Analysing Trends and Success Factors of International Cybersecurity Capacity-Building Initiatives

Faisal Hameed, Ioannis Agrafiotis, Carolin Weisser, Michael Goldsmith, Sadie Creese

Department of Computer Science
University of Oxford, UK
email:{*firstname.lastname*}*@cs.ox.ac.uk*

Abstract—**The global community has been engaged extensively in assessing and addressing gaps in cybersecurity commitments and capabilities across nations and regions. As a result, a significant number of Cybersecurity Capacity Building (CCB) initiatives were launched to overcome cyber-risks and realise digital dividends. However, these efforts are facing various challenges such as lack of strategy, and duplication. Although extensive research has been carried out on CCB, no single study exists which focuses on analysing CCB initiatives. This gap presents an opportunity for investigating current trends in CCB efforts and identifying the principles for successful CCB initiatives. In this paper, we aim to bridge this gap by collecting and analysing 165 publicly available initiatives. We classify the initiatives based on Oxford's widely accepted Cybersecurity Capacity Maturity Model (CMM) and perform a descriptive statistical analysis. We further reflect on these initiatives, drawing on well-established success factors from the literature of capacity-building. Towards this end, we also conduct qualitative analysis based on CMM reports for two countries which have experienced socio-economic challenges, Mexico and Brazil, to understand which factors are essential in successful CCB initiatives. We conclude the paper with some interesting results on regional trends, key players, and ingredients of success factors.**

Keywords*–*Cybersecurity; Capacity Building Initiatives; Capacity Maturity Model.

I. INTRODUCTION

There has been an extensive engagement from the global community in combating cyber-risks, for numerous reasons. These efforts are in response to the increasing proliferation of cyber-threats and cyber-harm [1]–[4]. Such activities are adversely affecting the cyber-landscape that forms the foundation of today's interconnected societies. Thus, the desire to maintain cyber-hygiene and to protect against the proliferation of cyber-threats across nations is increasing rapidly [5]–[7]. Additionally, these efforts to protect investments in digitalising nations [8] [9] aim towards their economic and social development [10] [11]. Traditionally, CCB is also perceived as a pursuit of foreign-policy objectives such as advocating specific models of Internet governance, i.e., open and liberal vs closed and restrictive [5]. Moreover, foreign governments' involvements can promote their local companies to gain the competitive advantage of being influencers and decision-makers of these projects, which create opportunities and innovation [5]. Finally, donors are interested in capacity-building in order to promote and advance adoption of specific technical standards by recipient nations [5].

As such, there is a substantial investment being made by the international community aimed at helping nations to develop their capacity in cybersecurity [12]. However, various challenges emerged as nations and institutions rushed to implement instruments to combat cyber-risks. Key challenges includes duplication of initiatives [13], lack of strategy [8], and the widening of the 'cyber-capacity gap' between favored and neglected countries [12].

Thus, the research question to be addressed is *What are the lessons learnt from the current cybersecurity capacity-building activities and what aspects of these initiatives are crucial to their success?* This paper has a twofold objective: firstly, to analyse trends in regional and international capacity-building in cybersecurity, the nature of the work and the partnerships that exist to support it. That analysis of the initiatives will be guided by the University of Oxford Global Cyber Security Capacity Centre (GCSCC) CMM [14]. There are no efforts so far in linking initiatives with benchmarking models, and thus this effort from the GCSCC is presented. There is also no clear consensus on which capacity measures or initiatives work well [8]. Thus, the second objective is to provide the principles for successful cybersecurity initiatives based on a rigorous analysis of a small number of them reflected on Brazil and Mexico within the Latin America and the Caribbean (LAC) region to bring practical context. The LAC region was selected as it was available in both the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) and the CMM review by the Organization of American States (OAS). Within that region, Brazil and Mexico have been selected explicitly as both experienced significant regression and progression changes in cybersecurity maturity respectively, as identified by their GCI scores between the GCI 2014 and 2017 reports.

We define the term *initiative* in a capacity-building context to be any effort, activity, project, control, programme or instrument geared toward progressing capacity-building through assessing, implementing, supporting or developing the aims and objectives of that initiative. We adopt the definition of *Cybersecurity Capacity Building* (CCB) as "A way to empower individuals, communities and governments to achieve their developmental goals by reducing digital security risks stemming from access and use of Information and Communication Technologies" [8]. This definition incorporates consideration of the element of risk, which is an essential component of CCB.

The paper adopts mixed qualitative and quantitative approaches. We identify successful and unsuccessful factors of CCB initiatives, and we conduct a systematic review of current CCB initiatives. We accumulate 165 CCB initiatives and collect data related to critical success factors. We map these initiatives to the dimensions of Oxford's CMM and perform descriptive statistical analysis aiming at understanding trends in initiatives and areas which are neglected by the international community. We then engage in qualitative research to understand which factors are key in successful initiatives. To this end, we conduct a comparative analysis of CMM assessment and cybersecurity capacity-building initiatives to bring context and the overall understanding of trends in Brazil and Mexico. Our overall results present current trends among CCB initiatives, their distribution across regions, and key success factors to CCB.

In what follows, Section II provides a review of the literature underpinning the critical ingredients of unsuccessful and successful CCB. Section III investigates the assessments and indices relevant to the study and selects CMM and GCI as the guiding benchmarking instruments. It also provides preliminary insights into global trends in the field and analyses trends in capacity-building initiatives. Section IV compares and contrasts Brazil and Mexico cybersecurity capacity commitments, CMM comparison, relevant initiatives and the effects of externalities. Section V covers conclusion, limitations and future work.

II. Background and Related Work

To frame the research question, data collection and analysis, we conducted a literature survey answering the following questions: what are the known challenges in delivering effective CCB? What are the key ingredients of a successful CCB programme?

A. Overview of challenges identified with current CCB efforts (factors of unsuccessful initiatives)

One prominent challenge is that there is a lack of explicit linkage between developmental work in Information and Communications Technology (ICT) and cybersecurity. This lack of linkage is due to the lack of convincing empirically based evidence to demonstrate that improving cybersecurity in ICT projects would directly benefit development capacity initiatives [15]. Additionally, the development community does not perceive cybersecurity to be as mission-critical as terrorism or the migration crisis are [12]. Conversely, many cybersecurity strategies lack development-linked goals and activities [12]. Lack of such linkages discourages the community from integrating cybersecurity as a core element of their ICT development, and de-incentivises contributing efficiently to much-needed initiatives. Despite these challenges, there are initial steps in defining a CCB model that can be linked to the development agenda. This model is still struggling to operationalise a development-specific capacity-building approach that is both value-based [16], context-specific and brought in as a broader governance issue rather than tied to the technical silo [12]. There are other efforts that aim to bridge the gap by linking between ICT development and cybersecurity. Dutton et al. [17] examined various datasets related to national cybersecurity capacity for over 120 countries, and identified a strong positive correlation between increased ICT development, more mature cybersecurity posture and safer online environments for end-users [17]. The analysis is an initial step in the right direction regarding grounded evidence-based empirical proof, while admittedly lacking strong statistical proofs of their results [17]. Finally, the GCI 2017 report correlates ICT development and cybersecurity as it compares the GCI index with the ITU ICT for Development Index (IDI), without however providing strong statistical proofs of their results [18]. There is a general sense that improving cybersecurity would contribute to improving ICT yet there are a few outliers in which a country invests heavily in cybersecurity but does not invest in ICT, as in the case of Rwanda. Conversely, countries might invest heavily in ICT while neglecting cybersecurity. In summary, meaningful direct correlation between ICT development and cybersecurity would be a challenge, since multiple factors impact countries' cybersecurity readiness and commitment, such as geopolitical and socio-economical issues, as we highlight in the comparison of Mexico and Brazil below.

Another challenge is the double paradox of CCB maturity in which the development community requires rich empirical and conceptual foundations while also perceives CCB to have a mismatch with the core mission of the development community. However, when the development community decides to get involved with CCB, they often lack security expertise [12]. In contrast, the security experts in law enforcement and cybersecurity lack methodological toolkits and know-how to engage appropriately with the development community [12].

