Routledge
Taylor & Francis Group

The International Spectator
Italian Journal of International Affairs

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rspe20

Interrogating the Cybersecurity Development Agenda: A Critical Reflection

Louise Marie Hurel

To cite this article: Louise Marie Hurel (2022) Interrogating the Cybersecurity Development Agenda: A Critical Reflection, The International Spectator, 57:3, 66-84, DOI: 10.1080/03932729.2022.2095824

To link to this article: https://doi.org/10.1080/03932729.2022.2095824

Published online: 24 Aug 2022.

THE INTERNATIONAL SPECTATOR
2022, VOL. 57, NO. 3, 66–84
https://doi.org/10.1080/03932729.2022.2095824

Istituto Affari Internazionali
Routledge
Taylor & Francis Group

ESSAY

Interrogating the Cybersecurity Development Agenda: A Critical Reflection

Louise Marie Hurel

London School of Economics and Political Science

ABSTRACT

The intertwinement between innovation, the expansion of digital technologies and insecurity has contributed to the surfacing of concerns related to the development of cyber capacities and capabilities, that is, having the means to respond to cyber insecurity through the mobilisation of technological, human, strategic and economic resources. While some scholars have engaged critically with the concept of 'cyber capacities', most of the literature remains associated with the consolidation of a positive agenda on the topic. Drawing on literature from International Relations, international political economy and development studies, an analysis is offered of the formation of an international development agenda for cybersecurity, looking specifically at the consequences of the articulation of the concept of cyber capacities (what is necessary, acceptable, desirable and innovative in responding to cyber threats) as a key driver for setting particular visions for what 'being capable' and 'developed' is. This also contributes to a critical assessment of the inequalities and power asymmetries embedded in such development projects, with a particular focus on Global South countries.

KEYWORDS

cyber capacity-building (CCB); cybersecurity; development; critical cybersecurity studies

The expansion of Information and Communication Technologies (ICT) since the 1960s has been marked by the emergence of new threats, such as cyberattacks. A response to increasing cyber insecurity has required the development of cyber capabilities, that is, the mobilisation of technological, strategic and economic resources. Some countries have been at the forefront of developing national mechanisms for responding to these threats. These mechanisms include, but are not restricted to, passing data protection laws that provide breach notification requirements, establishing national computer security incident response teams (CSIRTs), launching a national cybersecurity strategy, having well-protected infrastructures, fostering investment in research and development for cybersecurity and digital transformation, and the list goes on.

As cyberattacks and other incidents helped propel cybersecurity into national agendas across different countries, new frameworks, methodologies and models also emerged to qualify and quantify what kinds of expertise, best practices, institutional arrangements

CONTACT Louise Marie Hurel l.h.dias@lse.ac.uk @LouMarieHSD

and policies would be required to ensure that countries are prepared to deal with a dynamic threat landscape. Two emblematic cases at the international level are the International Telecommunication Union's Global Cybersecurity Index and the Oxford Cybersecurity Capacity Maturity Model. Both are cyber capacity-building (CCB) models that have been widely referenced and have contributed to the process of ranking and/or measuring capacities of national governments. While these metrics often play an important part in mobilising political agendas and resources for cybersecurity, they are not produced in a vacuum. Discourses around preparedness, maturity, resilience and response to these cyber insecurities need to be examined not only in their intent of achieving 'better cybersecurity' or producing indicators for doing so; rather, they can serve to open up a critical theoretical reflection on how development is framed and established in this field and what kinds of power relations it maintains (McEwan 2019).

Notions of development are positioned against a wider backdrop of ongoing political and economic cybersecurity challenges at the international level. Discourses concerning cyber threats, for example, have been considerably marked by offensive/defensive narratives revolving around a small group of 'big players' such as the United States (US), China and Russia. Such discourses also point to an economy of private actors that are directly invested in securing, maintaining and 'solving' cybersecurity issues through their services: an economy that has been criticised for focusing on a small group of countries (China, Russia, Iran, North Korea) and state-sponsored activities (Oosthoek and Doerr 2021). Many of these companies, such as Microsoft, Mandiant, SentinelOne, CrowdStrike and others, are based in the 'Global North' (Hurel and Lobato 2021). However, countries in Latin America and Africa might not be that concerned with the latest Advanced Persistent Threats (APT) but with combatting everyday cybercrime and competing priorities such as economic stability, for example (Muggah and Thompson 2018; Kshetri 2019; Hurel 2022). One of the key arguments for the differences in the respective threat landscape between 'big players' and developing countries is that economic instability, high unemployment and low wages can often serve as contributing factors for individuals in developing countries to feel attracted to cyber-criminal activities (Kshetri 2010). These and other illustrations highlight the economic and political considerations that shape notions of 'cyber threats' from the perspective of the 'most capable countries' and how this contributes to crystallising certain ideas about cyber powers vis-à-vis 'others'.

Far from conclusive, these geopolitical and economic dynamics of cybersecurity often leave little space for considering the values, interests and assumptions embedded in the construction of 'cyber capacities'. The more connected countries in the Global South become, the greater are the pressures for them to have the capacities to deal with cyber threats and other digital harms. Against this backdrop, this essay draws on literature on cybersecurity, International Relations and development studies to discuss the notion of cyber capacities (what is necessary, acceptable, desirable and innovative in responding to cyber threats), that is, its emergence as a global development agenda as well as its consequences for developing regions. As Andrea Calderaro and Anthony Craig (2020) highlighted, international cooperation in the cyber domain needs to go beyond the Global North in order to develop a coherent and coordinated transnational approach to cyber governance. While CCB has consolidated itself as a key concept underpinning a global developmental agenda for cybersecurity, little reflection has been given

to the literature on development and inequalities. Indeed, the CCB agenda has been largely portrayed as a progressive and positive agenda by both scholars and practitioners. Patryk Pawlak and Panagiota-Nayia Barmpaliou (2017), for example, note that divergent understandings of 'cybersecurity' and 'capacity-building', political interests in steering investments and the multiplicity of actors and channels through which implementation and design of CCB take place have led to fragmentation of efforts. Nonetheless, Pawlak and Barmpaliou's paper remains committed to developing a sustainable perspective to addressing the 'cybersecurity gap' between Global North and South. While policy-relevant, such an approach leaves little space for questioning the basic assumptions underpinning the construction of a 'gap', the alleged lack of capacity and the instruments that are devised to respond to and address these 'gaps' by global and regional agendas.

With that in mind, this essay engages, first and foremost, in a theoretical endeavour. It seeks to contribute to a critical assessment of the cybersecurity-development nexus by examining literature from development studies that draws from post-colonial and decolonial critiques as well as literature on cyber capacity-building. In so doing, the article also hopes to contribute to the widening of cybersecurity studies both in terms of the theoretical lenses used to approach the taken-for-grantedness of security issues in their economic/developmental dimensions and of trying to move beyond and/or contest views that depart from the universalised 'North' or 'West'. In other words, it aims to engage in an exercise of destabilising some of the narratives that have been consolidated around 'good' cybersecurity and a turn to questions of 'who do they favour' and 'who do they pressure'. This essay should be regarded as an invitation and a provocation to widen the literature on cybersecurity and reflect on existing (and alternative) cooperation frameworks in and from 'the South'.

