioritizes the development of sovereign cyber capabilities) and the Foreign Ministry (which articulates positions that imply a more defensive orientation toward cyberspace). If an issue does not affect Lula's political project, then his administration is likely to let the defense and security establishment do its own thing, up to a point. That said, it is frankly difficult to imagine Lula approving an offensive cyber operation during his presidency given his foreign policy views, Brazil's long-established national strategic outlook, and the likely maturity of Brazil's existing capabilities.

Social Media and Political Extremism in Brazil

The Lula administration has much greater strategic and domestic political interest in specific digital policy issues. This is particularly evident in the area of countering online disinformation, misinformation, and extremism, notably how social media platforms are used both to spread disinformation and as a wider tool by domestic extreme right-wing groups, political parties, and former president Bolsonaro himself.[34] This is a significant issue for the Lula administration's domestic policy agenda, which will be coordinated directly from the president's office.[35] It is also an issue that Lula has already raised in his foreign policy, for example during his February visit to Washington, DC. This is the most obvious and highest-profile example of a cyber-adjacent issue that aligns with the administration's political priorities.[36]

Social media is very popular in Brazil, and there has been an increasing focus in recent years on the role of social media platforms in political communication, particularly in misinformation, far-right radicalization, and domestic extremism.[37] Bolsonaro frequently used social media to disseminate his messages, building a following of over 1 million users on Telegram (a platform with over 50 million Brazilian users), 8 million on Twitter, and 14 million on Facebook. (His Facebook account ranked third in terms of followers among heads of state active on the platform.) Telegram was briefly banned in Brazil by the Supreme Court in early 2022 for failing to address the court's concerns over misinformation.[38] During his presidency, pro-Bolsonaro social media disinformation and misinformation campaigns were investigated by the Federal Police.[39] Ahead of the 2022 presidential elections, Brazil's electoral court secured a series of agreements with social media platforms to enhance corporate procedures to counter misinformation, but these were criticized for being insufficiently detailed and likely ineffective.[40] One nonprofit's investigation revealed apparent failure in Facebook's vetting of misinformation in political advertising. Meanwhile, the ability of another popular platform, Twitter, to counter the dissemination of violent and antidemocratic messages was reportedly undermined by the firing in November of its in-country content moderation team following the acquisition of the company by Elon Musk.[41]

The political impact of social media has been apparent both during the presidential election and since Lula's victory, especially during the January 8 protests.[42] On January 11, 2023, Supreme Court Justice Alexandre de Moraes ordered Telegram to suspend accounts associated with a federal legislator and other pro-Bolsonaro individuals who used social media to encourage criminal acts during the January 8 attacks. After Telegram failed to comply with the order, de Moraes issued a fine, which Telegram tried to contest.[43] Early indications suggest the Lula government intends to enhance its ability to take action regarding disinformation and misinformation propagated against the government and its policies.[44]

There are doubts, even within Lula's own party, that proposed internet regulation legislation will pass through Congress. These doubts have precipitated discussion of alternative plans.[45] The reported short-term priority is to reform legislation for digital election campaigns ahead of municipal elections in 2024. Proposals include prohibiting digital propaganda during the election period and reducing the time frame of deadlines for social media platforms to remove proscribed content, with even larger fines for failing to comply. Civil society members have criticized broader reforms because of doubts about their implications for maintaining the accountability of electoral candidates for material they post, as well as the impact of reforms on the power of the judicial elections regulator.[46] A further expedient is to use the Justice Department's national consumer secretariat (Senacon) as a tool to shape the behavior of social media platforms. This follows, rather than breaks with, a trend evident under the Bolsonaro government, during which Senacon initiated such proceedings against TikTok to remove content perceived as harmful to child safety.[47]

Overall, the experience of digital disinformation during the election galvanized the Lula administration to pursue a wide-ranging agenda to counter it. While the president is expected to coordinate counter-disinformation policies, the Human Rights Ministry also recently appointed its own working group of researchers and civil society campaigners to advise on measures to counter online disinformation and extremism.[48] The administration is making an early legislative push on countering fake news, but technical complexity, fraught politics, and even big philosophical questions about the balance between freedom and control lie ahead.[49] This is important context for understanding the domestic political priorities of the administration, the challenges it faces in producing legislation, and the sometimes tense relations between Brazil's government and multinational technology companies. Some companies, such as Google, have campaigned publicly against the government's regulatory proposals.[50] They have also hired prominent lobbyists to influence outcomes in Congress.[51] These debates in wider digital policy are occupying the Lula administration and represent direct, significant political priorities. From the perspective of political priorities, cybersecurity and cyber diplomacy are second-order problems.

Digital Freedom and Civil Society

An important area of global cyber diplomacy encompasses a competition between authoritarian and liberal democratic models for cyber governance. It is therefore worthwhile to explore the domestic reality in Brazil regarding the vitality of digital freedom, civil society, and democracy in the context of the constitution and government regulation. Brazil's constitution designates privacy, private life, honor, and the image of individuals as fundamental human rights. In 2014, Brazil adopted the Marco Civil, which was a landmark piece of legislation that some call the "Constitution of the Internet"[52] and that defines users' rights and responsibilities in cyberspace. Most importantly, this legislation provides explicit protection for digital rights. It requires that all internet users must respect net neutrality, a principle aimed at preserving the internet's open architecture, maintaining the user's power of choice, incentivizing innovation, and promoting freedom of competition. The legislation also protects the rights of internet access, freedom of expression, and privacy (by preventing

service providers from misusing users' information), among others.

More recently, Constitutional Amendment 115 (2022) identified data protection as a fundamental human right protected by the constitution. After many years of legislative discussions, the Brazilian General Data Protection Law (LGPD) was enacted in 2018 and came into force two years later. In developing the online protections set out in the Marco Civil, the LGPD is the most detailed and important data protection law in Brazil, regulating how personal data is collected, used, processed, and stored. The LGPD is inspired by and modeled on international guidelines, especially the provisions of the European Union's General Data Protection Regulation. Brazil's National Data Protection Authority plays a central role in structuring the country's data protection culture and is the regulatory authority responsible for supervising, regulating, and enforcing sanctions regarding all data processing activities in Brazil.

Freedom House rated Brazil as "partly free" in its 2021 Freedom of the Internet report, citing the tension between, on one hand, its efforts to improve internet access and its progressive legislation on digital freedom and rights and, on the other hand, the widespread problem of online misinformation and efforts under the Bolsonaro presidency to restrict the freedom of social media platforms and monitor and criminally investigate social media users.[53] But just as the Brazilian government has developed its capabilities to collect and access digital data, so too have civil society groups organized to promote digital freedom and privacy. This was particularly apparent during the Bolsonaro presidency, when several nonprofits coalesced to protest a perceived move toward "techno-authoritarianism" in the government's effort to collect and analyze citizens' data.[54] The Lula administration is expected to be more active and adept than the Bolsonaro administration in reaching out to civil society organizations on issues of digital freedoms and rights, but its agenda to counter online disinformation could bring it into disagreement with these same civil society groups if it leads to legislative efforts that could be perceived as restricting digital freedoms. It is clear from the administration's early communications on this issue that it understands this will be a delicate balance to strike in its legislative efforts to counter disinformation.[55] The administration has encountered problems in Congress, opposition from technology companies, and the inherent challenge of squaring its objective to increase government control with its commitment to safeguard the rights of users. Early evidence suggests the administration is pursuing a reactive approach, willing to change tack and pursue incremental gains while its more ambitious legislative plans flounder in Congress.[56]

Domestic Politics and Hacking

Under Joe Biden's administration, the United States has highlighted the global threat posed by the commercial spyware market. This has become a hot topic of cyber diplomacy and a target for coordinated action, for example under the auspices of the Biden administration's Summit for Democracy agenda.[57] The context for this development is a series of concerning reports about the global prevalence of spying software and its reported use in human rights

abuses.[58] Digital surveillance and hacking controversies are another example of the salience of cyber-related issues in Brazil's domestic politics. Recent years have seen the increasing use of hacking to derive insight into the activities of political rivals, and hacked material has been used to influence public narratives and political events.