There is also the 'dual-use challenge' of cybersecurity, as cybersecurity capabilities and technologies can potentially be used adversely to increase surveillance and social control and to empower repressive governments as well as cyber-warfare, espionage and cybercrime [8]. Hence, CCB can also be considered a double-edged sword. As such, it is paramount to take a risk-aware approach when providing CCB capabilities to nations and regions [8]. Reflection on authoritarian regimes which have dubious human-rights records highlights the risk of abuse of capacity-building for repressive purposes. For that reason, some international partners such as the Global Forum on Cyber Expertise (GFCE) require their members to adhere to UN charters and laws which respect human rights such as freedom of expression and right to privacy [12].

Another critical challenge is discrimination between countries, a concept coined as 'cyber security gap'. Certain countries, known as 'darling countries', receive more attention in developmental benefits than marginalised or 'orphan' countries. Such discrepancies are observed in CCB according to the Official Development Assistance (ODA) distribution [12]. Typically, countries which are ready to cooperate, which explicitly express interest in joining efforts, which have an established rule of law, and which possess like-minded policy orientation are more likely to be considered for capacity-building assistance [12].

A further challenge is the absence of any widely accepted cybersecurity taxonomy, which results in a lack of mutual understanding of cybersecurity terminology. This confusion in the community is evident in the existence of more than 400 cyber and information-security related definitions within the Global Cyber Definitions Database [19] [20]. There are discrepancies in understanding the meaning of cybersecurity and capacity-building from various policy communities which result in fragmentation, leading to short-sighted and ad-hoc initiatives which are unsustainable [12]. It is essential to have a common level of understanding of the meaning of cybersecurity capacity-building, especially between crucial actors supporting any initiative. Established and accepted definitions serve to maintain a consistent approach to analysing and comparing initiatives, as well as to benchmarking these initiatives with assessments and indices.

Pawlak et al. [13] highlight specific factors shaping the politics of CCB due to the increased involvement of the international and regional communities: siloed mentality, the fragmentation of the CCB community and the duplication of work motivated by either institutional interests or potential business opportunities. Another factor shaping the politics of CCB is the persistence of mission-specific perspectives on capacity building within a policy area. These factors have resulted in adverse effects on donors, such as duplication of work, and inefficiencies amongst beneficiaries, confusion on objectives and conditions and motivations [13]. Another specific CCB challenge is the lack of policy coordination arising from lack of formal intergovernmental negotiations in their approval process. CCB initiatives that are not based on methods of assessment may cause harm as decisions by donors about engagement are not based strictly on the calculation of where the recipient country's most significant needs are or whether the intervention is appropriate to their level of maturity. Placing CCB within developmental traditions of increasing good governance, the rule of law and a human-rights-based approach would be a way forward.

Incomparable or clashing ideologies is yet another specific challenge that CCB encounters. This challenge is evident from lack of involvement in cybersecurity capacity-building from countries such as China and Russia due to their political and policy approaches. The absence of these countries demonstrates that it is not only the technical dimension that raises challenges, but also the political and socio-economical aspects of cybersecurity [12]. However, the formation of the Shanghai Cooperation Organisation (SCO) is an example of how countries within that region are perceiving CCB and conforming to the rapid advancements of technology, while retaining their views and understanding of CCB within that region and internationally [21].

Pawlak et al. [12] summarise signs of unsuccessful developmental initiatives as lack of coordination, budgetary constraints, overly ambitious targets, unrealistic timescales, and political self-interest [12]. Additionally, Hohmann et al. [8] summarise traits of unsuccessful CCB initiatives as lack of integration between key CCB players, few lessons-learned and best-practices available, a piecemeal approach to CCB by donor countries, competing agencies on the same initiatives, unclear mandates from donors, and lack of experts; also, a lack of clear consensus on which capacity measures work well and of adequate metrics to monitor and evaluate CCB projects are two further traits of unsuccessful CCB [8]. Finally, Muller highlights that there is often a lack of valid information due to the security context, as countries are unwilling to share valid information or follow up assessments to demonstrate progress [22].

B. Key ingredients of successful CCB programmes

A majority of the successful ingredients come as a negation of the challenges given in Section II.A above. An initiative is deemed successful if it achieves its aims and objectives and displays the characteristics summarised in the following: donors are major CCB influencers and thus what they deem successful is considered crucial. The UK Foreign and Commonwealth Office (FCO) CCB Programme summarises its requirements for supporting and funding any CCB program as follows: "When projects are part of the country's strategy; have strong host-government support; take a holistic approach that considers host government digital and cyber policies, national strategies, regulation, private sector interests, civil society, technical capability, development context and human rights; take account of what other donors are doing or planning; have co-funding from another country or organisation; and build on previous capacity building projects or partnerships [23]."

A more generic viewpoint at the CCB ecosystem as apposed to individual initiatives is proposed by Pawlak [12]:

- Cyber knowledge brokers at all levels of cross filtration and breaking silos to increase education and awareness.
- Principles-based CCB models and principle-based approach solutions.
- Closing the 'cyber capacity gap' Darling vs orphaned countries.
- Continuous mapping of CCB activities to identify substantial overlaps or gaps.
- Regional champions who are mature and willing to engage.
- Imminent needs to security translated into Computer Security Incident Response Teams (CSIRTs), forensics capabilities and strategies.
- Avoiding securitisation of development initiatives in fears of adverse effects on civil liberties.

Although these proposed solutions are critical components of successful CCB, they are intangible at an initiative level. It is a challenge to quantify and analyse the initiatives gathered against closing the 'cyber capacity gap' or identifying cyber-knowledge brokers at an individual initiative level, for example.

As an alternative view to Pawlak, Hohmann et al. [8] provides an initiative-specific viewpoint with five principles for advancing CCB initiatives. These are:

- National and international *coordination* (in activities) and *cooperation* (in measurements.) At national level coordination translates into an explicit national CCB approach with set strategy prioritisation, streamline institutional setup and stakeholders (academic, civil society, government, public and private) *coordination*. At an international level, *cooperation* would be in the form of sharing and leveraging the results of maturity models and indices to guide CCB efforts. *Coordination* can be enabled by strengthening multilateral and international coordination such as the efforts of the GFCE.
- The second principle would be *integration* of cybersecurity and development expertise as they work together and out of silos. Establishing common language and increased joint projects is also part of integration.
- Recipient countries need to take *ownership* and leadership from setting their own strategies to providing and backing capable institutions. The CCB programmes must be tailored to the country's specific requirements.
- *Sustainability*, in the sense of experts exchanging and benefiting from traditional capacity-building activities

that support sustainable long-term success and continuation of the projects with defined vision, goals and strategy-level components included.

- *Continued and mutual learning* by evaluating and learning how effective the initiatives are, and by developing clear capacity-measure frameworks for measurements and assessments, with useful metrics; also by encouraging openness over the results of assessments and conducting regular (annual) re-assessments, to follow up assessments in order to demonstrate progress and determine best practices available.

Moving forward, the focus in our analysis will be on success factors that are measurable at the initiative level. This will help guide the descriptive statistical analysis of the initiatives in Section IV to produce meaningful insights. As such, we are adopting the Hohmann et al. [8] five principles for advancing CCB, which incorporates the FCO mandates. We also adopt adequate *funding* and sufficient *duration* as the sixth and seventh success factors. These were taken from the budgetary-constraints and unrealistic-timescales points highlighted by Pawlak et al. [12] in the summarised signs of unsuccessful developmental initiatives and the FCO requirements [23] above. The following are therefore the selected key success factors of CCB initiatives:

1) Coordination & Cooperation.
2) Integration.
3) Ownership
4) Sustainability
5) Learning
6) Funding
7) Duration

III. Analysing trends in Cybersecurity Capacity-Building initiatives

A. Methodology

The paper adopts mixed qualitative and quantitative approaches. An initial literature review of existing research has been performed to underpin the key successful and unsuccessful factors of CCB initiatives and thus to identify critical metrics on initiatives, as a basis for the comparative analysis. To identify trends and gaps in CCB, we have collected information related to publicly available CCB initiatives. We have performed web searches to elicit current regional and international initiatives. To conduct the systematic review, a search for initiatives using phrases that focus on cyber-harm, cybersecurity and cyber-risk was performed, as these are crucial themes in combination with capacity-building initiatives, instruments, activities and efforts. Initiatives that exclusively focus on e-governance or privacy, as opposed to cybersecurity, as their core objective were excluded. The scope was limited to publicly available information in English. We accumulated 165 CCB initiatives in total and collected data related to the key success factors. The results were published on the Global Cybersecurity Capacity Portal [24]. Established in 2015, the portal is an output of the GCSCC in cooperation with the GFCE. The portal is a central point of reference of current regional and international capacity-building efforts globally in the critical areas of cybersecurity.