In this effort, the article is structured as follows. The first section provides a literature review of the concept of 'capacities' as part of a global development agenda. In the attempt to create a dialogue between the existing development-focused and the emerging cybersecurity literature, the second section unpacks the development of a global CCB agenda and discusses the inner workings of CCB by examining two of its dimensions: measurement and norms diffusion. The former refers to the circulation and consolidation of 'capacity-building' across multilateral and multi-stakeholder fora, the latter to the consolidation of cyber capacities as objective and normative indicators (measurements) of inequality, progress and gaps. Arguably, these political and economic dynamics of CCB continue to reproduce inequalities between the Global North and the Global South. The third section points to pathways for rethinking CCB in the Global South, followed by a conclusion.

The multiple origins and contestations of capacity-building

Historically, capacity-building has been an important concept for international development, and one that cuts across cybersecurity, sustainable development, climate change, maritime governance, peacekeeping (Bueger *et al.* 2020) and other areas. Capacity-building has been a preferred solution by policymakers and experts working with development across different transnational challenges. It has been portrayed in international and national agendas as a 'lighter touch' to assistance or a 'less political' alternative to more traditional approaches such as state-building, development assistance (Webster

2009; 2011), peacebuilding (Donais 2009) or security sector reform (Denney and Valters 2015; Bueger and Tholens 2021).

The concept of capacity-building emerged after World War II. Throughout the 1950s, the UN Technical Assistance Administration (TAA) "was a hub for social democratic experts concerned with the importance of planning for economic development" (Webster 2011, 249). In the context of decolonisation across Africa and Asia, terms such as 'technical assistance' – a precursor to 'capacity-building' – seemed like a non-colonial way of approaching development, given the focus on skills-building. The term came to prominence in Harry Truman's Point Four Program on US foreign relations. One of the objectives of the programme was to modernise underdeveloped countries by sharing expertise, capital and technology (US 1949; Webster 2011). Most of the funding from the Point Four Program went to bilateral foreign aid, while other parts were directed to support the United Nations' (UN) work on technical assistance.

As many scholars have argued, Truman's Program did much more than just create the promise of assistance, it created 'underdevelopment' and with it a subordinate position. It operated as a "mantle for sanctifying all kinds of interventions in the name of higher goals" (Esteva 2018, 2). It created a centre-periphery relation in the global economy and order, whereby underdevelopment became "considered a creature of development, or rather, as a consequence of the impact of the technical processes and the international division of labour commanded by a small number of societies" (Furtado 1970, xvi).

Even though the TAA ceased to exist at the end of the 1950s, the development agenda continued to expand and favour new forms of thinking to communicate the need for targeting specific 'capacities' and to establish thematic agendas for economic and social growth. Following the end of the Cold War, the UN adopted Agenda 21 at the United Nations Commission on Environment and Development 'Earth Summit' held in Rio de Janeiro in 1992; the document dedicated a chapter exclusively to "capacity-building", defining it as activities that encompass "the country's human, scientific, technological, organizational, institutional and resource capabilities" (UN 1992).

Despite the fact that the Agenda 21 meeting had been held in the Global South and that its aim was to propose a more sustainable and inclusive development agenda, critical perspectives on the Agenda highlight that it was successful in "selling a concept of sustainable development which continues to promote the Enlightenment goals of progress through economic growth and industrialisation at all costs" (Doyle 1998). Throughout the years, the UN's conferences on sustainable development continued to use the term to refer both to a problem that needs to be addressed and to a tool for implementing development. Recent developments, such as the 2030 Agenda for sustainable development, for example, have introduced a broader definition of capacity-building that encompasses North-South, South-South and triangular cooperation as part of the implementation of the Sustainable Development Goals (UN 2015).

In addition to a gradual shift in language, non-governmental actors have also become increasingly present in shaping the international agenda on capacity-building. This is particularly the case for cybersecurity, where organisations, think tanks and companies have assumed a role in providing capacity-building either through training, development of frameworks or funding. Initiatives range from multi-stakeholder platforms such as the Global Forum on Cyber Expertise (GFCE) to companies engaging in more traditional aid through 'tech for good' projects – one example being Microsoft's 2017 five-year

partnership with the UN Human Rights Office that included services that ranged from dashboards to track rights violations to outreach campaigns (Microsoft 2017). Lynne Phillips and Suzan Ilcan (2004, 397-8) note that these cooperative ties "may well reflect an emerging relationship between public and private under neoliberal governance, wherein the boundaries become blurred". Capacity-building thus becomes a complex interplay between both governmental and non-governmental actors that are, from a financial, political, technical and an expertise standpoint, able to support the identification or development of targeted sites that need 'building'.

What these and other histories illustrate is how the concept of 'capacity-building' is intimately connected not only to the consolidation of development agendas in their international and institutional sense, but also to specific capital flows between North and South countries as well as being associated with a host of similar terms (such as technical assistance, expertise and knowledge). The objective here was not to discard the concept, but to revisit the contentious and complex histories through which it emerges in different forms and across multilateral debates.

The emergence of CCB agendas

In its most literal sense, the term 'capacity' refers to being able to do, or being capable of dealing with, something. More broadly, "capacity-building" has been used interchangeably with "capacity development" (Venner 2015); it has been defined as "a serious-sounding alternative to training" (Eade 2007, 631–2) and as a "more technical" alternative to aid and other terms that reflect colonial and asymmetric dynamics (Bueger and Tholens 2021). When linked with cybersecurity issues, 'capacity' has been associated with having the resources to build institutional capacities, the maturity to deal with emerging threats, the skills within the national workforce, and the strategies and technologies in place to respond to incidents in a timely and coordinated manner. On the one hand, these capacities have been commonly linked to development contexts and capabilities (Pawlak 2016; Calderaro and Craig 2020; Collet 2021); on the other hand, they have also been associated with military capabilities (Egloff and Shires 2021). Overall, both capacities and capabilities can be used interchangeably to refer to 'being able' to conduct and maintain a 'good' cybersecurity.

Capacity-building has been systematically introduced as a familiar term to international cybersecurity agendas throughout the years. Scholars, however, have noted that one of the main challenges for CCB practice is that, instead of creating a broader agenda, it has resulted in a "patchwork of efforts, methodologies, principles, mandates and organisations" involved in designing, planning and implementing CCB (Pawlak and Barmpaliou 2017, 126).