As they have in many countries, "hack and leak" incidents have become more politically salient in Brazil. The most notable such case involved the 2019 compromise of a large number of Telegram accounts associated with political and legal officials.[59] The leak of this data to the Intercept Brasil was instrumental in the events that ultimately led to Lula's release from prison and his regaining of the political right to contest the 2022 presidential election.[60] More recently, a hacker sentenced for his role in the 2019 incident was reportedly implicated in a conspiracy associated with a pro-Bolsonaro federal legislator to hack the communications of a senior electoral judge.[61] This revelation adds to wider reporting of alleged plots to undermine or invalidate Lula's election victory.[62] The methods involved in these incidents and alleged plots—the compromise of social media accounts and cell phones—might seem novel, but the instrumental use of intercepted communications to influence political events has a longer history. For example, in 2016, then federal judge Sergio Moro released recordings of Lula's telephone conversations with Rousseff, leading to protests against Rousseff's presidency and specifically against an alleged (and ultimately unsuccessful) plan to help Lula avoid prosecution by appointing him to a position in Rousseff's presidential office.[63]

Brazil's Position in the Global Debate Over Cyber Governance

Two broad, opposing camps have emerged in the debate over cyber governance. In one camp, the group of so-called like-minded states—which are bound together by a mutual respect for democracy, human rights, and the rule of law[64]—look to maintain the existing multistakeholder structure of cyber governance based on openness, inclusion, collaboration, and consensual decisionmaking among private industry, international technical governance institutions, governments, and civil society.[65] This model pushes for a free and open cyberspace in which human rights are protected and governmental control is limited. In the other camp, China and Russia want to rewrite the rules on cyber governance and create a new structure that confers greater authority and control on national governments at the expense of other stakeholders.

Particularly under previous Workers' Party administrations, Brazil has championed the multistakeholder approach to cyber governance—for example, by convening the NetMundial conference in 2014 as an alternative to existing platforms for global internet

governance deliberations. This approach to cyber diplomacy aligns with broader currents in Brazil's foreign policy. Brazil has been a prominent advocate of protecting human rights online, working with Germany to successfully lobby the UN General Assembly to adopt a landmark resolution entitled "The Right to Privacy in the Digital Age."[66] Moreover, despite its initial reluctance to sign the 2001 Budapest Convention on Cybercrime on the basis that it is a Western project formulated without the involvement of the Global South, Brazil acceded to the convention in late 2022. That said, Brazil is reluctant to fully endorse the approach of like-minded (or Western) states. Brazil has cautiously cultivated closer cyber cooperation with China and Russia and supported some of their cyber initiatives, such as the idea of a universal international cyber treaty in 2012.[67] These initiatives are generally opposed by the like-minded states, who see them as attempts by China and Russia to secure greater government control over cyberspace and limit the enjoyment of fundamental human rights and the free flow of information.[68]

The reality is that Brazil does not position itself in one camp. Rather, it seeks to maintain an independent foreign policy by presenting itself as an influential "middle power" operating in the interstices of the two camps.[69] In particular, Brazil sees itself as leveraging soft power on the international stage and engaging in soft diplomacy. In this way, Brazil acts as a "broker" or "strategic bridge-builder" rather than a "swing state,"[70] doing so with the objective of "reaping the influencing-enhancing benefits that come with being an honest broker."[71] This broker role has led it to become an active player in multilateral and multistakeholder cyber diplomacy.[72] For example, Brazil has been a member of the UN Group of Governmental Experts (GGE) since the group's inception in 2003, and Brasília has participated in all sessions except for the one between 2012 and 2013. In fact, Brazilian Ambassadors chaired two sessions of the UN GGE; Carlos Luís Dantas Coutinho Perez chaired the 2013–2015 session and Guilherme de Aguiar Patriota chaired the 2019–2021 session.[73]

Notwithstanding its ambitions as an international playmaker, there has been variable momentum behind Brazil's foreign policy, depending to some extent on the foreign policy instincts and outlook of the president.[74] It is clear the Lula administration intends to reset Brazilian foreign policy, emphasizing its differences in key respects from the Bolsonaro government. That does not mean, however, that cyber diplomacy looms particularly large in the administration's priorities. The areas in which Lula's reset are more likely to be visible are reinvigorated regional leadership (for instance, by attending the Community of Latin American and Caribbean States summit meeting in January 2023);[75] environmental diplomacy; a greater focus on the Global South; and the tone (if not the substance) of Brazil's bilateral relations with China. Like other leaders in the region, Lula has cultivated a nonaligned position on the Russian invasion of Ukraine, upholding the principles of sovereignty and territorial integrity but minimizing direct criticism or isolation of Russia.[76] Notably, while Russia opposed, and the other BRICS countries (India, China, and South Africa) abstained in the recent UN General Assembly vote condemning the Russian invasion, Brazil voted in favor of condemnation.[77] In February 2023, Brazil again voted in favor of a resolution demanding that the "Russian Federation immediately, completely and unconditionally withdraw all of its military forces from the territory of Ukraine."[78]

Furthermore, critics disagree about the administration's potential to succeed in its ambition to reinvigorate BRICS. The fact that it is a stated goal reflects Lula's intention to establish pragmatic partnerships with these nations, not that he will align Brazil's position with BRICS states on all issues (as the UN vote demonstrates).[79]

None of this wider foreign policy context, however, implies a direct impact on the course of Brazilian cyber diplomacy. If the administration wished, Lula's wider foreign policy objectives could exert second-order impacts on Brazil's cyber diplomacy. For example, the administration could pursue its regional diplomacy by identifying cyber contributions to improved cooperation in Latin America. This could lead over time to a more constructive regional cyber role, but there is a lot of ground to make up. However, there is no evidence that Lula's administration perceives cybersecurity as being a worthy object of intensified regional cooperation. Moreover, the administration's wider regional diplomacy has encountered some difficulties.[80] Even more negatively, the administration's wider dynamics could be reflected in domestic cyber policy, for example, in bureaucratic stasis and policy drift potentially caused by delays in replacing many Bolsonaro appointees in key institutions of cyber policy, such as the GSI. It is not yet clear what—if any—impact this will have on the effectiveness of the GSI as an institutional actor in national cyber strategy. It deserves credit for producing its PNCiber consultation draft relatively swiftly, but the real challenges are securing approval and implementation.

In multilateral forums, Lula's commitment to reinvigorate BRICS will likely mean closer efforts than under Bolsonaro to coordinate diplomatic positions with other BRICS states. This is unlikely to result in substantial shifts in Brazil's foreign policy, regarding cyber or other issues.[81] It does, however, suggest that Lula's commitment to an active, independent, nonaligned global role for Brazil means the West should not take Brazil's support for granted. For example, members of the North Atlantic Treaty Organization (NATO) should continue to support the Brazilian Armed Forces' efforts to improve Brazil's status as a cyber partner, a partnership that gained momentum when Brazil accepted NATO's invitation to participate in its flagship cyber exercise, Locked Shields. The long-term goal for Brazil is to build its cyber defense capabilities and underlying ecosystem. Like-minded states are well-placed to support this ambition with offers of training and other assistance or collaboration. This would be a prudent, precautionary step, in the context of BRICS presenting a possible hypothetical alternative pole of alignment for Brazil's future cyber defense policies and capability development. It should be stressed that a Brazilian cyber tilt toward BRICS would represent a sharp divergence from the trajectory of its cyber defense strategy. There is no indication the Lula government wants to pursue such a move, still less to pick an unnecessary fight with the Armed Forces (which would not want to change its present orientation) in order to do so. Looking ahead, so long as Brazil perceives itself as benefiting from closer cyber alignment with NATO and its member states, there is unlikely to be such a shift, so it would be prudent for NATO to continue to nudge progress forward in cyber cooperation with Brazil.