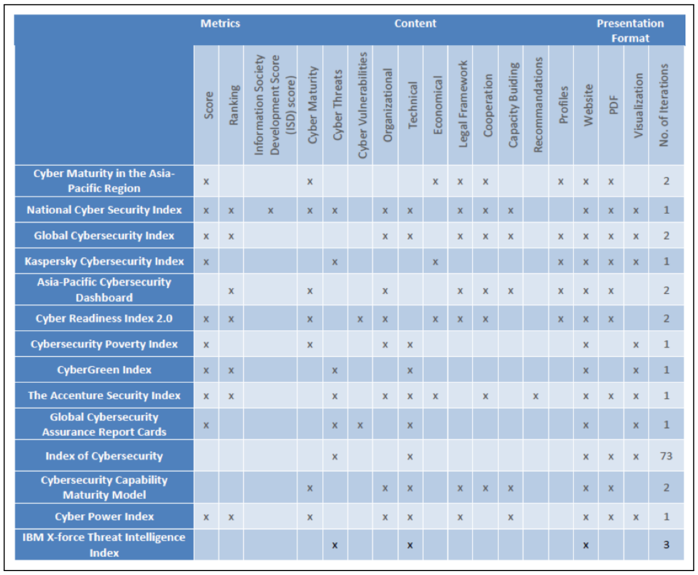
We then investigated various available regional and international CCB benchmarks, assessments and indices. The process was guided by the ITU 2017 Index of Cybersecurity Indices to determine which assessment and index to use to judge progression in cybersecurity. As a result, we have selected the CMM and GCI. A direct mapping between the initiatives and their respective dimensions and factors was performed to determine the linkage between the initiatives and their impacts on regions and nations. After the mapping, we then performed descriptive statistical analysis aimed at understanding trends in initiatives and areas which are neglected by the international community. We then engaged in qualitative research to understand which factors are key in successful initiatives.

A comparative analysis of the selected indexes for all countries within the Latin America and the Caribbean (LAC) region between 2014 and 2017 was performed to select countries that have progressed, remained static or regressed most regarding their cybersecurity capacity commitment.

To this end, we conduct a comparative analysis of CMM assessment and CCB initiatives to bring context and the overall understanding of the trends in Brazil and Mexico.

B. Selection criteria for cybersecurity maturity models and indexes

Various cybersecurity indices and maturity models have sprung up within the international community, academia and the private sector to capture the cyber-readiness and maturity progression. The ITU has developed the Index of Cybersecurity Indices [25] to form a reference that evaluates and presents various prominent organisational, regional and global efforts at producing maturity models and Indices. The 2017 Index of Cybersecurity Indices was instrumental in guiding our investigation of the effectiveness of CCB initiatives and the relevance of various cybersecurity Indices and assessments. The Index evaluates 14 prominent indices for assessing countries and organisations, as well as other scopes of assessment. See Figure 1. Our focus is on regions and nations, thus indices that focus on organisations (e.g. IBM X-Force [3] were excluded. As we are interested in answering the research question "What are the lessons learnt from current cybercapacity-building



	Metrics			Content										Presentation Format				
	Score	Ranking	Information Society Development Score (ISD) score)	Cyber Maturity	Cyber Threats	Cyber Vulnerabilities	Organizational	Technical	Economical	Legal Framework	Cooperation	Capacity Buiding	Recommandations	Profiles	Website	PDF	Visualization	No. of Iterations
Cyber Maturity in the Asia-Pacific Region	x			x					x	x	x			x	x	x		2
National Cyber Security Index	x	x	x	x	x		x	x		x	x	x			x	x	x	1
Global Cybersecurity Index	x	x					x	x		x	x	x		x	x	x	x	2
Kaspersky Cybersecurity Index	x				x				x					x	x	x	x	1
Asia-Pacific Cybersecurity Dashboard		x		x			x			x	x	x		x	x	x		2
Cyber Readiness Index 2.0	x	x		x		x	x		x	x	x			x	x	x		2
Cybersecurity Poverty Index	x			x			x	x							x		x	1
CyberGreen Index	x	x			x			x							x		x	1
The Accenture Security Index	x	x			x		x	x	x		x		x		x	x	x	1
Global Cybersecurity Assurance Report Cards	x				x	x		x							x		x	1
Index of Cybersecurity					x			x							x	x	x	73
Cybersecurity Capability Maturity Model				x			x	x		x	x	x			x	x		2
Cyber Power Index	x	x		x			x	x		x		x			x	x	x	1
IBM X-force Threat Intelligence Index					x			x							x			3

Figure 1. Overview of Cybersecurity Indices [25]

activities and what aspects of these initiatives are crucial to their success?" it is essential for our comparison to identify the countries or regions with the highest levels of progression (or regression) in their cybersecurity maturity and readiness journey. This assumes that initiatives would be most visible in terms of lessons learnt and key success factors when the progress of the country is demonstrable by the indices within the period. As such, we would be looking only at indices that provide metrics, whether scores or ranking, and also indices used for multiple iterations of evaluating countries. This further focuses the scope down to six indices and maturity models. Our preliminary research at this stage was across all nations and states before zooming in on a particular region. That eliminates sub-regional indices such as the Asia-Pacific Cybersecurity Dashboard [26] and the Cyber Maturity in the Asia Pacific Region model [27]. Since we are evaluating initiatives from various viewoints, our criteria include indices and models that incorporate at least four aspects of the five areas: Technical, Economical, Legal, Cooperation, and Capacity-Building. Based on the given criteria, the remaining applicable instruments for measurements were the GCI index [18] and the CMM assessment model [14].

The LAC region was selected as it was represented in both the GCI and the CMM review and it had a reasonably significant number of initiatives as well. Within that region, Brazil and Mexico have been selected, since both experienced significant changes (progression or regression) in their GCI scores between the GCI 2014 and 2017 reports. The Cyber Readiness Index 2.0 [28] would not be used in our analysis as it did not produce a report covering LAC region at the time of this research.

C. The Cybersecurity Capacity Maturity Model for Nations (CMM)

The GCSCC Cybersecurity Capacity Maturity Model for Nations supports comprehensive analysis of detailed appraisal of a country or region [14]. The analysis is based on self-assessments through partners or interviews and workshops with key stakeholders and representatives from donors, recipient countries and relevant organisations [14]. The CMM benchmarks a country's cybersecurity capacity across five distinct dimensions of cybersecurity capacity. The CMM has been developed and used to benchmark countries since 2015, with over 60 nations reviewed so far. The resulting CMM review report is in the form of an overview of the maturity level for the country in each dimension as well comprehensive detailed assessments with specific recommendations advising the state on ways to elevate its capacity to a higher maturity stage [14].

There are five dimensions of cybersecurity identified in the model:

1) Cybersecurity Policy and Strategy.
2) Cyber Culture and Society.
3) Cybersecurity Education, Training and Skills.
4) Legal and Regulatory Frameworks.
5) Standards, Organisations, and Technologies.

Each dimension is divided further into factors. Maturity levels are divided into five stages: start-up, formative, established, strategic, and dynamic.

D. The ITU Global Cybersecurity Index (GCI)

The index spans different mechanisms for evaluating cyber-maturity to derive rankings and scores that enable comparisons between nations and regions. It is being led by the ITU as part of its Global Cybersecurity Agenda (GCA) [29]. The GCI examines levels of commitment on five distinct pillars [18]: 1. Legal. 2. Technical. 3. Organizational. 4. Capacity building, and 5. Cooperation.

In addition to the overall ranking, the index includes regional rankings and an individual score for each country. This focus enables us to compare the country or region in question. The index is primarily based on surveying ITU's members and publicly available information. The identified weakness, however, is that the index is more policy and organisationally oriented more technical, and that distilling a single number to capture maturity necessarily equates incomparable considerations. The index assesses countries' commitments with regards to cybersecurity as opposed to actual readiness.

While there are in some cases a direct one-to-one mapping between the CMM Dimensions and the GCI Pillars, such as in the areas of strategy, legal and technical, there are GCI pillars such as Capacity Building and Cooperation that cut across all CMM Dimensions. See Table I.

