Digital IR | COMMENTARY

FEBRUARY 2022

A Conversation with Brazil's Cyber Diplomat

LOUISE MARIE HUREL

Throughout the years, many countries have sought to develop new institutional mechanisms to adapt to the challenges deriving from emerging technologies, increased connectivity and heightened levels of vulnerability associated with these systems. The recurrence of major global cyberattacks, that historically range from 2011's Stuxnet to the latest ones reported in Ukraine, made it clear that cyberspace is the realm of ongoing geopolitical disputes. With that in mind, Ministries of Foreign Affairs in countries such as Denmark, Netherlands, Singapore, Australia and others have designated cyber diplomats to engage specifically with these agendas across national and international levels. In 2019, Brazil assigned its first cyber diplomat, Minister Marcelo Câmara. The decision came at the time where the country was also tasked with chairing, for the second time, the United Nations Group of Governmental Experts on the developments in the field of information and telecommunications in the context of international security under the chairmanship of Ambassador Guilherme Patriota.

> '[Minister Marcelo Câmara...] has worked in multiple thematic areas such as national defence, nuclear diplomacy, and cybersecurity. In this interview I discuss with him the present and future pathways for Brazil's foreign policy on the topic.'

Brazil has previously been portrayed as a pioneer in Internet Governance.[1] This legacy draws on multiple events, that include but are not restricted to: the development of its own national multistakeholder Internet governance model, consolidated in the form of the Internet Steering Committee (CGI.br) in 1995;[2] the country's active engagement in the World Summit on Information Society (2003 and 2005) and negotiations that preceded the creation of the UN Internet Governance Forum (IGF); and push back against surveillance and espionage post-Snowden revelations.

Less known, however, are Brazil's endeavours in cybersecurity. Since the early 2000s the country has gradually developed a reservoir of norms and policies focusing on cybersecurity and information security,[3] which has culminated in the publication of Brazil's first cybersecurity strategy, the national incident response network, the national data protection authority among other developments in the last three years.

Internationally, however, Brazil has also played a role in some cybersecurity-related agendas. The country chaired two UNGGE processes, one in 2015 and the other in 2021, both of which led to a consensus report advancing the discussion on the applicability of international law in cyberspace as well as delineating the necessary commitments from states in abiding by norms of responsible behaviour in this domain.

Minister Marcelo Câmara has been a career diplomat since 1995 and has held various positions in Brazil and abroad. He has worked in multiple thematic areas such as national defence, nuclear diplomacy, and cybersecurity. In this interview I discuss with him the present and future pathways for Brazil's foreign policy on the topic.

Who is Brazil's first cyber diplomat?

Cybersecurity became part of my portfolio in 2015 as I took over the Disarmament and Sensitive Technologies Division in the Brazilian MFA. Later on, I participated (2016-2017) as the Brazilian Expert in the Group of Governmental Experts (GGE) on the developments in the field of information and telecommunications in the context of international security, established by UNGA Resolution A/RES/70/237. In October 2019, I was nominated coordinator for cybersecurity issues in the Brazilian MFA and in the following year, Director of the Defence Department. In the period 2019-2020, I was assistant to the chair of the GGE on advancing responsible State behaviour in the cyberspace in the context of the international security, pursuant to UNGA Resolution A/RES/73/266.

Cybersecurity has undoubtably become a key aspect for countries' foreign policies. Denmark, Australia, Brazil, and others have been designating their own cyber diplomat and adjusting their MFAs to deal with some of the issues deriving from cyber threats. How do you see this global move towards cyber diplomacy as an institutionalised practice?

I think that there has been of late a widespread recognition by diplomatic actors of the growing dependence of modern societies on the cyberspace and its implications to the international security agenda. Admittedly information and communications technologies provide ample resources for social and economic advances. However, the malicious use of those technologies pose, at the same time, serious challenges to both domestic and international environments. Diplomacy should keep pace with these historic developments, or it will lose relevance. A more institutionalized practice of cyber diplomacy is therefore a necessity. We need diplomatic practitioners with a grasp of the complexity of the various cyber security issues. Many MFAs, including Itamaraty [Brazil's MFA], have invested human and institutional resources to strengthen their participation in international discussions on cybersecurity.

What does cyber diplomacy entail in the context of Brazil's foreign policy? Which themes, topics and spaces have been at the core of this emerging area within Brazil's Ministry of External Relations?

Diplomatic initiatives aimed at preserving the integrity of the cyberspace have gained more salience worldwide, including in Brazil's foreign policy. In coordination with other areas in the Federal Government, Itamaraty's work in cybersecurity has focused on enhancing a multistakeholder perspective, effective cooperation to tackle the common challenges and the full application of the international law in the cyberspace, including the international humanitarian law and human rights. In the UN, Brazil has actively participated in the Open-Ended Working Group (2021-25) on security of and in the use of information and communication technologies created by UNGA Resolution 75/240, as well as in the discussions within the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes.

Brazil has been the first country in Latin America to officially publish its views on the applicability of international law in cyberspace. How can Brazil advance in the implementation of the norms agreed in the GGE?

The first step is to reflect those norms and principles in the domestic cybersecurity policies. Secondly, the responsible Governmental institutions can also enforce them in their relationships with the private sector as well as civil society and academia. To a large extent, this task boils down to further fostering a cybersecurity culture in the country, which is a long-term undertaking.

Since the start of the COVID-19 pandemic, Ministries and other government bodies have suffered multiple cyberattacks, including ransomware. Threats that might have seemed distant are now hitting the country in new ways. How has Brazil responded to these emerging threats?

Brazil has undertaken several measures to address those challenges, such as, the strengthening of defence capabilities in the public networks, particularly in the national critical infrastructures; fostering cybersecurity by design; supporting capacity building initiatives; reinforcing regulatory frameworks and institutional capacity to prevent, investigate and prosecute cybercrime and terrorist use of ICT's in line with international law obligations. It is worth singling out last year's establishment of a steering federal network of cyber incidents.[4]

One of the pillars of Brazil's National Cybersecurity Strategy is international cooperation. How can countries in Latin America and in the Global South enhance cooperation in cybersecurity? Any best practices from other areas of international cooperation you would highlight?

Latin American countries share many challenges in cybersecurity with their peers in other regions of the Global South. There is therefore a great potential to shore up cooperation platforms among those countries in areas such as capacity building and sharing information on best practices, experiences and expertise among all relevant stakeholders, including from industry and civil society/academia. I believe that the regional networks of Computer Emergency Response Teams (CERTs) [e.g. CSIRT Americas, TF CERT, FIRST and others] provide a good example of effective cooperation. ■

Endnotes

[1] https://doi.org/10.1590/0034-7329201600111.

[2] https://www.sipa.columbia.edu/sites/default/files/20-RibeiroRosa_GlobalInternetGovernanceBrazil_WorkingPaper.pdf

[3] https://ciberseguranca.igarape.org.br/en/ecosystem/

[4] https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2021/07/governo-cria-a-rede-federal-de-gestao-de-incidentes-ciberneticos

Louise Marie Hurel S. Dias is a PhD Researcher in the Department of Media and Communications at the LSE and her research focuses on expertise, cybersecurity incidents, risks and cultural perspectives to security. Louise Marie is also Special Digital Policy Advisor at Igarapé Institute's Digital Security Programme, a think-and-do-tank based in Brazil.

Personal website: www.louisemariehurel.com

LSE IDEAS
9th Floor, Pankhurst House (PAN)
Clement's Inn Passage
London WC2A 2AZ
United Kingdom

+44 (0)20 7849 4918
ideas@lse.ac.uk
lse.ac.uk/ideas