Brazil's Views on International Cyber Norms

Brazil has actively contributed to the development of international cyber norms,[82] including helping shape the UN's eleven voluntary, nonbinding norms on responsible state behavior in cyberspace. Brazil has contributed to this process under various presidencies, including Bolsonaro's, and is likely to continue to do so under Lula, even though cybersecurity is not one of the administration's political priorities.

In terms of binding international law, Temple Law School Professor Duncan Hollis led an initiative in 2015 to develop a better understanding of how Organization of American States (OAS) members view the application of international law to cyberspace. Hollis sent a questionnaire to OAS member states, and while Brazil responded to the questionnaire (unlike many OAS member states), it merely stated that it would set out its views on the application of international law to cyberspace during the 2019–2021 GGE.[83] The aim of the 2019–2021 session was to include a compendium of state positions on the application of international law to cyberspace. That Brazil preferred to sidestep the OAS initiative and include its views in the GGE compendium came as no surprise given that Brazil was chair of the 2019–2021 GGE session and did not want to undermine the compendium initiative, which it saw as an important value-added benefit of that session.

A compendium attached to the 2021 GGE report contained voluntary national contributions on how international law applies to information and communication technologies (ICTs). In the compendium, Brazil affirmed the application of international law to cyberspace, including the UN Charter, international human rights law, and international humanitarian law. As with many states, Brazil sought to push discussions forward by explaining that "the question is no longer whether, but how international law applies to the use of ICTs by states."[84] In this statement, Brazil offered relatively detailed views on how it sees international law applying to cyberspace. The following sections explain Brazil's views and spotlight key points of convergence and divergence with other states.

Due Diligence

The question of whether due diligence constitutes an operative rule of international law is contested. Some states, such as Finland,[85] Italy,[86] the Netherlands,[87] and Switzerland,[88] see due diligence as a binding rule of international law. But other states, including the United Kingdom[89] and the United States,[90] prefer to characterize due diligence as a voluntary, nonbinding norm as set out in Norm 13(c) of the 2015 GGE report.

Brazil does not deal with the question of due diligence in a particularly straightforward manner. When discussing the right of self-defense, Brazil explains that states "should" adopt measures to prevent armed attacks emanating from their territory and notes that a failure to do so "might constitute an internationally wrongful act, thus entailing their international

responsibility."[91] Although its discussion of due diligence under the banner of self-defense is rather curious, as is its use of language ("should" and "might"), the inference seems to be that Brazil sees due diligence as a binding obligation under international law requiring states to prevent their territory from being used in a manner injurious to the legal rights of other states. Even if Brazil sees due diligence as a binding rule, its statement does not attempt to clarify the nature, content, or scope of this obligation.

Sovereignty

An important international legal question is whether sovereignty is a political principle of international relations or a binding rule of international law, the breach of which gives rise to an internationally wrongful act. The United Kingdom[92] (and possibly the United States[93]) has adopted the view that sovereignty is a political principle rather than an operative rule of international law. The overwhelming majority of states, however, construe sovereignty as a rule of international law that is legally consequential. Brazil firmly locates itself in this camp when, in the GGE compendium, it explains that the principle of sovereignty is a "standalone rule" of international law. Brazil's position on sovereignty affords states more protection against cyber operations than the United Kingdom's approach and, by doing so, limits the cyber operations that states can conduct against other states.[94]

Brazil further claims that there is "neither broad state practice nor sufficient *opinio juris* to generate [a] new customary international norm allowing for the violation of state sovereignty by ICT means."[95] This is an important statement because the majority of states that see sovereignty as a rule of international law tend to integrate a de minimis threshold into it. According to the de minimis approach, a breach of the principle of sovereignty occurs only when cyber operations cause sufficiently serious harmful effects on the cyber infrastructure of other states, that is, when they at least impair the functionality of computer systems or networks.

Generally, this approach to cyber sovereignty differs from how these states see sovereignty applying to their physical territory. For these states, they tend to see any nonconsensual intrusion into their national air space, territorial waters, or land territory as constituting a breach of their sovereignty, regardless of whether the intrusion produces sufficiently serious effects within their territory. For Brazil, however, customary practices indicate that the principle of sovereignty affords a state's cyber infrastructure with the same protection it affords a state's physical territory; any nonconsensual cyber operation against the cyber infrastructure of a state is prohibited.[96] This approach to the principle of sovereignty aligns with the positions of France,[97] Iran,[98] and Switzerland.[99]

Brazil's strict approach to the application of sovereignty to cyberspace is also exemplified by the following statement:

> "Interceptions of telecommunications, for instance, whether or not they are considered to have crossed the threshold of an intervention in the internal affairs of another state, would nevertheless be considered an internationally wrongful act because they violate state sovereignty."[100]

Brazil's determination that the principle of sovereignty prohibits the interception of telecommunications comes as no surprise. Brazil led international condemnation of the United States' reported cyber espionage operations in the wake of the Edward Snowden revelations, which included allegations about U.S. spying on then president Rousseff and other Brazilian diplomatic and parastatal targets.[101] Notably, Rousseff canceled a scheduled presidential visit to Washington, DC, to meet U.S. president Barack Obama and instead proceeded to the UN General Assembly, where she rebuked the reported U.S. actions as a breach of Brazilian sovereignty.[102] That said, Brazil's approach jars with the views of other states, such as Canada[103] and New Zealand,[104] which have recently determined that remote-access cyber espionage operations do not breach the principle of sovereignty.

Brazil's statement on the illegality of the interception of communications in the 2021 GGE compendium is interesting because it is cast in broader terms than the approach Brazil advocated during the fallout from the Snowden revelations. Consider the statement by the Southern Common Market (MERCOSUR), of which Brazil is a member, following the Snowden revelations in 2013. MERCOSUR said that it was:

> "Strongly rejecting the interception of telecommunications and the acts of espionage carried out in our countries, which constitute a violation of the human rights, the right to privacy and the right to information of our citizens, and which also constitute unacceptable behaviour that violates our sovereignty."[105]

As is apparent, this statement condemns the interception of communication "carried out in our countries." Although it is not stated explicitly, Brazil's statement in the 2021 GGE compendium seems to suggest that the interception of its telecommunications on any infrastructure is unlawful. If this reading is correct, the implication is that Brazil sees its data as being clothed with Brazilian sovereignty regardless of whose cyber infrastructure it is located upon.

Nonintervention

Brazil regards the principle of nonintervention as a rule of customary law applicable to cyberspace; thus, the use of cyber means to intervene in the internal affairs of another state is unlawful. For Brazil, cyber operations "must involve an element of coercion affecting the right of the victim state to freely choose its political, economic, social and cultural

system, and to formulate its foreign policy."[106] Where coercion is present, Brazil maintains that interfering in "electoral processes" amounts to a prohibited intervention because they constitute "the core of a state's internal affairs."[107]

Brazil adopts a conventional interpretation of the principle of nonintervention that is largely in line with the 1986 judgement of the International Court of Justice (ICJ) in *Nicaragua v. United States*.[108] In *Nicaragua*, the ICJ explained that coercion forms the "very essence" of intervention,[109] which means a state breaches the principles of nonintervention where it compels another state to do something or not to do something, as the case may be. Understood in this way, the principle of nonintervention protects a state's freedom of choice.