TABLE I. MAPPING CMM DIMENSIONS WITH GCI PILLARS

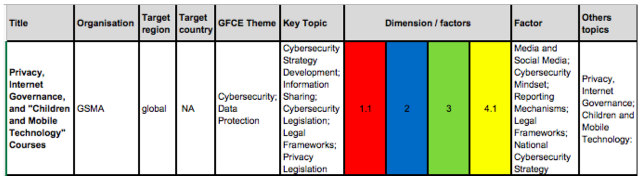
GCSCC CMM Dimensions	*ITU GCI Pillars*	
Cybersecurity Policy and Strategy	Organizational	Cooperation
Cyber Culture and Society	–	
Cybersecurity Education, Training and Skills	Capacity building	
Legal and Regulatory Frameworks	Legal	
Standards, Organizations, and Technologies	Technical	

E. An overview of the Global Cybersecurity Capacity Portal.

Initiatives were collected and hosted on the Portal which contains a dedicated informational web-page per initiative. To bring more understanding and context to the initiatives, as well as to form the basis of the comparative analysis, an off-line dataset (spreadsheet) of the initiatives was created manually to help gain insights from these efforts, such as an analysis of stakeholders and linkage between the initiatives and the CMM model. The dataset includes the *Title* of the initiative; the name of the sponsoring or initiating *Organisation*; the *Target Region*; *Target Country*; the *GFCE Theme*; *Key Topic*; *Dimension* and *Factors*; and *Others Topics*; vital *Partners*; affected or *Target Groups*, planned *Budget*, main *Aims* and *objectives*, *Outputs*, underlying *Activities*, *Period* or duration of the effort, and finally *Contact* details. Mapping initiatives to dimensions and factors of the CMM can be demonstrated by the Dimension and Factors columns identified in the following colour scheme. See Figure 2:

- Red: Cybersecurity Policy and Strategy
- Blue: Cyber-Culture and Society
- Green: Cybersecurity Education, Training and Skills
- Yellow: Legal and Regulatory Frameworks
- Purple: Standards, Organisations, and Technologies

The purple is not illustrated in the following example as this particular initiative did not have mapping with the *Standards,* *Organisations, and Technologies* CMM dimension. The unique numbers within the Dimensions and Factors columns are mapped directly to the CMM (e.g., 4.3 refers to Dimension 4 Factor number 3). A complete mapping between the initiatives in scope and the CMM has been performed.



Title	Organisation	Target region	Target country	GFCE Theme	Key Topic	Dimension / factors				Factor	Others topics
Privacy, Internet Governance, and "Children and Mobile Technology" Courses	GSMA	global	NA	Cybersecurity; Data Protection	Cybersecurity Strategy Development; Information Sharing; Cybersecurity Legislation; Legal Frameworks; Privacy Legislation	1.1	2	3	4.1	Media and Social Media; Cybersecurity Mindset; Reporting Mechanisms; Legal Frameworks; National Cybersecurity Strategy	Privacy, Internet Governance; Children and Mobile Technology:

Figure 2. Initiatives example

IV. Descriptive Statistical Analysis of the Initiatives

A. Regional analysis

As of July 2018, we had gathered 165 distinguished initiatives. Initiatives are either global in nature or within one of seven geographical regions. We are adopting the World Bank geographical regions [30]. Figure 3 displays the target regions, respective counts, and percentages of initiatives per region. An initiative that spans countries in multiple regions is counted in all those regions.

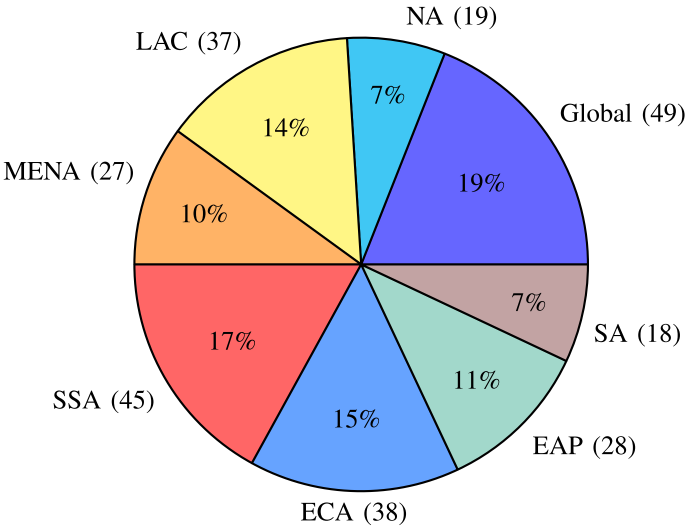


Figure 3. Global initiatives, and those for North America (NA), Latin America and the Caribbean (LAC), The Middle East and North Africa (MENA), Sub-Saharan Africa (SSA), Europe and Central Asia (ECA), East Asia and Pacific (EAP) and South Asia (SA)

B. Organisational analysis

105 organisations, countries or entities are initiating or leading initiatives across all regions and globally. Table II represents the Top 10 most active Organisations that are either initiating or leading initiatives. It is important to highlight that the top 10 active organisations account for 75% of initiatives. This is followed by a demonstration of the top Partners in supporting CCB across all initiatives within the portal. See Table III.

TABLE II. Organisational analysis

Organisation	*# of initiatives*
UK Foreign & Commonwealth Office	27
International Telecommunications Union (ITU)	15
e-Governance Academy (eGA)	12
Global Forum on Cyber Expertise (GFCE)	9
United Nations Development Programme	6
Council of Europe (CoE)	5
United Nations Economic Commission for Africa (UNECA)	5
United Nations Conference on Trade and Development (UNCTAD)	4
Association of Southeast Asian Nations (ASEAN)	3
DiploFoundation (Diplo)	3

TABLE III. Partner analysis

Partners	*# of initiatives*
ITU Oman Regional Cybersecurity Centre	8
European Union (EU)	6
Organization of American States (OAS)	5
Economic Community of West African States (ECOWAS)	4
European Cybercrime Centre – EC3 (Europol)	4
FIRST	4
Global Cyber Security Capacity Centre (GCSCC) – University of Oxford	4
INTERPOL (INT)	4
National Crime Agency	4
Netherlands	4
Norway	4
UK Foreign and Commonwealth Office	4
United States of America	4

C. Initiatives mapped to the CMM and GCI

When surveying the current trends over the gathered CCB initiatives, it visibly demonstrates that about half of the initiatives 47% are geared towards the first dimension of the CMM model, *Cybersecurity Policy and Strategy*; followed by the fourth dimension: *Legal and Regulatory Frameworks* 33%. The third dimension: *Cybersecurity Education, Training and Skills* concerns 14% of the initiatives, followed by the fifth dimension: *Standards, Organisations, and Technologies* with 7%, and finally the lowest number of initiatives are focused on the second dimension *Cyber Culture and Society* 7%. See Figure 4 which summarises the analysis.

Our results are in close alignment with the observations in ITU GCI 2017 report. The mapping between the initiatives and the CMM indicates that the current trends are focusing on building the foundational aspects of CCB, such as devising or enhancing national Cybersecurity strategies, establishing effective CSIRT programmes, or creating robust regulatory frameworks. Since only 38% of the surveyed countries have a published cybersecurity strategy, in which only 11% of it has a dedicated standalone tailored strategy [18], implementing or enhancing cybersecurity strategy is of paramount importance at this stage of global CCB. Similarly, efforts focusing on the development of legal and regulatory frameworks (33% of initiatives) endeavour to bridge the gap identified in ITU GCI report, where it was identified that 57% of legal actors lack specialist cybersecurity training [18].

Furthermore, there is also a close alignment between the initiatives that relate to incident management and gaps in CSIRTs that the 2017 GCI report has acknowledged. CSIRT enhancement is part of the Cybersecurity Policy, and Strategy CMM dimension with one third of the initiatives of that dimension focused on Incident Response, and 16 initiatives focused on Crisis Management. This is in line with the GCI finding that 79% of existing CSIRTs require metrics or measurements criteria to be used for effective management of incidents. There are, however, apparent gaps and imbalances since initiatives are oblivious to other dimensions such as Standards, Organisations, and Technologies and Cyber Culture and Society, which are vital in ensuring a balanced, capable, resilient, and dynamic cyberspace.