As mechanisms, policies, metrics and strategic priorities started being devised by many countries, so did expectations as to what was needed to secure and protect populations and economies from impending cyber threats. Many scholars have highlighted how, in the early 2000s, cybersecurity became an often securitised and militarised subject (Dunn Cavelty 2008; 2013). This securitisation of cybersecurity enabled many countries to concentrate resources on the development of military capabilities, consolidation of cyber commands and strategic policy documents. This was the period – and more specifically the 2010s – when the US established its Cyber Command. During

that same time, countries such as Brazil also benefitted from the concentration of resources in the Ministry of Defence and the political will to push for including cyberspace as one of the strategic domains for national security. This movement enabled the country to also set up its own cyber command and cyber defence doctrines (Hurel and Lobato 2018; Hurel 2021). Another example is Colombia, which also started building its own capacities through the adoption of a defence-oriented national cybersecurity strategy back in 2011 (CONPES 2011). However, while there was a greater emphasis on national security concerns associated with cyberspace back then, cybersecurity also became increasingly attached to national development agendas, often reflected in digital transformation/digital innovation strategies that sought to consolidate a less militarised vision and allocate resources to foster innovation and address digital risks more broadly (OECD 2015; Chenou 2021). Internationally, organisations like the UN, regional bodies such as the Organisation of American States and the Organisation for Security and Cooperation in Europe, and multi-stakeholder initiatives such as the GFCE, among others, have devised CCB efforts to tackle emerging cybersecurity threats.

While there are multiple potential histories to the emergence of CCB, international organisations such as the UN started approaching the subject in the early 2000s. In 2003, the General Assembly approved a resolution on the "Creation of a Global Culture on Cybersecurity" (UN 2003). While it was not the first resolution to specifically address cybersecurity or cybercrime, it was nonetheless an important landmark as it linked cybersecurity concerns with broader discussions on the information society. The approval of the resolution took place in the same period as the preparations for the World Summit on the Information Society (WSIS) that would later lead to the consolidation of the Tunis Agenda focusing on sustainable development and governance of the Internet. One of the objectives of resolution A/RES/57/239 was to invite member states to consider the need for a global culture in the WSIS process and thus help governance, security and development converge. However, one point that is often neglected is that the resolution dedicates a specific section to capacity-building, which "*stresses* the necessity to facilitate the transfer of information technology and capacity-building to developing countries, in order to help them to take measures in cybersecurity" (UN 2003, 2). In documents such as these, capacity-building refers less to technical assistance than to the need to transfer knowledge and information to developing countries. Yet, while states agree that CCB is essential, little is still known as to what this means in practice.

In order to analyse how CCB has been used as a policy tool for cyber development, two aspects will be analysed in the following: *measurement* and *norms diffusion*. This will be done by tapping into some of the inner logics that underpin knowledge about CCB and the themes and mechanisms associated with it: namely, logics of *objectivity*, *socialisation* and *othering*. Methodologically, the findings are a result of the analysis of reports, resolutions, transcripts, blog posts and pages from international and regional organisations working in this field. Furthermore, having been actively engaged in multiple discussions and conferences on such topics, I also draw on participant observation across a range of international and regional fora. In this regard, having had access to these spaces and discussions positions me not as a distant observer but as a researcher navigating complex intersections of political, economic, geographic and gendered dynamics in this field.

Operationalising capacities: measuring inequality and creating a market

Different instruments and frameworks[1] have been devised to assess 'capacity', 'maturity', 'power' and 'capability' of states by establishing quantitative and qualitative variables for measurement. With the aim of evaluating how capacities are shaped through measurements and what kinds of knowledge these measurements produce that in turn enable and/or constrain CCB activities, this section reviews two mechanisms that have been widely referred to and used for measuring countries' capacities, namely: the Oxford Cybersecurity Capacity Maturity Model (CMM) and the International Telecommunications Union Global Cybersecurity Index (ITU GCI). Both mechanisms play a significant role in operationalising and socialising capacity-building as an ultimately objective process, whereby a country is ranked or properly evaluated according to specific metrics. The results help to map gaps, strengths and particularities of a country. This section unpacks the *logics of objectivity* that operate through maturity measurements and the political effects of these tools for stabilising development narratives.

Established in 2014 by the Global Cyber Security Capacity Centre (GCSCC) at the Oxford Martin School, the Oxford Cybersecurity Capacity Maturity Model is, as the name suggests, a methodological framework designed to review a country's cybersecurity capacity. The CMM has been incrementally developed since then through focus groups, thematic coding, desk research, expert consultations (from different sectors) and many other methodological approaches for framework development. From 2015 to October 2021, the CMM was deployed in over 87 countries together with strategic implementation and regional partners. As Table 1 shows, the CMM has five general dimensions that "constitute the breadth of national capacity that a country requires to be effective in delivering cybersecurity" (GCSC 2022a, 5). The model also provides five stages of maturity "from which a country can improve or decline depending on the actions taken (or inaction)", ranging from "start-up stage" (lowest level) to "dynamic stage" (highest level).

Indeed, the first way in which a logic of objectivity operates is through measurement. In becoming measurable, cyber capacities also become objective and normative measurements of inequality, progress and gaps. Amartya Sen (2001) notes that the measures of inequality in economic literature fall broadly into two categories: one where inequality is measured in an *objective* manner, that is, through the deployment of quantitative methods, statistical models and analyses that can, for example, identify variations in income; and another that tries to capture inequality in *normative* ways, such as using social welfare as an indicator and measurement. These measurements, not only in economic terms but also in areas such as cybersecurity, can be advantageous as they allow countries and experts to identify levels of inequality and establish specific values for normatively assessing them. Therefore, following Sen's approach, the development of models for measuring capacities is not problematic *per se*, as an act of measuring. The challenge is when these measurements are taken and used as an *objective* measure that, while value-laden, is supposedly 'technical' and 'non-political', 'neutral'. In this

[1]There are many ways through which the private sector has sought to measure capacities. These include risk assessments and measurements that allow for better monitoring of best practices in place. Other practices, such as the designation of CISOs (Chief Information Security Officer) and the development of professional certifications, have become accepted standards for measuring the 'global cyber workforce' or a company's maturity, for example.

Table 1. Dimensions for measuring cyber capacity-building: Oxford Cybersecurity Capacity Maturity Model

Dimensions	Description
Policy and Strategy	Explores the country's capacity to develop and deliver cybersecurity strategy, and to enhance its cybersecurity resilience by improving its incident response, cyber defence and critical infrastructure (CI) protection capacities.
Cultural	Reviews important elements of a responsible cybersecurity culture such as the understanding of cyber-related risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online.
Capacity-building	Reviews the availability, quality and uptake of programmes for various groups of stakeholders, including the government, private sector and the population as a whole, and relate to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes and professional training programmes.
Legal Framework	Examines the government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation and related legislation.
Standardisation and Technologies	Examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

Source: author's adaptation from GCSCC (2022b).

perspective, these sets of measurements can be replicated, applied and reapplied to starkly different contexts only to provide an account of the 'state of the art', or a map of capacities, without a reflection on their consequences in implicitly supporting a targeted approach to CCB, for example.