Use of Force

There seems to be near consensus among states that, in principle, cyber operations can constitute a prohibited use of force under Article 2(4) of the UN Charter. A tricky question is what effects must be caused for the impugned conduct to fall within the scope of this prohibition. When cyber means are used to cause effects similar to kinetic attacks, such as when a cyber attack is launched against air traffic control systems with lethal effects, there is little doubt that a use of force is committed. But what about cyber attacks causing online harm only, such as those disabling critical government communications systems?

States are currently divided as to whether purely cyber harm is sufficient to trip the prohibition on the use of force.[110] Brazil maintains that cyber operations amount to a prohibited use of force "if their impact is similar to the impact of a kinetic attack."[111] Brazil emphasizes a lack of "precedent" to determine that the use of force prohibition applies to cyber attacks not producing physical effects and urges caution "when making analogies between cyber and kinetic actions in assessments related to *jus ad bellum*."[112] Brazil therefore appears to interpret this prohibition narrowly, seeing it apply to cyber attacks only where they produce physical, offline harm.

Self-Defense

Article 51 of the UN Charter preserves the inherent right of self-defense when an "armed attack occurs," and Brazil adopts the widely (although not universally)[113] held view that armed attacks are "the gravest forms of the use of force."[114] Brazil claims that, as an exception to the nonuse of force principle, the right of self-defense must be interpreted "restrictively." This restrictive approach is evident in Brazil's discussion of whether nonstate actors can author armed attacks and thus be made the subject of self-defense action. For Brazil, self-defense is "only triggered by an armed attack undertaken by or attributable to a state. It is not possible to invoke self-defense as a response to acts by non-state actors, unless they are acting on behalf or under the effective control of a state."[115]

Brazil's approach to self-defense and nonstate actors is shared by states such as China, Mexico, and Sri Lanka.[116] However, it is at odds with the views of (mainly Western) states such as Australia, Azerbaijan, Belgium, Denmark, Estonia, the Netherlands, Türkiye, the United Kingdom, and the United States.[117] These states emphasize that Article 51 of the UN Charter affirms the right of self-defense when an "armed attack occurs." On the basis that Article 51 does not stipulate that the author of the armed attack must be a state, these states argue that self-defense can be engaged against state and nonstate actors.

Brazil's statement in the 2021 GGE compendium also addresses the thorny question of anticipatory self-defense. For Brazil, self-defense can be invoked only when there is an "actual or imminent armed attack"; to put the matter beyond doubt, Brazil explains that there is "no right to preventive 'self-defense'—a notion that does not find legal grounds neither in art. 51 of the Charter nor in customary international law."[118]

This approach is largely congruent with international practice. One of the United States' justifications for its military invasion of Iraq in 2003 was the doctrine of preemptive self-defense (the so-called "Bush Doctrine"), which maintained that states could use force to counter incipient or embryonic threats. The invasion of Iraq sparked an intense discussion of the legality of the doctrine of preemptive self-defense. The outcome was that states rejected this broad interpretation of the right of self-defense, instead holding that this doctrine can be invoked only where necessary to counter an *imminent* threat of an armed attack. As the UN secretary-general explained:

> "Imminent threats are fully covered in Article 51 [of the UN Charter], which safeguards the inherent right of sovereign States to defend themselves against an armed attack. Lawyers have long recognized that this covers an imminent attack as well as those that have already happened. . . . Where threats are not imminent but latent, the Charter gives full authority to the Security Council to use military force, including preventively, to preserve international peace and security."[119]

New Norms and Rules?

An important question in the cyber governance debate is whether the existing regulatory framework for cyberspace (as reflected in the UN GGE/Open-Ended Working Group *acquis*)[120] is sufficient to ensure responsible state behavior or whether new norms and rules are needed. Like-minded states tend to view the existing framework as sufficient, with the immediate task being to flesh out the content of this framework and better understand how existing norms and rules apply to cyberspace and the activities occurring within it. An alternative approach, largely spearheaded by China and Russia, pushes for new norms and rules, particularly in the form of a universal cyber treaty or subject-specific cyber treaties. The concern of like-minded states is that these cyber initiatives may act as a Trojan horse for China and Russia to establish greater control over cyberspace and chisel away the free, open, and decentralized nature of this domain.

Given Brazil's influence across the BRICS, Latin America, and the Global South, coupled with its role as an international deal broker, its position on the future regulation of cyberspace is important. As already noted, in 2012, Brazil expressed support for a UN-sponsored treaty on the regulation of the internet but has not subsequently made this a priority in its cyber diplomacy. Moreover, Brazil has been a supporter of cyber-specific sectoral treaties. For example, with regard to Russia's proposed Convention on Cybercrime, Brazil explained that it is "fully engaged" and "fully committed to the idea of a universal [cybercrime] convention."[121] Under Lula, it is unclear whether Brazil will continue to push for new international treaties on cyberspace, beyond the recent positions established under previous administrations.

Conclusion

Lula did not bring a preconceived blueprint for cyber strategy into office. His administration will focus on its political priorities, which most notably intersect with cyber on the domestic issues of disinformation and online extremism. Progress in Lula's cyber strategy is therefore likely to be slow. It risks being held back by his administration's lack of prioritization of cyber issues and the absence to date of a single senior political figure or institution willing to assume the role of driving forward the administration's cyber strategy. The GSI deserves credit for publishing its PNCiber consultation, but when the administration wants to legislate to advance its cyber agenda, it will need to navigate through the political reality that congressional support will not be guaranteed.

Delays are likely, but opportunities still exist for like-minded states to engage with the Lula administration. These states are well-placed to continue providing training and other support for initiatives to build Brazil's cyber capacity and grow its national cyber ecosystem. This will include opportunities to support the development and work of cyber professionals in Brazil's federal law enforcement, national defense, and incident response communities. At the strategic level, the experience of like-minded states in cross-government coordination of cyber policies—with an important role for the central executive—would be a useful example for Brazil, as it is not always apparent that different institutional actors in the Brazilian system (for instance, the Foreign Ministry and the Armed Forces) coordinate effectively with each other. It would be prudent for like-minded states to embrace these opportunities, not least to prevent geopolitical competitors from gaining a foothold through their own offerings of cyber-related support to Brazil.

Internationally, Brazil resists external pressure and influence and maintains an independent foreign policy. It sees itself as an alliance builder rather than a swing state, and this is particularly the case with regard to cyber governance. As a BRICS member and a prominent voice of the Global South, Brazil is an important strategic partner for like-minded states.

These states share common values and objectives when it comes to cyber governance, such as a commitment to the existing multistakeholder structure, the protection of human rights, the applicability of international law, and the need for cyber capacity building. But divergences between Brazil and like-minded states are also evident. There are fissures in *how* they see international law applying to cyberspace, such as whether the principles of due diligence and sovereignty are rules of international law. Perhaps most importantly, Brazil and like-minded states seem to embrace different views as to next steps in cyberspace regulation. Brazil has previously expressed support for the development of new laws and regimes, a position that aligns with China and Russia but is largely opposed by like-minded states. These normative cleavages may make an effective partnership between Brazil and like-minded states more difficult.

About the Authors

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

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

Notes

1 Bruna Santos, "Navigating the Crossroads: Lula's First 100 Days," Wilson Center, April 14, 2023, https://www.wilsoncenter.org/blog-post/navigating-crossroads-lulas-first-100-days. For more recent reflections on the performance of Lula's government and the political context in which it operates, see "AQ Podcast: The Ups And Downs Of Lula's First Six Months," Americas Quarterly, June 28, 2023, https://www.americasquarterly.org/article/aq-podcast-the-ups-and-downs-of-lulas-first-six-months/; and "The Lula Administration›s Greatest Challenges with Fábio Sá e Silva," Brazil Unfiltered, July 5, 2023, https://www.spreaker.com/user/15263692/bu-fabio-sa-silva.