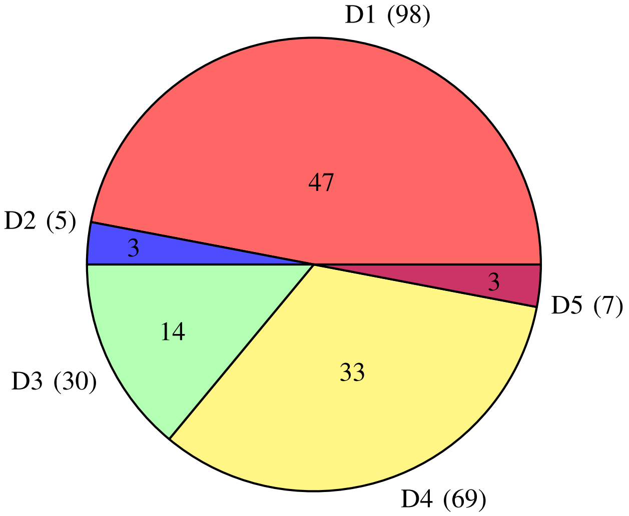


Figure 4. Percentage of initiatives per CMM Dimension: D1 *Cybersecurity Policy and Strategy*, D2 *Cyber Culture and Society*, D3 *Cybersecurity Education, Training and Skills*, D4 *Legal and Regulatory Frameworks*, D5 *Standards, Organisations, and Technologies*

D. Analysing initiatives based on key success factors

A direct mapping between key success factors identified in Section II.B and the initiatives gathered is a challenge, as such a mapping is subject to interpretation and subjective judgments. However, the following is an effort at translating what it is observed in the CCB initiatives against key success factors.

The first success factor is national and international *coordination* (in activities) and *cooperation* (in measurements). When applied properly, this factor should tackle challenges such as duplication of effort, lack of policy coordination, cyber-capacity gap and lack of strategy, as well as agencies competing on the same initiatives.

Coordination can be perceived by determining whether the initiating or sponsoring actor of an initiative is engaged with a partner or a set of partners. An actor could in itself be a consortium of multilateral entities, such as the ITU or the OAS. Thus, it has been observed that 84% of the initiatives have one or more partners supporting the effort. Although the remaining 16% do not have an explicit partnership, they are based on bilateral or multilateral entities, such as the Association of Southeast Asian Nations (ASEAN). These observations imply that the overwhelming majority of initiatives conform with the coordination factor of successful initiatives.

Cooperation is achieved when nations collaborate in cybersecurity assessments. It has been determined that there are twelve initiatives in which the aims and objectives contain some form of assessment. There are a further twenty-two initiatives where assessment or self-assessment is part of either their essential or other topics covered. All these are indications of high-level activity in cooperation between entities concerning measurement. This remains a challenge to quantify, however, as there are potential overlaps between the objectives of the initiatives.

The second identified factor is *intended Integration* of cybersecurity and development expertise. This is interpreted by the involvement and engagement of key stakeholders from across various levels of the targeted society. There were 10% of initiatives that included members of academic institutions, civil society, defence, non-profits, the private sector and governmental institutions. Further detailed analysis of each initiative is required to gain a deeper level of understanding of the true state of integration (or lack thereof) between the development sector and cybersecurity efforts.

Ownership by the recipient country or entity is the third success factor. Leveraging assessments, whether against the CMM or other models, represents an initial step in refining capacity-building to eliminate existing discrepancies between donors' objectives and beneficiaries' priorities. From the perspective of the initiatives gathered, investigating whether the target country or region is also part of the organisation leading the initiative or the partners supporting it was determines effective ownership. Many initiatives are global, however, and involve many countries and regions. Unfortunately, it was not possible to extract sufficient information to determine whether this factor is appropriately incorporated into the design of a given initiative.

The fourth factor of a successful initiative is *sustainability* of efforts, as evidenced by experts exchanging and benefiting from traditional capacity-building activities that support sustainable long-term success and continuation of the projects, as opposed to short-term one-off training activities. Successful initiatives tend to be based on an increase in the pool of experts in the recipient countries and in building on proven successful methodologies. Also, utilising cross-sectoral approaches to engage and involve the public and private sectors and academia, and getting them to work together, is another key ingredient. There were 10% of cross-sectoral initiatives identified based on this analysis.

The fifth factor is *continued and mutual learning* by developing clear capacity measurements while encouraging openness. This factor addresses the lessons learnt from designing and implementing CCB initiatives. Continued and mutual learning should also address the cybersecurity-context challenge, in which resistance by countries to information-sharing exists. There are only four initiatives which contain educational aspects, but there are a further twelve initiatives where education or learning elements are part of the aims and objectives. Finally, only two partners in all initiatives were associated with education. However, analysing continued learning within initiatives requires more in-depth data from each initiative, which is lacking.

Adequate *funding* is the sixth factor. It is challenging to obtain data on the funding aspects of initiatives. Currently, there are only three initiatives that indicate the initial budget of that initiative. As such, currently, the funding element is not being evaluated.

The seventh and final factor of successful initiatives is their *duration*. As capacity-building initiatives take time to develop and produce real impact, it can possibly be assumed that the longer the initiative remains, the more precise its measurement can be. Hence this factor is not necessarily a direct factor of a successful initiative. Caveatting that there are initiatives that are naturally limited in time, such as targeted workshops. 70% of the initiatives have their project duration identified among which 14% have a very short term.

V. Reflections on the Latin America and the Caribbean (LAC) region

To provide further insights on the key factors that render an initiative successful, we engage in qualitative research and analyse reports detailing the cybersecurity capacity maturity of countries in the LAC region. The LAC region was selected as it was represented in both the GCI and the OAS reviews. The Inter-American Development Bank (IDB) and the OAS have partnered together and carried out a CMM review of the thirty-two countries in LAC, based on the GCSCC CMM [24], [31]. The report reflects a dim view on the security posture and readiness of the region as only five countries have strategies, eight are planning or developing capabilities for Critical Infrastructure Protection, and 30% of citizens are not aware of cybersecurity risk [31]. Within that region, Brazil and Mexico have been specifically selected as they experienced significant regression and progression respectively in their GCI scores between 2014 and 2017.

The LAC region is a heterogeneous pool of countries with different economic developments, historical backgrounds, languages and different challenges. According to the World Bank 2017 annual report and regional perspective, the LAC region experienced an economic slowdown during the last six years including two recessions [30]. This slowdown has adversely reversed the gains realised due to hard earned social reforms at the beginning of the 21st century. As a result, GDP growth for LAC was 2.3% in 2000, 4.7% in 2010 and currently down -1.8%. However, the region is slowly gaining growth and recovering economically [30].

Cybercrime is proliferating within the Latin America and the Caribbean region due to multiple factors including the rapid digitisation of economies without considerations of appropriate cybersecurity controls; the foundational establishment of criminal networks; and the socio-economic and geopolitical situations affecting the region [32]. The cost of Cybercrime in Mexico was estimated to be $3 billion, while Brazil $8 billion in 2013 [33].

A. Descriptive statistical analysis of the initiatives in LAC

The distribution of the CCB initiatives within the LAC region reflects similar distributions among the global regions. See Table IV.

TABLE IV. CMM Dimensions and the corresponding number of initiatives for LAC.

D#	*GCSCC Dimensions*	*# of initiatives*
D1	Cybersecurity Policy and Strategy	31
D2	Cyber Culture and Society	1
D3	Cybersecurity Education, Training and Skills	3
D4	Legal and Regulatory Frameworks	11
D5	Standards, Organisations, and Technologies	1

Each country was measured and assessed by the GCI between 2014 and 2017 on various GCI pillars with a subsequent total score presented. Tables V and VI display the top 3 countries of the LAC region based on the GCI scores in 2014 and 2017, respectively. Mexico's 2014 results are also presented to highlight the progress achieved. According to the results, Brazil has descended from the highest rank of the LAC region regarding cybersecurity commitment in the year 2014 down to the third rank in 2017. Conversely, Mexico has ascended from the 7th rank to the first rank.

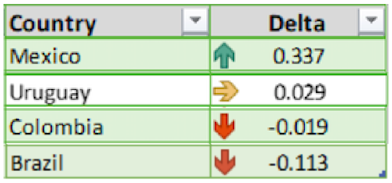
TABLE V. Top 3 LAC and Mexico GCI Index 2014 Results.