In Latin America, Brazil has been the only country with an exclusive CMM analysis, while analyses of other countries in the region have been included in publications by the Organization of American States (OAS) and the Inter-American Development Bank (IDB) (IDB and OAS 2016; 2020). Countries such as Colombia have mentioned the CMM assessment as a key reference for the development of their national digital security strategy for the electricity sector. What is more, the document uses the metrics in the CMM to make a comparative analysis of major economies in the region, namely, Brazil, Chile and Mexico (CREG 2019). In Brazil's case, the assessment was referenced in the country's National Cybersecurity Strategy, which explicitly mentions that the CMM dimensions served as a baseline for the development of the country's own strategic pillars (see E-Ciber 2020). These examples highlight how the use of frameworks for capacity assessment travels through national documents and how the principles and normative commitments that informed the development of the CMM are appropriated as a tool for national awareness of one's own 'maturity status' vis-à-vis other countries.

However, while measurements via CCB indexes and models provide a detailed account of how countries have been approaching cyber capacities, it is important to reflect on the consequences, politics and transformations that derive from the introduction of these knowledge-production projects that become frameworks for measuring development. One of the by-products of the logic of objectivity is the desire and an immediate demand that this type of measurement produces as it engages in the exercise of mapping gaps in capacities. From a policy perspective, such a measurable by-product is precisely the goal to be achieved, but a critical development perspective shifts the focus to *what* and *who* created that desire as well as the consequences of these knowledge-production frameworks. As Wolfgang Sachs (2009, viii-ix) argues, the idea of

development is charged with hopes and self-affirmations. "The desire for recognition and equity is framed in terms of the civilizational model of the powerful nations, the South has emerged as the staunchest defender of development. Countries in general do not aspire to become more 'Indian', more 'Brazilian' […] they long to achieve industrial modernity".

As Brazil's and Colombia's cases illustrate, these measurements provide a diagnostic perspective of not being prepared and not having enough capacities. The challenge here is not one of critiquing the use of such measurements in isolation – as they have provided significant knowledge about national contexts – but of proposing that critical cybersecurity scholarship needs to ask questions about how these cybersecurity frameworks developed in the Global North become entangled with the realities and discourses in the Global South: they are a universalised tool produced in the North that is territorialised in the South, reproducing notions of development though ranking and measurement of gaps. Ramón Grosfoguel (2000) notes, in conjunction with a considerable group of scholars that range from black feminists to Global South researchers, that the universalistic, neutral and objective point of view is the world-system, and that there is no escaping power structures (Mignolo 2000). "The western is a point of view that does not assume itself as a point of view" (Grosfoguel 2009, 11). This is not to say that consultations with practitioners and scholars from the Global South are not considered in methodologies such as the CMM, but that there ultimately is a positionality, a base from which such measurements occur. Even though this might change as CMM deployment expands, the list of 87 countries covered at the time of writing shows a considerable focus on developing countries (with a few exceptions, such as the United Kingdom and Switzerland). Even in Europe, the list of countries assessed are mostly in Eastern Europe. The South, in particular, becomes the territory of application of such measurements: it is the space, or the 'other', that needs to be better understood and mapped. To be sure, these studies are conducted in agreement or cooperation with local governments, which means that development is not only an externality: measurement and evaluation are indeed desired and perceived as a means of self-awareness (Cowen and Shenton 1996). The logics of objectivity, rooted in these measurement practices, are thus connected to a *logic of othering*; the other needs to be 'know-able' not only to be self-aware of its own condition (that is, more or less mature according to the pre-defined indicators) but also to become known and identifiable as a target for future funding.

Each model for measurement performs differently and has specific consequences for the knowledge produced and reproduced across countries. While the CMM's objective is to review a country's cybersecurity capacity with the aim of mapping effectiveness of delivery of cybersecurity, the ITU's Global Cybersecurity Index (GCI), being an index, is more explicit about its intent to measure. Established in 2015, the objectives of the GCI are "to measure":

- The type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- The progress in cybersecurity commitment of all countries from a global perspective;
- The progress in cybersecurity commitment from a regional perspective;
- The cybersecurity commitment divide (i.e. the difference between countries in terms of their level of engagement in cybersecurity initiatives) (ITU 2022a).

One of the recurring goals of the GCI (Table 2) is to measure progress and to assist countries in "identifying areas for improvement in the field of cybersecurity and encourage them to take action towards those areas". As ITU (2022a, 130) notes: "This would also be the opportunity to helping to raise the overall level of cybersecurity commitment worldwide, harmonizing practices and fostering a global culture of cybersecurity. The GCI aims to illustrate successful examples in cybersecurity that might serve as good practice and guidelines to countries with similar national environments." In this regard, the GCI is presented as a global tool for insight designed to inform capacity-building strategies and provide key criteria through which local practices can be harmonised with global aspirations and frameworks.

Based on structured data from a questionnaire sent to national focal points – that covers 20 indicators through a set of 82 questions – the index ranks countries based on their score and provides a visual representation of each country's profile according to the distribution of scores across the five pillars of the GCI (see ITU 2022a). The GCI, as a tool from the ITU, is strategically positioned to legitimise and expose whether countries are able to meet the benchmarks set by the dimensions. As a mechanism for national assessment, the GCI seeks to provide a tool to qualify and quantify capacities. It has gained considerable recognition from countries and, as will be illustrated later, became a point of reference for state and non-state actors alike. The challenge is that it can result in countries looking to 'tick the box' instead of reflecting on what variables might best fit their cultural contexts. For example, having official documents such as a national cybersecurity strategy or conducting public consultations in the process of its development does not necessarily mean that such strategy has a clear implementation plan, that consultations ultimately guarantee multi-stakeholder participation in the consolidation of a national vision for cybersecurity or even that there is democratic oversight

Table 2. Dimensions for measuring cyber capacity-building: ITU's Global Cybersecurity Index

General pillars	Definition and sub-indicators
Legal	Measures based on the existence of legal frameworks dealing with cybersecurity and cybercrime *Sub-indicators*: cybersecurity, cybercrime, critical infrastructure data protection legislations
Technical	Measures based on the existence of technical institutions and framework dealing with cybersecurity *Sub-indicators*: active CERT, engagement CERTs regionally, child online protection mechanisms, CyberDrills, implementation of international cybersecurity standards
Organisational	Measures based on the existence of coordination institutions, policies and strategies for cybersecurity development at the national level *Sub-indicators*: national cybersecurity strategy, responsible cybersecurity agency, cybersecurity metrics
Capacity Development	Measures based on the existence of research and development, education and training programmes, certified professionals and public sector agencies fostering capacity-building *Sub-indicators*: public cybersecurity awareness campaigns, training for cybersecurity professionals, academic curricula development, research and development programmes, incentives for national cybersecurity industry
Cooperative	Measures based on the existence of partnerships, cooperative frameworks and information-sharing networks *Sub-indicators*: bilateral agreements, participation in international mechanisms, cybersecurity multilateral agreements, Public-Private Partnerships, inter-agency partnerships