2 Gabinete de Segurança Institucional da Presidência da Republica (Secretaria de Segurança da Informação e Cibernética), "Política Nacional de Cibersegurança – Apresentação do Projeto," May 18, 2023, https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf. For our analysis of the consultation document and its significance, see p.4 of this report.

3 Joe Devanny, Luiz Rogerio Franco Goldoni, and Breno Pauli Medeiros, "The Rise of Cyber Power in Brazil," Revista Brasileira de Politica Internacional 65, no. 1 (2022): 1–21, https://doi.org/10.1590/0034-7329202200113. The wider national cyber security landscape has recently been mapped by Louise Marie Hurel, Mapping Cyber Policy in Latin America: The Brazilian Case, Centro Latam Digital (April 2023), https://centrolatam.digital/publicacion/mapping-cyber-policy-in-latin-america-the-brazilian-case.

4 Carlos Solar, Cyber Security Governance in Latin America: States, Threats, and Alliances (Albany, NY: SUNY Press, 2023).

5 "Brazil's Court System Under Massive RansomExx Ransomware Attack," Bleeping Computer, November 5, 2020, https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack.

6 "Brazil's Health Ministry Website Hacked, Vaccination Information Stolen and Deleted," ABC, December 11, 2021, https://www.abc.net.au/news/2021-12-11/brazils-national-vaccination-program-hacked-/100692952.

7 Louise Marie Hurel, "Brazil's First National Cybersecurity Strategy: An Analysis of Its Past, Present And Future," Internet Governance Project, April 5, 2020, https://www.internetgovernance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-past-present-and-future.

8 Article 1 of the Complementary Law No. 97 (June 9, 1999) affirms Article 142 of the constitution.

9 Joe Devanny and Vinicius Mariano de Carvalho, "Politics and Civil-Military Relations: Where Next for Brazil Under Bolsonaro?," King's College London, April 1, 2021, https://www.kcl.ac.uk/politics-and-civil-military-relations-where-next-for-brazil-under-bolsonaro.

10 Brad Brooks, "Brazil Army Commander ‹Repudiates Impunity› on Eve of Lula Ruling," Reuters, April 4, 2018, https://www.reuters.com/article/us-brazil-politics-lula-idUSKCN1HB09J.

11 For a report describing U.S. diplomacy to support Brazilian democracy during the elections and transition, see Michael Stott, Michael Pooler, and Bryan Harris, "The Discreet U.S. Campaign to Defend Brazil's Election," Financial Times, June 21, 2023, https://www.ft.com/content/07533564-2231-47a6-a7b8-2c7ae330efc5.

12 Bruno Boghossian, Igor Gielow, and Cézar Feitoza, "Lula demite comandante do Exército após crise de confiança," Folha de S.Paulo, January 21, 2023, https://www1.folha.uol.com.br/poder/2023/01/lula-demite-comandante-do-exercito-apos-crise-de-confianca.shtml.

13 Cézar Feitoza, "Mudança de comando no Exército pode resultar em novas demissões," Folha de S.Paulo, January 23, 2023, https://www1.folha.uol.com.br/poder/2023/01/mudanca-de-comando-no-exercito-pode-resultar-em-novas-demissoes.shtml.

14 Author's translation from Cézar Feitoza, "Comandante do Exército diz a generais que fala vazada sobre Lula buscava pacificar temas politicos," Folha de São Paulo, February 28, 2023, https://www1.folha.uol.com.br/poder/2023/02/comandante-do-exercito-diz-a-generais-que-fala-vazada-sobre-eleicao-de-lula-foi-tirada-de-contexto.shtml.

15 Renato Machado, "Lula afirma ter compromisso de militares para despolitizar Forças Armadas," Folha de São Paulo, March 21, 2023, https://www1.folha.uol.com.br/poder/2023/03/lula-afirma-ter-compromisso-de-militares-para-despolitizar-forcas-armadas.shtml.

16 For an overview of the wider institutional landscape of cyber policy in Brazil, see Hurel, Mapping Cyber Policy in Latin America.

17 Ranier Bragon and Victoria Azevedo, "Militares que trabalhavam na Presidência foram a atos golpistas em frente a quartel," Folha de São Paulo, January 19, 2023, https://www1.folha.uol.com.br/poder/2023/01/militares-que-trabalhavam-na-presidencia-foram-a-atos-golpistas-em-frente-a-quartel.shtml.

18 Gonçalves Dias had served in a similar role under Lula's Workers' Party successor, president Dilma Rousseff. See Jéssica Sant'Ana e Pedro Henrique Gomes, "Lula anuncia general da reserva Marco Edson Gonçalves Dias para chefia do GSI," O Globo, December 29, 2022, https://g1.globo.com/politica/noticia/2022/12/29/lula-anuncia-general-da-reserva-marco-edson-goncalves-dias-para-chefia-do-gsi.ghtml.

19 Like Gonçalves Dias, General Amaro has previous experience serving under Rousseff in a similar role. See Ana Luiza Antunes, "Quem é o general Marcos Antônio Amaro dos Santos, escolhido de Lula para o GSI," Estadao, April 28, 2023, https://www.estadao.com.br/politica/quem-e-general-marcos-antonio-amaro-dos-santos-novo-ministro-gsi-governo-lula-dilma-rousseff-nprp.

20 Weslley Galzo, "General Amaro assume comando do GSI em reunião fechada com Lula após exoneração em massa na pasta," Estadao, May 4, 2023, https://www.estadao.com.br/politica/general-amaro-assume-comando-do-gsi-em-reuniao-fechada-com-lula-apos-exoneracao-em-massa-na-pasta/.

21 Jeniffer Gularte and Thiago Bronzatto, "Entrevista: 'É melhor que haja lei sobre fake news,' diz Paulo Pimenta," O Globo, February 27, 2023, https://oglobo.globo.com/politica/noticia/2023/02/entrevista-e-melhor-que-haja-lei-sobre-fake-news-o-judiciario-e-lento-diz-paulo-pimenta.ghtml; and Presidencia da Republica, "Estrutura e Competências," gov.br, January 5, 2023, https://www.gov.br/secom/pt-br/composicao/secretaria-de-politicas-digitais/estrutura-e-competencias.

22 Gov.br, "Esther Dweck defende Estado eficiente para combater desigualdades," January 2, 2023, https://www.gov.br/pt-br/noticias/comunicacao/2023/01/esther-dweck-defende-estado-eficiente-para-combater-desigualdades.

23 Amanda Audi, "Lula Creates Working Group to Fight Online Extremism," Brazilian Report, February 22, 2023, https://brazilian.report/liveblog/2023/02/22/lula-working-online-extremism.

24 ABIN's remit is constitutionally mandated to be domestic only. It cannot conduct intelligence operations overseas.

25 Marcelo Freire, "Veja quem é Rui Costa, novo ministro-chefe da Casa Civil de Lula," CNN Brasil, December 9, 2022, https://www.cnnbrasil.com.br/politica/veja-quem-e-rui-costa-novo-ministro-chefe-da-casa-civil-de-lula. Interestingly, it has been reported that Lula has set countering cybersecurity threats as one of ABIN's top priorities. However, it is unclear what capacity ABIN has to achieve this and how effectively it coordinates its cyber-related activities with other relevant institutional actors such as the Armed Forces, the GSI, and the Federal Police. See Fabio Serapiao, "Atos golpistas, Amazonia e ciberseguranca são prioridade, diz diretor de escola da Abin," Folha de S.Paulo, June 10, 2023, https://www1.folha.uol.com.br/poder/2023/06/atos-golpistas-amazonia-e-ciberseguranca-sao-prioridade-diz-diretor-de-escola-da-abin.shtml.