Regional Rank	*Country*	*GCI Score*	*Global Rank*
1	Brazil	0.7059	5
2	Uruguay	0.6176	8
3	Colombia	0.5882	9
7	Mexico	0.3235	18

TABLE VI. Top 3 LAC GCI Index 2017 Results

Regional Rank	*Country*	*GCI Score*	*Global Rank*
1	Mexico	0.6600	28
2	Uruguay	0.6470	29
3	Brazil	0.5930	38

The differences between countries' scores from 2014 and 2017 were computed to demonstrate progression, staticness or apparent regression concerning their commitments to cybersecurity. The differences demonstrate dramatic changes in the GCI scores, with Mexico being the highest positive change of 0.337, in stark contrast to Brazil (-0.113) as illustrated in Figure 5.



Country ▾	Delta ▾
Mexico	↑ 0.337
Uruguay	⇨ 0.029
Colombia	↓ -0.019
Brazil	↓ -0.113

Figure 5. LAC Delta results between 2014 and 2017 GCI reports

According to the GCI 2017 report "The GCI 2014 and GCI 2017 are not directly comparable due to a change in methodology. While the 2014 index used a simple average methodology, the 2017 index employed a weighting factor for each pillar." [18]. However, both reports are based on the 5 pillars mentioned in Section III.D. The difference is that the 2017 index is finer grained with 157 scale points while the 2014 one has 34. The pillars are further broken down into 17 indicators in the 2014 GCI report. Each indicator is weighted against three levels of none (0), partial (1) and full compliance (2) with a full mark of 17 x 2 = 34. The ranking is calculated based on the following notations [34]:

χ_{qc} Value of the individual indicator q for country c, with q=1,..., Q and c=1,..., M.
I_{qc} Normalized value of individual indicator q for country c.
CI_c Value of the composite indicator for country c.

$$GCI2014 : CI_c = \frac{I_{qc}}{34}$$

$$I_{qc} = Rank(\chi_{qc})$$

The 2017 GCI is finer grained having 25 indicators with 157 binary none (0) or full compliance (1) questions distributed among the indicators and therefore the pillars based on weighting factor from experts [18].

$$GCI2017 : CI_c = \frac{I_{qc}}{157}$$

Brazil, for example, scored CI_c: 24 out of 34 in 2014 with GCI2014 score of 0.7059 out of 1 as in Table V. In contrast, Brazil in GCI 2017 scored CI_c: 93 out of 157 which is 0.5930 GCI out of 1 as shown in Table VI. Although GCI 2017 is finer grained as each mark is weighted (0.6%) in contrast to the (2.9%) of 2014, both GCIs benchmark countries between 0 and 1 or at a percentage scale. This deviation in granularity has been considered when performing the analysis and the averages of the GCI 2014 and 2017 scores between the two indices as we compute each country's delta with itself before comparing with others. As we use the delta as indicators that guides us in selecting Mexico and Brazil as countries of interest. The country's rank would be another indicator that we consider which is aligned with the delta comparison as well.

B. Comparative analysis between Mexico and Brazil

Figure 6 depicts security risks on (human, physical, and financial) areas including crime, riots, terrorism, military conflicts, and other threats. It also shows political risks which indicate the probability of political instability in a given country. In 2018, Mexico is Low in political risk and mixed between High, Medium and Low in security risks depending on the area of the country, whereas Brazil is Medium in both security and political risk according to the company Control Risks [35].

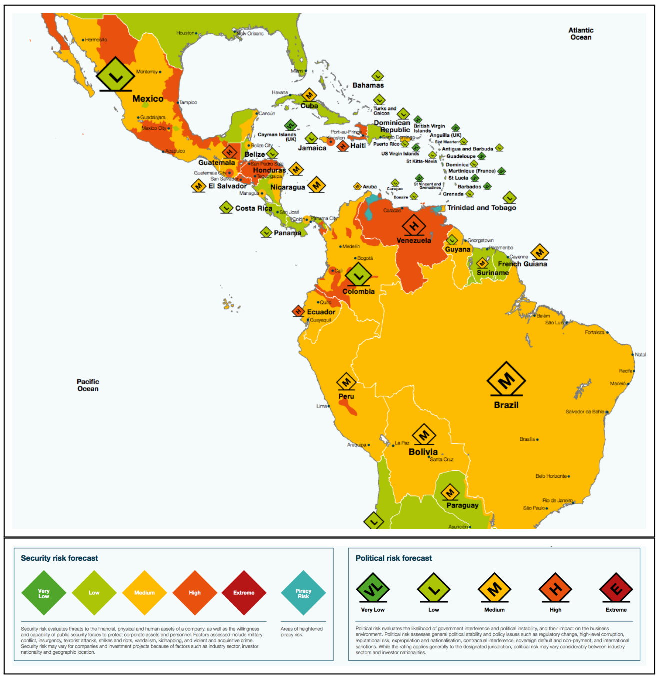

Atlantic Ocean
Pacific Ocean
Mexico
Cuba
Bahamas
Turks and Caicos
Dominican Republic
British Virgin Islands
Anguilla (UK)
Cayman Islands (UK)
Jamaica
Haiti
Puerto Rico
US Virgin Islands
Antigua and Barbuda
Guadeloupe
St Kitts-Nevis
Dominica
Martinique (France)
St Lucia
Barbados
St Vincent and Grenadines
Grenada
Aruba
Curaçao
Bonaire
Trinidad and Tobago
Belize
Guatemala
Honduras
El Salvador
Nicaragua
Costa Rica
Panama
Venezuela
Guyana
Suriname
French Guiana
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Security risk forecast
Very Low
Low
Medium
High
Extreme
Piracy Risk
Security risk evaluates threats to the financial, physical and human assets of a company, as well as the willingness and capability of public security forces to protect corporate assets and personnel. Factors assessed include military conflict, insurgency, terrorist attacks, strikes and riots, vandalism, kidnapping, and violent and acquisitive crime. Security risk may vary for companies and investment projects because of factors such as industry sector, investor nationality and geographic location.
Areas of heightened piracy risk.
Political risk forecast
VL
L
M
H
E
Very Low
Low
Medium
High
Extreme
Political risk evaluates the likelihood of government interference and political instability, and their impact on the business environment. Political risk assesses general political stability and policy issues such as regulatory change, high-level corruption, reputational risk, expropriation and nationalisation, contractual interference, sovereign default and non-payment, and international sanctions. While the rating applies generally to the designated jurisdiction, political risk may vary considerably between industry sectors and investor nationalities.

Figure 6. Americas Geopolitical socio-economical Risk Map 2018. [35].

According to the OAS reviews, both Brazil and Mexico have similar maturity levels across many dimensions; Brazil is further advanced in cyberdefence consideration, cybersecurity mindset, cybersecurity training, procedural laws, incident response and cybersecurity marketplace. In contrast, Mexico is more advanced in on-line privacy, responsible reporting and disclosure, identification of incidents, and critical infrastructure response planning. Both countries are rated in the OAS report between Formative (2) and Established (3) levels of maturity, with Brazil averaging at 2.55 and Mexico at 2.40.

Mexico has been demonstrating strength in the legal pillar of the GCI index as it invests substantial efforts in cyber legislation covering criminality, data protection, data privacy and electronic transactions [18]. As it aims to join the Budapest treaty on Cybercrime [36], Mexico has undergone tremendous amendments to substantive and procedural laws [31]. It also has hosted the 2016 Meridian Process [37] which produced The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy Makers [38].

We have analysed the eight distinctive initiatives targeting Mexico and mapped the initiatives with the applicable key success factors. Table VII demonstrates that most of the initiatives have multiple success factors.

TABLE VII. INITIATIVES IN MEXICO WITH KEY SUCCESS FACTORS

Initiatives in Mexico	*Success factors*
Cybersecurity in the OAS Member States.	Coordination & Cooperation, Integration, Ownership, Sustainability, Learning, Funding, Duration
Japan International Cooperation Agency (JICA). Countermeasures Against CyberCrime.	Coordination & Cooperation, Integration, Funding
Mexican Financial Sector, FCO, Control Risks: Cybersecurity Health check.	Coordination & Cooperation, Ownership, Learning
Cybercrime Workshops, OAS, Federal Police: Mexican National Cybersecurity Week.	Coordination & Cooperation, Integration, Ownership
Cybercrime@Octopus, Council of Europe (CoE).	Coordination & Cooperation, Learning, Funding, Duration
Data Privacy Pathfinder APEC	Coordination & Cooperation, Integration
Latin American e-Commerce Legislation Harmonisation UN, Finland, ACS	Coordination & Cooperation, Ownership
Strengthening Cyber Skills in the Federal Police, FCO, BSI	Coordination & Cooperation, Integration, Ownership

In addition to these eight initiatives, Mexico is also part of the regional LAC initiatives, of which 24% cover Legal and Regulatory Frameworks.