Source: author's adaptation from the 2021 version of the Global Cybersecurity Index (ITU 2022a; 2022b).
Note: the author reviewed all GCI Editions but focused on using the table as a representation of the latest set of indicators. In the review, particular attention was given to the methodology and questionnaires. Examples of sub-indicators were more clearly communicated in previous editions; however, the author used the 2021 questionnaire as a basis for outlining the recent sub-indicators as well as the sub-sections designated for each pillar throughout the report.

over the development process. That is the case for Brazil, which jumped from 70th in the 2018 global ranking to 18th in 2020 (ITU 2019; 2022a) especially due to the approval of several norms, including its cybersecurity strategy. While the overall GCI score paints a positive picture – and indeed, one might argue that, from a normative point of view, the country has progressed – it does not account that, for example, the period of consultations for the development of Brazil's national cybersecurity strategy was open to the general public for less than 15 days, considerably shorter than regular legislative/normative consultations that last at least 30 days or that the national cybersecurity strategy is not an implementation-focused document. The challenge is thus less one of criticising the mechanism itself, but understanding the shortcomings and consequences it produces across national environments.

Even so, despite the alleged 'technical' nature of the priorities prescribed by models such as the GCI, cyber capacities are a realm of global contestation over priority areas that require further investment from the state. Nonetheless, dominating views and mechanisms that help shape political agendas tend to present themselves as universalistic. In the case of the GCI, the fact that it is implemented by the ITU reinforces its international reach and applicability. While important in capturing governments' attention and pushing the political agenda towards better cybersecurity, the different metrics developed to measure cyber maturity, power and insecurity may have problematic aspects. In pushing for a comparative overview, the ranking of states also produces a measure that is made ready for policy justifications and discourses around progress/underdevelopment. In that sense, *measuring* also perpetuates a logic of security haves and have-nots, cans and can-nots in global cybersecurity politics, and the hope that 'gaps' will be addressed and acted upon.

Establishing normative expectations: norms diffusion and the consolidation of CCB

CCB, both as a term and as a global agenda, transcends the UN's developmental focus, having instead to be read as part of the cybersecurity-development nexus. This is supported by the emergence of cyber norms that seek to outline common expectations from states and non-governmental stakeholders regarding best practices and responsible behaviour in cyberspace. In doing so, CCB is presented as a central component to ensure peace and stability in cyberspace that enables countries and non-governmental actors to implement norms and define expected standards of behaviour that can only be achieved if these actors have the capacities to do so. As Martha Finnemore and Duncan Hollis note (2016, 427), "norms are social creatures that grow out of specific contexts via social processes and interactions among particular groups of actors". In addition, scholars have noted that global cyber norms presuppose the capacity of states to implement them, which then turns CCB into a necessary tool for the implementation of such norms and a way to bridge existing inequalities in ICT development (Homburger 2019). In this regard, CCB becomes entangled to the production of normative agendas while these agendas simultaneously stabilise CCB as a prerequisite for norms implementation – thus attaching cyber norms to an underlying concern with capacities development. As this section will illustrate, CCB has become a taken-for-granted element in cybersecurity development, encoded in multiple cyber norms processes. What kinds of understandings of CCB are being socialised at the international level?

Many state and non-state actors have gradually devised different sets of norms outlining cybersecurity best practices that stakeholders should uphold.[2] International cyber norms have been traced back to the late 1990s with the establishment of the UN Group of Governmental Experts (GGE) on the Developments in the Field of Information and Telecommunications in the Context of International Security. The GGE norms agreed in 2013, 2015 and 2021 provide a set of expectations regarding the behaviour and preparedness of states in securing their own infrastructure. That is the case, for example, for the principle of *due diligence*, whereby states should not allow their territory to be used for an internationally wrongful act. In international law, due diligence is associated with rules that impose obligations on states regarding their conduct in stopping, preventing or redressing transnational harms and risks. It presupposes, to some degree, that states can protect their ICT infrastructure and can thus demonstrate their attempts to perform their duty to protect. The socialisation of expected conducts and responsibilities through cyber norms feeds into the expansive logic of CCB as something that underpins norms achievement.

In the 2013, 2015 and 2021 GGE reports, reference to the term 'capacity' increased considerably with each iteration (12, 22 and 31 occurrences, respectively). As for the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG)[3], reference to 'capacity' is equally frequent, given that this was the first report of the process (33 mentions in total). In terms of content, the 2013 GGE report (GGE 2013) dedicates a specific section to recommendations for capacity-building measures. It emphasises the importance and directionality of capacity-building efforts towards developing countries and how such countries would benefit from the consolidation of channels for requesting assistance. Lacking capacities or being less prepared to deal with vulnerabilities is also framed as a shared concern ('problem for all') against which 'measures' must be taken through better CCB in technical and legal cooperation. The 2015 report goes on to frame CCB as "essential for cooperation and confidence-building" (GGE 2015). The report also proposes an extensive list of agreed cyber norms and notes that "while such measures may be essential to promote an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible, in particular for developing countries, until they acquire adequate capacity" (8). In this regard, the report recognises the pressure and positionality of developing countries in a race to develop capacities while acknowledging that these disparities are a shared concern that, if left unaddressed, could undermine peace and security in cyberspace.

Both the 2021 GGE and OEWG reports take a step further and explicitly recognise the cross-cutting role of capacity-building as a pre-condition for cyber norms implementation. In particular, the GGE report mentions capacities with reference to the constraints some countries face in the implementation of the agreed norms. These include, for example, a caveat that while states should not knowingly allow their territory as the

[2]For example, the Best Practice Forum on Cybersecurity of the Internet Governance Forum outlined a list of 35 cybersecurity agreements since 2009 (BPF 2021). The list does not seek to exhaust the diversity of norms and agreements, but it does provide a geographical distribution of norms featuring a multi-stakeholder approach.

[3]The OEWG was established in 2019 with the purpose of developing the rules, norms and principles of responsible behaviour of states, discuss pathways for their implementation and evaluate the possibility of consolidating regular institutional dialogue under the auspices of the UN.

base for internationally wrongful acts using ICTs, if a state is aware of its own lack of capacity to address such acts in its territory, it "may consider seeking assistance from other States or the private sector" (10). In this regard, capacities are not only recognised as a challenge for the implementation of cyber norms and international law, they also operate as a justification for (i) states struggling to implement norms as well as (ii) requesting assistance.