26 Marianna Holanda, "Governo Lula decide transferir Abin para Casa Civil," Folha de S.Paulo, February 9, 2023, https://www1.folha.uol.com.br/poder/2023/02/governo-lula-decide-transferir-abin-para-casa-civil.shtml.

27 ABIN experienced an early setback in the Lula administration's first three months related to a controversy over alleged digital surveillance. It was reported that an official investigation was launched into ABIN's use of commercial spyware under the Bolsonaro administration, reportedly to conduct warrantless surveillance against Bolsonaro's political opponents. See João Valadares and Isadora Peron, "PF vai investigar denúncia sobre espionagem da Abin," O Globo, March 15, 2023, https://valor.globo.com/politica/noticia/2023/03/15/dino-determina-abertura-de-inqurito-da-pf-para-apurar-caso-de-espionagem-da-abin.ghtml.

28 Luiz Rogerio Franco Goldoni, Karina Furtado Rodrigues, and Temístocles Murilo de Oliveira Júnior, "O urgente debate sobre a proposta de Política Nacional de Cibersegurança," Estadao, June 8, 2023, https://www.estadao.com.br/politica/gestao-politica-e-sociedade/o-urgente-debate-sobre-a-proposta-de-politica-nacional-de-ciberseguranca.

29 Carolina Cruz, "Proposta de política para cibersegurança levanta novo debate sobre quem deve fiscalizar," Tele Síntese, June 15, 2023, https://www.telesintese.com.br/proposta-de-politica-para-ciberseguranca-levanta-novo-debate-sobre-quem-deve-fiscalizar.

30 Luis Osvaldo Grossmann, "Orçamento de R$600 milhões é maior desafio para Agência Nacional de Cibersegurança," Convergência Digital, June 15, 2023, https://www.convergenciadigital.com.br/Seguranca/Orcamento-de-R%24-600-milhoes-e-maior-desafio-para-Agencia-Nacional-de-Ciberseguranca-63455.html.

31 Victor Correia, "'Não estamos distantes de uma proteção contra ciberataques,' diz Veneziano," Correio Braziliense, May 18, 2023, https://www.correiobraziliense.com.br/politica/2023/05/5095430-nao-estamos-distantes-de-uma-protecao-contra-ciberataques-diz-veneziano.html.

32 Ricardo Brito, "Brazil's Lula Says Intelligence Services Failed Ahead of Brasilia Riots," Reuters, January 19, 2023, https://www.reuters.com/world/americas/brazils-lula-says-intelligence-services-failed-ahead-brasilia-riots-2023-01-18.

33 "Lula Dismisses More Military Personnel From Security Detail After Brazil Riots," Reuters, January 18, 2023, https://www.reuters.com/world/americas/lula-dismisses-more-military-personnel-security-detail-after-brazil-riots-2023-01-18.

34 Carolina Caeiro, 'Bolsonaro's social media plan shows his election worry,' Chatham House, September 29, 2021, https://www.chathamhouse.org/2021/09/bolsonaros-social-media-plan-shows-his-election-worry; and Constance Malleret, Dan Milmo, and Alex Hern, "Pro-Bolsonaro Violence: Experts Highlight Role of Social Media Platforms," Guardian, January 9, 2023, https://www.theguardian.com/world/2023/jan/09/pro-bolsonaro-violence-social-media-platforms.

35 Jeniffer Gularte and Thiago Bronzatto, "Entrevista: 'É melhor que haja lei sobre fake news,' diz Paulo Pimenta," O Globo, February 27, 2023, https://oglobo.globo.com/politica/noticia/2023/02/entrevista-e-melhor-que-haja-lei-sobre-fake-news-o-judiciario-e-lento-diz-paulo-pimenta.ghtml; and Presidencia da Republica, "Estrutura e Competências," gov.br, January 5, 2023, https://www.gov.br/secom/pt-br/composicao/secretaria-de-politicas-digitais/estrutura-e-competencias.

36 It is worth noting that, in Brazil, disinformation is principally discussed as an issue of domestically generated fake news, whereas in other states the issue is often discussed in the context of state threats. In both cases, however, the fake news content is generally disseminated on major social media platforms.

37 Mariana Palau, "Inside Brazil's Dangerous Battle Over Fake News," Americas Quarterly, October 19, 2021, https://americasquarterly.org/article/inside-brazils-dangerous-battle-over-fake-news; Max Fisher and Amanda Taub, "How YouTube Radicalized Brazil," New York Times, August 11, 2019, https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html; and Robert Muggah, "Bolsonaro Is Already Undermining Brazil's Upcoming Election," Foreign Policy, May 4, 2022, https://foreignpolicy.com/2022/05/04/bolsonaro-brazil-election-2022-disinformation-misinformation-digital-social-media.

38 Jack Nicas and Andre Spigariol, "Brazil Lifts Its Ban on Telegram After Two Days," New York Times, March 20, 2022, https://www.nytimes.com/2022/03/20/world/americas/brazil-telegram-bolsonaro.html; and Marie Lamensch, "In Brazil 'Techno-Authoritarianism' Rears Its Head," Centre for International Governance Innovation, September 19, 2022, https://www.cigionline.org/articles/in-brazil-techno-authoritarianism-rears-its-head.

39 Lisandra Paraguassu and Gabriel Stargardter, "Bolsonaro Allies Allegedly Pushing Fake News, Brazil Police Document Says," Reuters, February 11, 2022, https://www.reuters.com/world/americas/bolsonaro-allies-allegedly-pushing-fake-news-effort-brazil-police-document-says-2022-02-11.

40 Angelica Mari, "Social Networks Partner With Brazil's Electoral Justice to Tackle Fake News During Elections," ZDNet, February 11, 2022, https://www.zdnet.com/article/social-networks-partner-with-brazils-electoral-justice-to-tackle-fake-news-during-elections; and Patricia Campos Mello, "Agreements With Platforms for Elections in Brazil Fall Short of Policies in the U.S.," Global Freedom of Expression (blog), Columbia University, July 14, 2022, https://globalfreedomofexpression.columbia.edu/updates/2022/07/agreements-with-platforms-for-elections-in-brazil-fall-short-of-policies-in-the-u-s.

41 "Facebook Fails to Tackle Election Disinformation Ads Ahead of Tense Brazilian Election," Global Witness, August 15, 2022, https://www.globalwitness.org/en/campaigns/digital-threats/facebook-fails-tackle-election-disinformation-ads-ahead-tense-brazilian-election; and Elizabeth Dwoskin, "Come to the 'War Cry Party': How Social Media Helped Drive Mayhem in Brazil," Washington Post, January 9, 2023, https://www.washingtonpost.com/technology/2023/01/08/brazil-bolsanaro-twitter-facebook.

42 Mac Margolis and Robert Muggah, "Why Disinformation Could Prove Decisive in Brazil's Election," Open Democracy, October 5, 2022, https://www.opendemocracy.net/en/democraciaabierta/disinformation-brazil-election-bolsonaro-lula-far-right; and Dwoskin, "Come to the 'War Cry Party.'"

43 Gabriela Coelho, "Telegram informa ao STF que fez o deposito de R$1,2 milhao e reitera pedido para revogacao," CNN Brasil, February 2, 2023, https://www.cnnbrasil.com.br/politica/telegram-informa-ao-stf-que-fez-o-deposito-de-r-12-milhao-e-reitera-pedido-para-revogacao.