In stark contrast to Mexico, Brazil had only five initiatives tailored to the needs of the country. These initiatives have commenced across a number of dimensions, focusing on the leadership role of the armed forces, or the establishment of the Cybersecurity strategy of the Federal Public Administration, or the coordination between the various CSIRTs, or the investments in education and awareness programs as well as establishing higher education centres of excellence [31]. However, Brazil was ranked the most dangerous country for Financial attacks in 2014 and has been the source and victim of cybercrime [39].

We have analysed the five distinctive initiatives targeting Brazil and mapped the initiatives with the applicable key success factors. Table VIII demonstrates fewer success factors linked to the initiatives at hand.

Brazil is one of the leading economies in LAC and has been investing heavily in ICT development. According to the World Bank national accounts data and the OECD national

TABLE VIII. Initiatives in Brazil with Key success factors

Initiatives in Brazil	*Success factors*
Fostering Cybersecurity Through Training the Judiciary on Digital and Cyber Issues. CFO, ITS	Coordination & Cooperation, Ownership
Introducing Estonian ICT Solutions for Delegations from Developing Countries. eGA	Coordination & Cooperation, Ownership, Learning, Funding, Duration
Tackling Cyber-Enabled Crime: Brazilian National Counter-Corruption and Anti-Money Laundering. FCO, NCA	Coordination & Cooperation, Learning
Cybersecurity and Cybercrime Workshop.	Learning
RNP-NSF for Research and Development Projects in Cybersecurity	Coordination & Cooperation, Ownership, Funding, Duration

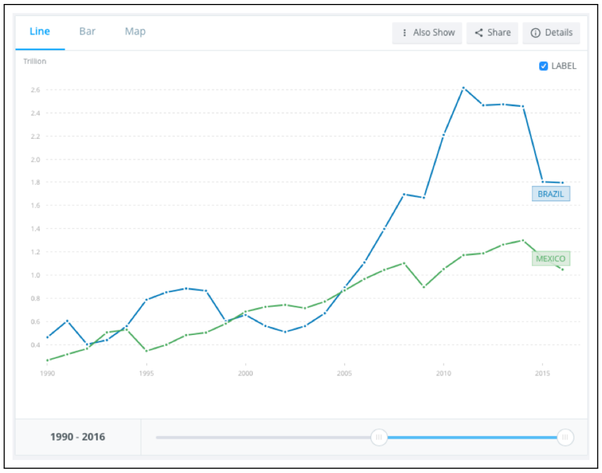


Figure 7. Economic (GDP) progress of Brazil and Mexico (1990-2016)) [40]

accounts data files, Brazil GDP in the year 2011 was 2.616 Trillion (USD) this has significantly fallen to a low 1.796 Trillion (USD) in the year 2016 losing 31% of GDP in this five-year period. See Figure 7. This slow economic progress might have contributed to the lack of progress in Brazil's cybersecurity maturity. Likewise, Mexico has also experienced economic slowdown but not as drastic as Brazil, and the number of targeted initiatives has facilitated the country's maturity growth.

VI. Conclusions, Limitations and future work

The global community has been engaged extensively in assessing and addressing gaps in the cybersecurity commitments and capabilities of nations and regions. As a result, a significant number of Cybersecurity Capacity-Building (CCB) initiatives have been launched to overcome cyber-risks. These efforts face various challenges, however, such as lack of strategy and duplication of initiatives. To our knowledge, no study has explored the areas where cybersecurity initiatives focus and the possible gaps. In this paper, we have tried to close this gap by collecting and analysing all publicly available initiatives. We have further reflected on these initiatives with respect to well-established success factors in the literature on capacity-building. Towards this end, we have also engaged in qualitative research and analysed reports for two countries, Mexico and Brazil, trying to understand which of these factors may have been influential in designing and implementing successful cybersecurity initiatives.

Our results suggest that the distribution of CCB initiatives across the regions has been divided evenly, except that North America has received the least, only 7% of initiatives. This is because the gathered initiatives are focused on developing countries. The current focus, as observed from analysing the trends, is on building the foundational aspects of capacity such as devising or enhancing national Cybersecurity strategies, establishing effective CSIRT programmes, or creating reliable regulatory frameworks. These findings are in line with the observations of the ITU 2017 Global Cybersecurity Index. There are, however, evident gaps and imbalances with other CMM dimensions such as *Standards, Organisations, and Technologies* and *Cyber Culture and Society* which are vital in ensuring a balanced, capable, resilient, and dynamic cyberspace. As the top 10 active organisations account for (75%) of initiatives it demonstrates that few critical organisations are leading initiatives.

The comparison of Brazil and Mexico using the GCI scores demonstrates that Mexico was more committed to cybersecurity than Brazil during the 2014 and 2017 period, while it received a bigger number of initiatives. Our analysis suggests that the socio-economic and geopolitical challenges Brazil experienced over the recent years could be a key factor in why Brazil has apparently regressed or at least not progressed enough concerning cybersecurity maturity in contrast to the key success factors associated with the initiatives conducted by Mexico as highlighted in Section V.B.

The scope of this paper was limited to publicly available information in English. Moreover initiatives are primarily focused on developing and middle-income countries, since data was gathered mainly from sponsors and publicly available initiatives. Additionally, due to the security context dilemma, understandably various nations and entities would be hesitant to provide insights on their current and effective initiatives. As such the information is limited in scope and does not cover the majority of initiatives available. We may conclude that transparency in providing CCB information is essential in demonstrating effectiveness. Finally, lack of key attribute data such as the amount and commitment of funding for most initiatives adversely affected the analysis. Our scope was focused on the gathered initiatives, which limited our analysis to success factors at the initiative level as opposed the general CCB programmes and ecosystems. Generic success factors such as closing the 'cyber capacity gap' or identifying cyber-knowledge brokers requires alternative methodologies which would include interviews and focus groups of relevant stakeholders to gain deep insights.

In the future, we intend to perform a comparison of the existing efforts in capacity-building with the economic and technology metrics that exist for a set of countries or a specific region. There is a niche space in exploring what data should be collected from governments and organisation to better reflect capacity-maturity development. We aim to identify gaps in the funding of capacity-building and misallocation of these funds to less critical factors. Once the appropriate datasets are identified, relationships that exist between capacity-building activities may be revealed, hopefully leading to optimisation of the development of countries towards a more secure cybersecurity posture. A deeper analysis over the generic success factors, based on interviews and focus groups of relevant stakeholders, will provide us with more thorough and encompassing insights.

Acknowledgment

Special words of appreciations to Dr. Maria Bada for her valuable feedback and insights during the review phase of the project. Numerous words of appreciations to the Global Cyber Security Capacity Centre (GCSCC) for their invaluable guidance and feedback as well as providing materials from the GFCE portal. This work is supported by the UK Engineering and Physical Sciences Research Council (EPSRC) and the Saudi Ministry of Education.