The 2021 OEWG report, instead, is more explicit regarding the purpose and form for CCB, highlighting that CCB should be sustainable, demand-driven, aligned with national priorities, tailored to specific contexts, respecting the principle of state sovereignty and "undertaken in full recognition of national ownership" (OEWG 2021, 8). Most of the language used to address CCB is more reflective of the concerns of developing countries – partly because of the broader scope of the OEWG's mandate and of its inclusion of all UNGA (United Nations General Assembly) member states in contrast with the UNGGE, limited to 25 experts and the chair.

Countries in the Asia-Pacific region and in Africa drafted their own normative commitments, some examples of which are the 2009 Shanghai Cooperation Organisation agreement on cooperation in the field of ensuring the international information security and the African Union Convention on Cybersecurity and Personal Data Protection from 2014. In the Americas, the OAS Inter-American Committee Against Terrorism (CICTE) has been one of the main bodies working to promote CCB efforts both regionally and bilaterally with member states, also directly providing technical assistance such as supporting the development of national cybersecurity strategies, enhancing cooperation among Computer Emergency Response Teams (CERT) within the region (CSIRT Americas initiative), promoting events and deploying targeted programmes directed at building cyber capacities of women professionals and diplomats (IDB and OAS 2020).

These and other examples illustrate how references to capacity-building flowed through different discussions focusing on cyber norms and across different multilateral and multi-stakeholder fora. However, the *logic of socialisation* is one of eventually generating commitment from all countries in incorporating and publicly endorsing the role of CCB as a key to development and norms implementation. How such a commitment is to be achieved becomes the crux of the logic of socialisation. For countries to advance on a more thorough interpretation of the GGE 2021's vision of capacities, for example, a continuous commitment from states is required in publishing their views of how international law applies to cyberspace, going beyond the 25 GGE member countries to a wider commitment from other developing states.

Rethinking knowledge production in CCB through South-South relations

At the heart of the contested nature of cyber capacities lies a deeper and more complex struggle for legitimacy and agency that is intimately related to a process of drawing boundaries, of othering and of determining what kinds of knowledge about cybersecurity are deemed acceptable and valid. As highlighted in the previous sections, CCB does not emerge in a vacuum; it is a term that has been historically linked to specific conceptions of development that have circulated since the 1950s. CCB is taken as a technical and, at times, value-laden term of reference in cyber norms, which is operationalised through different measurement strategies. These strategies (ranking or modelling) seek to

objectively measure inequalities – thus feeding into global, regional and national problem-solving agendas aimed at dealing with the 'gaps' identified. What is more, CCB, as with previous references in the broader development field, presents itself as an uncontested truth – after all, why would any country contest the need to improve its own capacities? The problem, however, is that the language and discourse around CCB imply a transactional relationship between developed and developing countries whereby not only values (norms, legal frameworks) and funding (donor-recipient relations) can and should be transferred from the former to the latter, but also cyber governance models (modes of governance) attached to these capacities (Homburger 2019).

Latin America, and the countries therein, are marked by a history of violent colonialism that enabled Europe to position itself at the centre of what would be conceived as a modern international system (Wallerstein 2003; Quijano and Ennis 2000). These dynamics of othering of Latin America have been continually perpetuated through understandings of economic progress as being separated between a centre and periphery (Dos Santos 2000). They have enabled new forms of control and power through modern agendas such as science, technology, globalisation and, more recently, knowledge about cybersecurity. As part of the 'Global South', these countries are also implicated, as Caroline Levander and Walter Mignolo (2011) suggest, in ordering and disordering what that term means. In this respect, CCB, as a positive agenda for development and change, is part of dis/ordering the place of the Global South. It provides metrics and norms of expected behaviour that objectively and subjectively translate donor-recipient, North-South practices to cybersecurity.

If one considers, for example, the discussions around public attribution, scholars have already noted that private sector interests and political bias from governments can often shape and narrow the understanding of cyber conflict (Egloff 2019), either due to political incentives to do so or due to private sector incentives to over-report on specific countries that are considered 'non-democratic' (Oosthoek and Doerr 2021). The re-production of threats, rather than exceptional and exogenous, is deeply embedded in the cultural, political and economic dynamics of cyber capacities.

This is highlighted, for example, by trends underlying CCB development in Latin America. As domestic cybersecurity capacities development processes in Latin America show, there are underlying trends that characterise CCB in the region. Many Latin American countries have decided to manage their cyber affairs through intergovernmental and military-to-military diplomacy with more powerful states (Solar 2020). The institutional aspiration of Latin American elites for the models devised in the Global North shows that the ideal types, models, regulations and institutions for development reproduced in CCB can often result in significant entanglements between the North and South, between Global and Local.

Indeed, the universalising, neutralised and 'objective' narratives around CCB would benefit from expanding to South-South cooperation. While the OAS played an important role in regional CCB, historically, the broader framing of South-South cooperation marked a production of knowledge and exchange that proceeds from the standpoint of developing countries. South-South exchanges in cybersecurity can complement global debates while also departing from priorities and themes that are closer to these countries' challenges. At the same time, the 'South' should not be taken as a coherent set of countries. China, for example, is one of the biggest commercial partners to

countries across Latin America and Africa. Big tech companies such as Huawei have provided attractive financing options for providing technical assistance and infrastructure implementation in these regions (Roy 2022). Scholars have also noted that the contemporary understandings of South-South exchanges, as outlined above, differ from the political ideals and rhetoric that emerged in the context of the 1960s dependency theory, that is, one that "presented development as a state-led challenge to Northern dominance that was potentially progressive and representative" (Morvaridi and Hughes 2018, 868).

Conclusion and future directions

As seen at the beginning of this essay, the short histories of capacity-building portray a vision of a universalised and sanitised version of plans for development. That is not dissimilar to some dynamics in cybersecurity whereby commercial and international organisations seek to separate skills-building paradigms from the commercial and political interests underlying funding or framework-building strategies. As this essay illustrated, the myth of pure cybersecurity knowledge (Shires 2018) goes beyond economic interests, it also conceals the geographic and normative place from which 'golden standards' for cybersecurity are drawn and whom they target.

From a scholarly perspective, international political economy and development theories help us question the sites of threat and security production. Scholars have increasingly focused on theorising and recognising the role of different actors and materialities in the making of security (Collier 2018; Stevens 2020), but less so on interrogating the geopolitical-centrism of capacities and capacity-building. That is why this article seeks to draw attention back to the role of states and, in particular, those that are not the 'usual cyber powers'. In this article, the concept of 'capacities' is reviewed in such a way to critically approach the cybersecurity-development nexus as well as the inequalities it produces.

The discussion around cyber capacities has also to be positioned within a broader shift from globalisation to fragmentation at the international level – which means that competition over markets, votes (in international fora) and values has also intensified due to geopolitical tensions between 'Western democracies' and countries such as Russia and China. The successive effects of economic crises, the outbreak of Covid-19 and the Ukraine War have only amplified such tensions.