44 Renata Galf, "Plano do governo Lula para combater fake news embute risco e gera divergência," Folha de Sao Paulo, January 20, 2023, https://www1.folha.uol.com.br/poder/2023/01/plano-do-governo-lula-para-combater-fake-news-embute-risco-e-gera-divergencia.shtml.

45 This paragraph draws on recent reporting by Patricia Campos Mello. See Patricia Campos Mello, "Governo Lula discute plano B para regulação de internet antes da eleição de 2024," Folha de S.Paulo, July 2, 2023, https://www1.folha.uol.com.br/poder/2023/07/governo-lula-discute-plano-b-para-regulacao-de-internet-antes-da-eleicao-de-2024.shtml.

46 For more background and commentary on proposed legislation, see Joan Barata, "Regulating Online Platforms Beyond the Marco Civil in Brazil: The Controversial 'Fake News Bill,'" Tech Policy Press, May 23, 2023, https://techpolicy.press/regulating-online-platforms-beyond-the-marco-civil-in-brazil-the-controversial-fake-news-bill.

47 Gabriel Shinohara and André de Souza, "Ministério da Justiça determina multa diária de R$ 1 mil se TikTok não retirar conteúdos impróprios para menores," O Globo, June 24, 2022, https://oglobo.globo.com/economia/noticia/2022/06/ministerio-da-justica-determina-que-tiktok-suspenda-exibicao-de-conteudo-improprio-para-menores.ghtml.

48 The working group is led by former vice-presidential candidate Manuela D'Ávila. See Amanda Audi, "Lula Creates Working Group to Fight Online Extremism," Brazilian Report, February 22, 2023, https://brazilian.report/liveblog/2023/02/22/lula-working-online-extremism.

49 Bruna Santos, "Brazil's 'Fake News Bill' Sets Global Precedent With Dangerous Implications," Brazilian Report, April 24, 2023, https://brazilian.report/opinion/2023/04/24/fake-news-bill-dangerous-implications.

50 Patricia Vilas Boas, "Presidente do Google no Brasil diz que empresa quer evitar regulação 'perversa,'" Folha de S.Paulo, June 27, 2023, https://www1.folha.uol.com.br/tec/2023/06/presidente-do-google-no-brasil-diz-que-empresa-quer-evitar-regulacao-perversa.shtml.

51 Patricia Campos de Mello, "Google contrata Temer para atuar nas negociações sobre regulação de big techs," Folha de S.Paulo, June 30, 2023, https://www1.folha.uol.com.br/poder/2023/06/google-contrata-temer-para-atuar-nas-negociacoes-sobre-regulacao-de-big-techs.shtml.

52 "Welcoming Brazil's Marco Civil: A World First Digital Bill of Rights," Web Foundation, March 26, 2014, https://webfoundation.org/2014/03/welcoming-brazils-marco-civil-a-world-first-digital-bill-of-rights.

53 "Freedom of the Net 2021," Freedom House, 2022, https://freedomhouse.org/country/brazil/freedom-net/2021; and "Marco Civil Law of the Internet in Brazil," CGI.br, 2014, https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180.

54 "Defending Brazil From Techno-Authoritarianism," Data Privacy Brasil, 2023, https://www.dataprivacybr.org/en/projeto/defending-brazil-from-techno-authoritarianism.

55 Jeniffer Gularte and Thiago Bronzatto, "Entrevista: 'É melhor que haja lei sobre fake news', diz Paulo Pimenta," O Globo, February 27, 2023, https://oglobo.globo.com/politica/noticia/2023/02/entrevista-e-melhor-que-haja-lei-sobre-fake-news-o-judiciario-e-lento-diz-paulo-pimenta.ghtml.

56 Patricia Campos Mello, "Governo Lula discute plano B para regulação de internet antes da eleição de 2024," Folha de S.Paulo, July 2, 2023, https://www1.folha.uol.com.br/poder/2023/07/governo-lula-discute-plano-b-para-regulacao-de-internet-antes-da-eleicao-de-2024.shtml.

57 "Remarks by President Biden at the Summit for Democracy Virtual Plenary on Democracy Delivering on Global Challenges," White House, March 29, 2023, https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/03/29/remarks-by-president-biden-at-the-summit-for-democracy-virtual-plenary-on-democracy-delivering-on-global-challenges.

58 Steven Feldstein and Brian (Chun Hey) Kot, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses," Carnegie Endowment for International Peace, March 14, 2023, https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

59 Catalin Cimpanu and Angelica Mari, "Telegram Voicemail Hack Used Against Brazil's President, Ministers," ZDNet, July 26, 2019, https://www.zdnet.com/article/telegram-voicemail-hack-used-against-brazils-president-ministers.

60 Dom Phillips, "Brazil's Former President Lula Walks Free From Prison After Supreme Court Ruling," Guardian, November 8, 2019, https://www.theguardian.com/world/2019/nov/08/lula-brazil-released-prison-supreme-court-ruling.

61 Amanda Audi, Gustavo Ribeiro, Euan Marshall, and Ana Ferraz, "The Plan to Hack Brazil's Chief Electoral Justice," Brazilian Report, February 7, 2023, https://brazilian.report/power/2023/02/07/hack-moraes-delgatti.

62 Leonardo Caldas, "Senador diz que contou a Braga Netto o plano golpista de Bolsonaro," Veja, February 5, 2023,https://veja.abril.com.br/politica/senador-diz-que-contou-a-braga-netto-o-plano-golpista-de-bolsonaro.

63 Bruce Douglas, "Release of Tapped Phone Calls Between Lula and Rousseff Sparks Mass Protests in Brazil," Guardian, March 17, 2016, https://www.theguardian.com/world/2016/mar/17/release-tapped-phone-calls-lula-rousseff-deepens-brazil-chaos.

64 For a discussion of the group of like-minded states, see Ash Jain, "Like-Minded and Capable Democracies: A New Framework for Advancing a Liberal World Order," Council on Foreign Relations, January 2013, https://cdn.cfr.org/sites/default/files/pdf/2012/11/IIGG_WorkingPaper12_Jain.pdf.

65 Julia Pohle and Thorsten Thiel, "Digital Sovereignty," Internet Policy Review 9, no. 4 (2020): [https://doi.org/10.14763/2020.4.1532, 1, 5.

66 UN General Assembly Resolution 68/167, December 18, 2013, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/47/PDF/N1344947.pdf?OpenElement.

67 Hannes Ebert and Laura Groenendaal, "Brazil's Cyber Resilience and Diplomacy: The Place for Europe," EU Cyber Direct (April 2020), 23–24, https://eucyberdirect.eu/research/brazils-cyber-resilience-and-diplomacy-the-place-for-europe#.

68 Alex Grigsby, "Do India and Brazil Really Moderate China's and Russia's Approach to Cyberspace Policy?," Net Politics (blog), Council on Foreign Relations, April 26, 2016, https://www.cfr.org/blog/do-india-and-brazil-really-moderate-china-and-russias-approach-cyberspace-policy.

69 "Brazil's Cyber Diplomacy Is Aligned With Neither of the Great Power Poles"; and Louise Marie Hurel, "Unpacking Brazil's Cyber Diplomacy," Directions (blog), EU Cyber Direct, March 14, 2022, https://directionsblog.eu/unpacking-brazils-cyber-diplomacy.

