



# Cybersecurity capacity-building: cross-national benefits and international divides

S. Creese, W. H. Dutton, P. Esteve-González & R. Shillair

To cite this article: S. Creese, W. H. Dutton, P. Esteve-González & R. Shillair (2021) Cybersecurity capacity-building: cross-national benefits and international divides, Journal of Cyber Policy, 6:2, 214-235, DOI: [10.1080/23738871.2021.1979617](https://doi.org/10.1080/23738871.2021.1979617)

To link to this article: <https://doi.org/10.1080/23738871.2021.1979617>



© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 20 Oct 2021.



Submit your article to this journal [↗](#)



Article views: 4712



View related articles [↗](#)



View Crossmark data [↗](#)

# Cybersecurity capacity-building: cross-national benefits and international divides

S. Creese <sup>a</sup>, W. H. Dutton <sup>a</sup>, P. Esteve-González <sup>a</sup> and R. Shillair <sup>b</sup>

<sup>a</sup>Global Cybersecurity Capacity Centre, Department of Computer Science, University of Oxford, Oxford, UK;

<sup>b</sup>Quello Center, Michigan State University, East Lansing, MI, USA

## ABSTRACT

The growing centrality of cybersecurity has led many governments and international organisations to focus on building the capacity of nations to withstand threats to the public and its digital resources. These initiatives entail a range of actions that vary from education and training to technology and related standards, as well as new legal and policy frameworks. While efforts to proactively address security problems seem intuitively valuable, they are new, meaning there is relatively little research on whether they achieve their intended objectives. This paper takes a cross-national comparative approach to determine whether there is empirical support for investing in capacity-building. Marshalling field research from 73 nations, the comparative data analysis: (1) describes the status of capacity-building across the nations; (2) determines the impact of capacity-building when controlling for other key contextual variables that might provide alternative explanations for key outcomes and (3) explores the factors that are shaping national advances in capacity-building. The analysis finds a low, formative status of cybersecurity capacity in most of the nations studied and also shows that relatively higher levels of maturity translate into positive outcomes for nations. The study provides empirical support to international efforts aimed at building cybersecurity capacity.

## ARTICLE HISTORY

Received 27 March 2021

Revised 28 July 2021

Accepted 4 August 2021

## KEYWORDS

Cybersecurity capacity;  
capacity-building;  
cybersecurity measures;  
cybersecurity stakeholders

## Introduction

The global diffusion and growing centrality of information and communication technologies (ICTs) have raised concerns over the security of digital devices, data, networks, platforms and ICT services – what has been broadly referred to as digital security or ‘cybersecurity’. While literally hundreds of definitions of cybersecurity have been offered (Maurer and Morgus 2014), the telecommunications sector of the ITU composed an early and widely accepted definition of cybersecurity as ‘the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches,

**CONTACT** R. Shillair  [shillai7@msu.edu](mailto:shillai7@msu.edu)

We thank the Organization of American States (OAS) for its helpful comments on earlier drafts and its collaboration implementing the CMM. This article was presented at the 2020 Closing the Gap conference (Cyber Direct) and at the TPRC48 conference held in Washington DC, 19 February 2021 (Creese et al. 2020).

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation, and user's assets' (ITU-T 2008, 2). In this broad sense, cybersecurity is an objective of all nations. That said, how can nations develop policies and practices to protect it?

An increasingly credible approach to this issue is building greater cybersecurity capacity, which entails 'the technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor' (Clark, Berson and Lin 2014, 9). The question then becomes whether capacity-building matters, which is the focus of this study.

Security issues are not new. However, in the early years of computing, 'computer security' was addressed in most circumstances by an organisation's information technology (IT) team, which often had the expertise and facilities to secure physical and electronic access to computing equipment and services within their organisation. As computing has moved toward 'resource-sharing systems' that allow many people to use the same system, security issues have become more complex (Ware 1970, xv). With the growing use of such systems tied to increasingly critical functions, and connected to the internet, responsibility for security has moved well beyond the reach of any single organisation's IT team. It can involve a diverse range of institutions and individuals across the world, including over four and a half billion internet-users, representing over half the world's population. Moreover, approaches to security are no longer as predominately technical, since they increasingly involve law and policy as well as the skills and practices of users, shaped by the diversity of cultures and societies online and around the world. Also, as the internet has become more central to everyday life and work, there is an increased recognition that security cannot simply be a reaction to problems, but should be anticipating security problems to increase resilience when they occur.

This increasing focus on the proactive role of multiple actors in providing a more secure and resilient system of digital technologies and services has become centred on initiatives to build 'cybersecurity capacity' (Baram et al. 2017; Cohen 2017). There are multiple perspectives on how best to enhance cybersecurity capacity, which has led to several different approaches in industry and academia, often based on prescriptive models for identifying the basic elements involved in building cybersecurity capacity. These models provide a basis for assessing the capacity of nations.