References

[1] J. Lewis, “Economic Impact of Cybercrime. No Slowing Down Report,” McAfee, Center for Strategic and International Studies (CSIS), Tech. Rep., 2018. [Online]. Available: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf

[2] I. Agrafiotis et al., “Cyber Harm: Concepts, Taxonomy and Measurement,” SSRN Electronic Journal, 8 2016, p. 23. [Online]. Available: http://www.ssrn.com/abstract=2828646

[3] M. Alvarez et al., “IBM X-Force Threat Intelligence Index 2017,” IBM X-Forcec Threat Research, NY, Tech. Rep., 2017. [Online]. Available: https://assets.documentcloud.org/documents/3527813/IBM-XForce-Index-2017-FINAL.pdf

[4] ISACA Information Systems Audit and Control Association, “State of Cyber Security 2017 Resources and Threats,” ISACA, Tech. Rep., 2017. [Online]. Available: https://cybersecurity.isaca.org/static-assets/documents/State-of-Cybersecurity-part-2-infographic_res_eng_0517.pdf

[5] P. Pawlak, “Capacity Building in Cyberspace as an Instrument of Foreign Policy,” Global Policy, vol. 7, no. 1, 2 2016, pp. 83–92. [Online]. Available: http://doi.wiley.com/10.1111/1758-5899.12298

[6] World Economic Forum, “Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience,” 2012. [Online]. Available: https://www.weforum.org/reports/risk-and-responsibility-/hyperconnected-world-/pathways-global-cyber-resilience

[7] H. Tiirmaa-Klaar, “Building national cyber resilience and protecting critical information infrastructure,” Journal of Cyber Policy, vol. 1, no. 1, 1 2016, pp. 94–106. [Online]. Available: http://www.tandfonline.com/doi/full/10.1080/23738871.2016.1165716

[8] M. Hohmann, A. Pirang, and T. Benner, “Advancing Cybersecurity Capacity Building,” Global Public Policy Institute (GPPI), 2017. [Online]. Available: http://www.gppi.net/fileadmin/user_upload/media/pub/2017/Hohmann__Pirang__Benner__2017__Advancing_Cybersecurity_Capacity_Building.pdf

[9] The World Bank Group, “World Development Report 2016: Digital Dividends.” The World Bank Group, Washington DC, Tech. Rep., 2016. [Online]. Available: http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf

[10] R. Heeks, “New Priorities for ICT4D Policy, Practice and WSIS in a Post-2015 World,” Centre for Development Informatics, 2014, pp. 1–59. [Online]. Available: http://www.cdi.manchester.ac.uk

[11] Organisation for Economic Cooperation and Development (OECD), Digital Security Risk Management for Economic and Social Prosperity, 1st ed., Organisation for Economic Cooperation and Development (OECD), Ed. OECD Publishing, 10 2015. [Online]. Available: http://www.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en

[12] P. Pawlak and P.-N. Barmpaliou, “Politics of cybersecurity capacity building: conundrum and opportunity,” Journal of Cyber Policy, vol. 2, no. 1, 2017, pp. 123–144. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1294610

[13] P. Pawlak, N. Robinson, M. G. Porcedda, E. Kvochko, and E. Calandro, “Riding the digital wave The impact of cyber capacity building on human development,” EU Institute for Security Studies, Paris, Tech. Rep. December, 2014. [Online]. Available: http://www.iss.europa.eu/publications/detail/article/riding-the-digital-wave-the-impact-of-cyber-capacity-building/-on-human-development/

[14] Global Cyber Security Capacity Centre, “Cybersecurity Capacity Maturity Model for Nations (CMM). Revised Edition,” University of Oxford, Oxford, Tech. Rep. CMM, 2017. [Online]. Available: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-revised-edition

[15] P. Pawlak, “Cyber Capacity Building in Ten Points Ten major take-away points,” European Union Institute for Security Studies, vol. 7, no. 1, 2014, p. 8392. [Online]. Available: https://www.iss.europa.eu/sites/default/files/EUISSFiles/EUISS_Conference-Capacity_building_in_ten_points-0414.pdf

[16] M. Schaake and M. Vermeulen, “Towards a values-based European foreign policy to cybersecurity,” Journal of Cyber Policy, vol. 1, no. 1, 1 2016, pp. 75–84. [Online]. Available: http://www.tandfonline.com/doi/full/10.1080/23738871.2016.1157617

[17] W. H. Dutton, S. Creese, R. Shillair, M. Bada, and T. Roberts, “Cyber Security Capacity: Does it Matter?” in Annual Meeting of the Telecommunication Policy Research Conference (TPRC), 2017, pp. 1–26. [Online]. Available: https://www.researchgate.net/profile/Ruth_Shillair/publication/319645577_Cyber_Security_Capacity_Does_it_Matter/links/59b7cdf4458515c212b505a3/Cyber-Security-Capacity-Does-it-Matter.pdf

[18] International Telecommunication Union, “Global Cybersecurity Index,” International Telecommunication Union (ITU), Geneva, Switzerland, Tech. Rep., 2017. [Online]. Available: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

[19] T. Maurer and R. Morgus, “Compilation of Existing Cybersecurity and Information Security Related Definitions,” 2014. [Online]. Available: https://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and/-information-security-related-definitions/

[20] V. Radunovic, “Towards A Secure Cyberspace Via Regional Co-operation,” Geneva, Switzerland, Tech. Rep., 2017. [Online]. Available: https://www.diplomacy.edu/sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf

[21] The Shanghai Cooperation Organisation, “About The Shanghai Cooperation Organisation SCO.” [Online]. Available: http://eng.sectsco.org/about_sco/

[22] L. P. Muller, “Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities,” Norwegian Institute of International Affairs, Oslo, Norway, Tech. Rep., 2015. [Online]. Available: https://brage.bibsys.no/xmlui/bitstream/id/331398/NUPI+Report+03-15-Muller.pdf

[23] UK Foreign & Commonwealth Office (FCO), “Cyber Security Capacity Building Programme 2018 to 2021,” 2018. [Online]. Available: https://www.gov.uk/government/publications/fco-cyber-security-capacity-building-programme-2018-to-2021

[24] The Global Cyber Security Capacity Centre (GCSCC), “Cybersecurity Capacity Portal,” 2018. [Online]. Available: https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/gfce

[25] International Telecommunication Union (ITU), “Index Of Cybersecurity Indices.” International Telecommunication Union (ITU), Geneva, Switzerland, Tech. Rep., 2017. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/2017_Index_of_Indices.pdf

[26] BSA and The Software Alliance, “Asia-Pacific Cybersecurity Dashboard,” Tech. Rep., 2015. [Online]. Available: http://cybersecurity.bsa.org/2015/apac/

[27] Fergus et al. Hanson, “Cyber Maturity in the Asia Pacific Region,” Australian Strategic Policy Institute (ASPI), Tech. Rep., 2017. [Online]. Available: https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017

[28] M. Hathaway, C. Demchak, J. Kerben, J. Mcardle, and F. Spidalieri, “Cyber Readiness Index 2.0,” Potomac Institute for Policy Studies, Virginia USA, Tech. Rep. November, 2015. [Online]. Available: http://www.potomacinstitute.org/images/CRIndex2.0.pdf

[29] International Telecommunication Union, “Global Cybersecurity Agenda (GCA),” 2017. [Online]. Available: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

[30] The World Bank Group, “The World Bank Group Annual Report Regional Perspective. LAC region. 2017,” 2017. [Online]. Available: http://www.worldbank.org/en/about/annual-report/region-perspectives#a

[31] The Inter-American Development Bank (IDB) and the Organization of American States (OAS), “Observatory Of Cybersecurity In Latin America And The Caribbean,” 2016. [Online]. Available: http://observatoriociberseguridad.com/graph/countries//selected//0/dimensions/1-2-3-4-5

[32] N. Kshetri, Cybercrime and Cybersecurity in the Global South. London: Palgrave Macmillan, 2013, vol. 53, no. 9. [Online]. Available: https://doi.org/10.1057/9781137021946_7

[33] Symantec and Organisation of American States (OAS), “Cyber Security Trends In LAC,” Symantec, Organisation of American States (OAS), Tech. Rep., 2014. [Online]. Available: https://www.thegfce.com/initiatives/c/cyber-security-initiative-in-oas-member-states/documents/publications/2014/06/01/latin-america-and-caribbean-cyber-security-trends

[34] International Telecommunication Union and ABI Research, “Global Cybersecurity Index 2014 & Cyberwellness Profiles,” International Telecommunication Union ABI Research, Geneva, Switzerland, Tech. Rep., 2015. [Online]. Available: www.itu.int

[35] Control Risks, “RiskMap Americas Region,” Control Risks, Tech. Rep., 2018. [Online]. Available: https://www.controlrisks.com/riskmap-2018/maps

[36] Council of Europe (CoE), “Convention on Cybercrime,” pp. 1–22, 2001. [Online]. Available: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

[37] “The Meridian Process,” 2016. [Online]. Available: https://www.meridianprocess.org/

[38] GFCE and Meridian, “Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers,” 2016. [Online]. Available: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

[39] F. Assolini, “Beaches, carnivals and cybercrime: a look inside the Brazilian underground,” Kaspersky Lab, Tech. Rep., 2015.

[40] The World Bank Group WBG, “WBG World Bank national accounts data and the OECD national accounts data files.” 2018. [Online]. Available: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2016&locations=BR-MX&start=1990&view=chart