Global competition and fragmentation can lead to new forms of subordination in development. Discussions around cybersecurity are not exempt from these dynamics, they can become yet another stage for colonising dynamics – be them in terms of maintaining a market that is biased towards the threats that are most common to the 'Global North' (a small group of 'cyber powers') or in terms of building models and agendas that might fall short of accounting for the particularities non-'cyber powers' in the Global South.

Not considering a critical approach to development and CCB has significant policy implications: international agendas and programmes would miss an opportunity to think creatively about funding strategies and models for preventing cyber attacks. Future work on cybersecurity should consider exploring the potential for triangular and South-South cooperation in tandem with regional efforts (Association of Southeast Asian Nations, OAS and others). In addition, neither the 'South' nor the 'North' should

be seen as a coherent and singular unit. Regarding the latter, for example, there are distinct differences between the US' and the EU's approaches to capacity-building, each of which engages distinctly in reproducing specific logics of objectivity, socialisation and othering.

To conclude, this article has focused on CCB mainly from an international development perspective. As capacity-building cuts across diplomatic and civil society participation in international cyber norms discussions, future research should consider deepening the intersectional approach to CCB and unpacking specific geographical, gender and racial politics that cut across the models, development agendas, concepts and programmes shaping the future of cybersecurity. Such an effort entails a critical engagement with other disciplines in building a critical research agenda for cybersecurity studies: one that is cognisant of the different positionalities and politics embedded in the making and shaping of knowledge, capacities, as well as the economics of cybersecurity.

Acknowledgments

The author would like to thank the journal's editors, Leo Goretti and Daniela Huber, the two reviewers for their invaluable feedback, the group of contributors to this Special Core for the fruitful and thought-provoking discussion and, last but not least, Xuechen Chen and Yifan Yang for their support throughout the development of this paper.

Notes on contributor

Louise Marie Hurel is a Doctoral Candidate in Data, Networks and Society in the Department of Media and Communications at the London School of Economics and Political Science (LSE), London, United Kingdom.

References

BPF (Best Practice Forum). 2021. Mapping and Analysis of International Cybersecurity Norms Agreements. Internet Governance Forum. November. https://www.intgovforum.org/en/filedepot_download/235/19829.

Bueger, Christian, Edmunds, Timothy, and McCabe, Robert. 2020. Into the Sea: Capacity-Building Innovations and the Maritime Security Challenge. *Third World Quarterly* 41 (2): 228-46.

Bueger, Christian, and Tholens, Simone. 2021. Theorizing Capacity Building. In Christian Bueger, Timothy Edmunds and Robert McCabe, eds. *Capacity Building for Maritime Security*: 21-45. Cham: Palgrave Macmillan.

Calderaro, Andrea, and Craig, Anthony J. S. 2020. Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building. *Third World Quarterly* 41 (6): 917-38.

Chenou, Jean-Marie. 2021. The Contested Meanings of Cybersecurity: Evidence from Post-conflict Colombia. *Conflict, Security and Development* 21 (1): 1–19.

Collett, Robert. 2021. Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures. *Journal of Cyber Policy* 6 (3): 298-317.

Collier, Jamie. 2018. Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision. *Politics and Governance* 6 (2): 13-21.

CONPES (Consejo Nacional de Política Económica y Social). 2011. Lineamientos de política para Ciberseguridad y Ciberdefensa [Policy Guidelines for Cybersecurity and Cyberdefense]. CONPES 3701. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf.

Cowen, Michael P., and Shenton, Robert W. 1996. *Doctrines of Development*. London: Routledge.

CREG (Comisión de Regulación de Energía y Gas). 2019. Documento de Consulta: Estrategia Integral de Seguridad Digital em el Sector Eléctrico [Consultation Document: Comprehensive Digital Security Strategy in the Electricity Sector]. CREG-065. http://apolo.creg.gov.co/Publicac.nsf/52188526a7290f8505256eee0072eba7/b3f5512e987fd6c4052584720057e239/$FILE/Circular072-2019%20Anexo1.pdf.

Denney, Lisa, and Valters, Craig. 2015. Evidence Synthesis: Security Sector Reform and Organisational Capacity Building. London: Department for International Development & UK Aid. https://odi.org/en/publications/evidence-synthesis-security-sector-reform-and-organisational-capacity-building/.

Donais, Timothy. 2009. Empowerment or Imposition? Dilemmas of Local Ownership in Post-Conflict Peacebuilding Processes. *Peace & Change* 34 (1): 3–26.

Dos Santos, Theotonio. 2000. *Teoria da Dependência: Balanço e Perspectivas* [Dependency Theory: Balance and Perspectives]. Editora Insular.

Doyle, Timothy. 1998. Sustainable Development and Agenda 21: The Secular Bible of Global Free Markets and Pluralist Democracy. *Third World Quarterly* 19 (4): 771–86.

Dunn Cavelty, Myriam. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Abingdon-New York: Routledge.

Dunn Cavelty, Myriam. 2013. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review* 15 (1): 105-22.

E-Ciber. 2020. Estratégia Nacional de Segurança Cibernética – Decreto n.10.222, de 5 de Fevereiro de 2020 [National Cyber Security Strategy – Decree n.10.222 of 5 February 2020]. Edição 26, Seção 1, Página 6. Diário Oficial da União. https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419.

Eade, Deborah. 2007. Capacity Building: Who Builds Whose Capacity? *Development in Practice* 17 (4–5): 630–9.

Egloff, Florian J. 2019. Contested Public Attributions of Cyber Incidents and the Role of Academia. *Contemporary Security Policy* 41 (1): 55–81.

Egloff, Florian J., and Shires, James. 2021. Offensive Cyber Capabilities and State Violence: Three Logics of Integration. *Journal of Global Security Studies* 7 (1). DOI: https://doi.org/10.1093/jogss/ogab028.

Esteva, Gustavo. 2018. What is Development? *Oxford Research Encyclopedia of International Studies*. DOI: https://doi.org/10.1093/acrefore/9780190846626.013.360.

Finnemore, Martha, and Hollis, Duncan B. 2016. Constructing Norms for Global Cybersecurity. *The American Journal of International Law* 110 (3): 425-79.

Furtado, Celso. 1970. *Obstacles to Development in Latin America*. New York: Anchor Books.

GCSCC (Global Cyber Security Capacity Centre). 2022a. Cybersecurity Capacity Maturity Model for Nations (CMM). 2021 Edition. Accessed 24 June 2022. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf.

GCSCC. 2022b. The Cybersecurity Capacity Maturity Model. Oxford Martin School. Accessed 24 June 2022. https://gcscc.ox.ac.uk/the-cmm.

GGE (Group of Governmental Experts). 2013. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement.

GGE. 2015. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly. https://digitallibrary.un.org/record/799853?ln=en#record-files-collapse-header.

GGE. 2021. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement.