70 Ebert and Groenendaal, "Brazil's Cyber Resilience and Diplomacy," 19.

71 Grigsby, "Do India and Brazil Really Moderate China's and Russia's Approach to Cyberspace Policy?"

72 For an overview, see Ebert and Groenendaal, "Brazil's Cyber Resilience and Diplomacy," 21–26.

73 James A. Lewis, "UN Publishes Latest Report of the Group of Government Experts," Center for Strategic and International Studies, August 27, 2015, https://www.csis.org/blogs/strategic-technologies-blog/un-publishes-latest-report-group-government-experts; and Louise Marie Hurel, "A Conversation With Brazil's Cyber Diplomat," London School of Economics, February 2022, https://www.lse.ac.uk/ideas/Assets/Documents/project-docs/digital-ir/commentary/LSE-IDEAS-Cyber-Diplomat.pdf.

74 Devanny, Goldoni, and Medeiros, "The Rise of Cyber Power in Brazil."

75 Oliver Stuenkel, "At CELAC Summit, Left-Wing Leaders May Not Find Agreement," Americas Quarterly, January 23, 2023, https://www.americasquarterly.org/article/at-celac-summit-left-wing-leaders-may-not-find-agreement.

76 Detlef Nolte, "Ucrânia divide a América Latina e a União Europeia e dificulta uma parceria estratégica," Folha de S.Paulo, February 9, 2023, https://www1.folha.uol.com.br/colunas/latinoamerica21/2023/02/ucrania-divide-a-america-latina-e-a-uniao-europeia-e-dificulta-uma-parceria-estrategica.shtml.

77 UN General Assembly Resolution A/ES-11/1, March 2, 2022, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/293/36/PDF/N2229336.pdf?OpenElement.

78 UN General Assembly Resolution A/ES-11/L.7, February 16, 2023, https://documents-dds-ny.un.org/doc/UNDOC/LTD/N23/048/58/PDF/N2304858.pdf?OpenElement, para. 5.

79 "Lula renova interesse pelo Brics em meio a diferenças no bloco e possível expansão," Folha de San Paulo, January 22, 2023, https://www1.folha.uol.com.br/mundo/2023/01/lula-renova-interesse-pelo-brics-em-meio-a-diferencas-no-bloco-e-possivel-expansao.shtml.

80 Cedê Silva, "Lula Fails to Recreate South American Bloc," Brazilian Report, May 31, 2023, https://brazilian.report/latin-america/2023/05/31/lula-unasur-south-american-bloc; and Martha Viotti Beck, "Brazil's Lula Vows to Grow Mercosur Amid Uruguay Flak, Argentina Crisis," Bloomberg, July 4, 2023, https://www.bloomberg.com/news/articles/2023-07-04/lula-vows-to-grow-mercosur-amid-uruguay-flak-argentina-crisis.

81 Hurel, "Unpacking Brazil's Cyber Diplomacy," 3.

82 Ebert and Groenendaal, "Brazil's Cyber Resilience and Diplomacy," 10.

83 "Fifth Report: Improving Transparency: International Law and State Cyber Operations," Organization of American States, August 7, 2020, 6 https://www.oas.org/en/sla/iajc/docs/themes_recently_concluded_International_law_State_cyber_operations_FINAL_REPORT.pdf.

84 Official Compendium of Voluntary National Contributions on the Subject of How International Applies to the Use of ICTs, Attached to the 2021 UN GGE Report (2021), 17, https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf.

85 "Finland's National Position: International Law and Cyberspace," Finland's Ministry of Foreign Affairs, 2020, 4, https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859.

86 "Italy's National Position: International Law and Cyberspace," 2021, 6–7, https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

87 "Netherlands National Position: Appendix: International Law in Cyberspace," 2019, 4, https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

88 "Switzerland's National Position: International Law and Cyberspace," 2021, 7, https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.

89 "There is not yet state practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace," in Official Compendium, 2021 UN GGE Report, 117.

90 Official Compendium, 2021 UN GGE Report, 141.

91 Official Compendium, 2021 UN GGE Report, 20.

92 Jeremy Wright, "Cyber and International Law in the 21st Century," UK Attorney General's Office, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; and Suella Braverman, "International Law in Future Frontiers," UK Attorney General's Office, 2022, https://www.gov.uk/government/speeches/international-law-in-future-frontiers.

93 U.S. Department of Defense, "DoD General Counsel Remarks at U.S. Cyber Command Legal Conference," 2020, https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference.

94 Official Compendium, 2021 UN GGE Report, 18.

95 Official Compendium, 2021 UN GGE Report, 18.

96 "Cyber operations against information systems located in another state's territory or causing extraterritorial effects might also constitute a breach of sovereignty," in Official Compendium, 2021 UN GGE Report, 18.

97 "France's National Position: International Law in Cyberspace," 2019, 7, https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf.

98 "Iran's National Position: International Law and Cyberspace," August 18, 2020, https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

99 "Switzerland's National Position," 2–3.

100 Official Compendium, 2021 UN GGE Report, 18.

101 Julian Borger, "Brazilian President: U.S. Surveillance a 'Breach of International Law,'" Guardian September 24, 2013, https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

102 "Global Perspective Human Stories," UN News, September 24, 2013, https://news.un.org/en/story/2013/09/450022.

103 "Some cyber activities, such as cyber espionage, do not amount to a breach of territorial sovereignty, and hence to a violation of international law," in "Canada's National Position: International Law Applicable in Cyberspace," Government of Canada, 2022, para. 19, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng.

104 "There is a range of circumstances—in addition to pure espionage activity—in which an unauthorised cyber intrusion, including one causing effects on the territory of another state, would not be internationally wrongful," in "New Zealand's National Position: The Application of International Law to State Activity in Cyberspace," New Zealand Department of the Prime Minister and Cabinet, 2020, para. 14, https://dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace.

105 UN Doc A/67/946, July 29, 2013, 2, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/411/07/PDF/N1341107.pdf?OpenElement.

106 Official Compendium, 2021 UN GGE Report, 19.

107 Official Compendium, 2021 UN GGE Report, 19.

108 Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgment (Merits) [1986] ICJ Rep. 14. para. 205, https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

109 Case Concerning Military and Paramilitary Activities in and Against Nicaragua.

110 For a review of state practice, see Marco Roscini, "Cyber Operations as a Use of Force," in Nicholas Tsagourias and Russell Buchan (eds.), Research Handbook on International Law and Cyberspace (Edward Elgar, 2021).

111 Official Compendium, 2021 UN GGE Report, 19.

112 Official Compendium, 2021 UN GGE Report, 19.

113 The United States, for example, regards all uses of force as armed attacks; see Harold Koh, U.S. Department of State, "International Law in Cyberspace," 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.

114 Official Compendium, 2021 UN GGE Report, 20.

115 Official Compendium, 2021 UN GGE Report, 20.

116 Adil Ahmad Haque, "Self-Defense Against Non-state Actors: All Over the Map," Just Security, March 24, 2021, https://www.justsecurity.org/75487/self-defense-against-non-state-actors-all-over-the-map.

117 Haque, "Self-Defense Against Non-state Actors."

118 Official Compendium, 2021 UN GGE Report, 20.

119 Report of the Secretary-General, "In Larger Freedom: Towards Development, Security, and Human Rights for All," UN Doc. A/59/2005, March 21, 2005, para. 124–125, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/270/78/PDF/N0527078.pdf?OpenElement.

120 "Overview: Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies," UN Office for Disarmament Affairs, 2021, https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021.

121 Permanent Mission of the Federative Republic of Brazil, "Brazilian Government's Position Regarding the Objectives, Scope and Structure of an International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes," 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Brazil_AHC_Brazilian_Position.pdf; and Summer Walker, Still Poles Apart: UN Cybercrime Treaty Negotiations, Global Initiative, June 2023, https://globalinitiative.net/wp-content/uploads/2023/06/Summer-Walker-Poles-apart-UN-cybercrime-treaty-negotiations-GI-TOC-June-2023.pdf.

Carnegie Endowment for International Peace

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

Technology and International Affairs Program

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

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org