Grosfoguel, Ramón. 2000. Developmentalism, Modernity, and Dependency Theory in Latin America. *Nepantla: Views from South* 1 (2): 347-74.

Grosfoguel, Ramón. 2009. A Decolonial Approach to Political-Economy: Transmodernity, Border Thinking and Global Coloniality. *Kult* 6 (1): 10–38.
Homburger, Zine. 2019. The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society* 33 (2): 224–42.
Hurel, Louise Marie. 2021. Cybersecurity in Brazil: An Analysis of the National Strategy. Igarapé Institute. https://ciberseguranca.igarape.org.br/en/estrategy/.
Hurel, Louise Marie. 2022. Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America. *Global Security Review* 2 (7): 1-12.
Hurel, Louise Marie, and Lobato, Luisa Cruz. 2018. Uma Estratégia para a Governança da Segurança Cibernética no Brasil [A Strategy for Cybersecurity Governance in Brazil]. Igarapé Institute. https://igarape.org.br/wp-content/uploads/2018/09/Uma-estrate%CC%81gia-para-a-governanc%CC%A7a-da-seguranc%CC%A7a-ciberne%CC%81tica-no-Brasil.pdf.
Hurel, Louise Marie, and Lobato, Luisa. 2021. Cyber-Norms Entrepreneurship? Understanding Microsoft's Advocacy on Cybersecurity. In Dennis Broeders and Bibi van den Berg, eds. *Governing Cyberspace: Behavior, Power and Diplomacy*. 285–314. London: Rowman and Littlefield.
IDB (Inter-American Development Bank) and OAS (Organization of American States). 2016. Cybersecurity: Are We Ready in Latin America and the Caribbean? https://gcscc.ox.ac.uk/files/cybersecurity-are-we-prepared-latin-america-and-caribbean.pdf.
IDB and OAS. 2020. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe [Cybersecurity Report 2020: risks, progress and the way forward in Latin America and the Caribbean]. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe.
ITU (International Telecommunication Union). 2019. Global Cybersecurity Index 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
ITU. 2022a Global Cybersecurity Index 2020. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/.
ITU. 2022b. GCI Scope and Framework. Accessed 27 June 2022. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/New_Reference_Model_GCIv4_V2_.pdf.
Kshetri, Nir. 2010. Diffusion and Effects of Cyber-Crime in Developing Economies. *Third World Quarterly* 31 (7): 1057-79.
Kshetri, Nir. 2019. Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management* 22 (2): 77-81.
Levander, Caroline, and Mignolo, Walter. 2011. Introduction: The Global South and World Dis/Order. *The Global South* 5 (1): 1–11.
McEwan, Cheryl. 2019. *Postcolonialism, Decoloniality and Development*. London-New York: Routledge.
Microsoft. 2017. Technology for Human Rights: UN Human Rights Office Announces Landmark Partnership with Microsoft. *Microsoft News Center*, 16 May. https://news.microsoft.com/2017/05/16/technology-for-human-rights/.
Mignolo, Walter. 2000. *Local Histories/Global Designs: Essays on the Coloniality of Power, Subaltern Knowledges, and Border Thinking*. Princeton (NJ): Princeton University Press.
Morvaridi, Behrooz, and Hughes, Caroline. 2018. South–South Cooperation and Neoliberal Hegemony in a Post-Aid World. *Development and Change* 49 (3): 867–92.
Muggah, Robert, and Thompson, Nathan B. 2018. Brazil Struggles with Effective Cyber-Crime Response. Igarapé Institute. https://igarape.org.br/brazil-struggles-with-effective-cyber-crime-response/.
OECD (Organisation for Economic Cooperation and Development). 2015. Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion Document. Paris: OECD Publishing. DOI: 10.1787/9789264245471-en.
OEWG (Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security). 2021. Final Substantive Report. United Nations General Assembly. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

Oosthoek, Kris, and Doerr, Christian. 2021. Cyber Threat Intelligence: A Product Without a Process? *International Journal of Intelligence and CounterIntelligence* 34 (2): 300-15.
Pawlak, Patryk. 2016. Capacity Building in Cyberspace as an Instrument of Foreign Policy. *Global Policy* 7 (1): 83–92.
Pawlak, Patryk, and Barmpaliou, Panagiota-Nayia. 2017. Politics of Cybersecurity Capacity Building: Conundrum and Opportunity. *Journal of Cyber Policy* 2 (1): 123–44.
Phillips, Lynne, and Ilcan, Suzan. 2004. Capacity-Building: The Neoliberal Governance of Development. *Canadian Journal of Development Studies* 25 (3): 393–409.
Quijano, Aníbal, and Ennis, Michael. 2000. Coloniality of Power, Eurocentrism, and Latin America. *Nepantla: Views from South* 1 (3): 533–80.
Roy, Diana. 2022. China's Growing Influence in Latin America. *Council on Foreign Relations*. https://www.cfr.org/backgrounder/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri.
Sachs, Wolfgang. 2009. *The Development Dictionary: A Guide to Knowledge as Power*. London: Zed Books.
Sen, Amartya. 2001. *Development as Freedom*. Oxford: Oxford University Press.
Shires, James. 2018. Enacting Expertise: Ritual and Risk in Cybersecurity. *Politics and Governance* 6 (2): 31–40.
Solar, Carlos. 2020. Cybersecurity and Cyber Defence in the Emerging Democracies. *Journal of Cyber Policy* 5 (3): 392-412.
Stevens, Clare. 2020. Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet. *Contemporary Security Policy* 41 (1): 129–52.
UN (United Nations). 1992. United Nations Conference on Environment and Development, Rio de Janeiro, Brazil, 3 to 14 June 1992: Agenda 21. United Nations Sustainable Development. https://sdgs.un.org/sites/default/files/publications/Agenda21.pdf.
UN. 2003. Creation of a Global Culture of Cybersecurity. United Nations General Assembly A/RES/57/239. https://digitallibrary.un.org/record/482184.
UN. 2015. Transforming Our World: the 2030 Agenda for Sustainable Development. United Nations General Assembly A/RES/70/1. https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E.
US (United States). 1949. Point Four: Background and Program. Washington: Committee on Foreign Affairs. https://pdf.usaid.gov/pdf_docs/Pcaac280.pdf.
Venner, Mary. 2015. The Concept of 'Capacity' in Development Assistance: New Paradigm or More of the Same? *Global Change, Peace & Security* 27 (1): 85-96.
Wallerstein, Immanuel. 2003. *Historical Capitalism with Capitalist Civilization*. London-New York: Verso.
Webster, David. 2009. Modern Missionaries: Canadian Postwar Technical Assistance Advisors in Southeast Asia. *Journal of the Canadian Historical Association / Revue de la Société Historique du Canada* 20 (2): 86–111.
Webster, David. 2011. Development Advisors in a Time of Cold War and Decolonization: The United Nations Technical Assistance Administration, 1950–59. *Journal of Global History* 6 (2): 249-72.