Reviews of nations that are based on these prescriptive models of cybersecurity capacity are designed to enable nations to raise their maturity level, such as by the identification of strengths and weaknesses that enable the prioritisation of investment in initiatives designed to improve capacity. But do such reviews and the investments they support pay off for nations? The expectation is that higher levels of maturity in cybersecurity capacity-building will result in concrete social and economic benefits for nations, such as in increased use of the internet in households, government and business. Critically assessing this expectation is the key focus of this analysis.

This analysis of the impact of cybersecurity capacity-building is anchored in data collected by one of the largest projects established to gauge the cybersecurity capacity of nations – Oxford's Global Cyber Security Capacity Centre (GCSCC). Its Cyber Security Capacity Maturity Model (CMM) provides a basis for a growing set of national reviews, gauging the maturity of capacity-building in over 70 nations. While the reviews are conducted to guide further development of capacity in each nation, the field research data

collected for these reviews also yields original data on the present state of cybersecurity capacity-building in each of the countries reviewed. This paper employs this field research data to develop an indicator of capacity, what we call a cybersecurity capacity scale that we then use to examine the impact of capacity-building, and the set of factors shaping national capacity-building, such as the wealth of nations.

### ***Studies of capacity-building***

Cybersecurity capacity-building is a relatively new area for research. Major initiatives include the development of a Cyber Readiness Index designed to 'evaluate a country's maturity and commitment to cybersecurity' (Spidalieri 2015, 4) and an approach developed by the Belfer Center for Science and International Affairs at the Harvard Kennedy School (Hathaway 2013), which has been applied to US states and in nations outside the USA. The National Institute of Standards and Technology (NIST) has developed a NIST Cyber Security Framework (Almuhammadi and Alsaleh 2017). Fully a dozen frameworks have been developed and reviewed (Azmi, Tibben and Winn 2018).

Measuring cybersecurity capacity-building efforts in a nation involves experts from many different disciplines, sectors and specialisations. Bringing these individuals together and finding measures or indicators they agree upon is one of the many challenges to assessing capacity. Given such challenges to any cybersecurity assessment initiative, there have been a limited number of reviews of capacity initiatives (Table 1). These initiatives use different frameworks, models, indices and tools to measure different issues related to cybersecurity, and they differ as well on the sample of countries, the methodologies they employ, and the availability of their outcomes.

The relatively recent advent of cybersecurity frameworks has led to a lack of systematic empirical research on the actual impact of cybersecurity capacity-building. Research has also been inhibited by the inherent difficulty of developing reliable indicators of cybersecurity capacity (Rosenzweig 2019) and its impact, given the many factors involved in cybersecurity and the reluctance of organisations to share such information (Solove and Citron 2017). An exception is a study by Makridis and Smeets (2019) of the role of institutional threats and returns in shaping changes in cyber readiness, which finds no significant relationship between factors such as wealth (GDP) and shifts over time in cyber-readiness indexes. They found that 'states that have more resources available to allocate are not at a systematic advantage in their cybersecurity investments.' (Makridis and Smeets 2019, 1). This suggests there are other factors beyond available resources that drive priorities in cybersecurity capacity-building.

### ***The Oxford project on cybersecurity capacity-building***

To develop empirical indicators for informing nations and comparative research, the Global Cyber Security Capacity Centre (GCSC) at Oxford University developed one of the earliest models of what is entailed in achieving different levels of maturity in capacity-building – the Cybersecurity Maturity Model (CMM). This was first published in late 2014 and has been systematically revised and refined since then to accommodate changes in technology and security issues. The CMM provides a basis for gauging a country's level of maturity in capacity-building through a systematic review process across multiple dimensions of cybersecurity (Table 2).

**Table 1.** Cybersecurity capacity-building indices, frameworks, tools and other initiatives.

Organisation (year started)	Model/tool	Description
E-Governance Academy (2002)	National Cyber Security Index	Index 'to measure countries' preparedness to prevent cyber threats' and manage cyber incidents based on public evidence of legal acts, official documents and official websites. <sup>a</sup>
Global Forum on Cyber Expertise (GFCE) (2015)	Global CSIRT Maturity Framework	Maturity model framework to guide national CIRTs and enhance global cyber incident management capacity. <sup>b</sup>
International Telecommunication Union (ITU) (2014)	Global Cybersecurity Index	Index to measure countries' commitment to cybersecurity based on an online questionnaire. <sup>c</sup>
MITRE (2014)	National Cyber Strategy Development and Implementation	Programme to assess cyber capacity-building through a field forum (interviews, seminars or workshops). <sup>d</sup>
Oxford's GCSCC (2015)	Cybersecurity Capacity Maturity Model for Nations	Framework to assess countries' capacity maturity on five different dimensions crucial to building cybersecurity based on field interviews, focus groups and desk research. <sup>e</sup>
Potomac Institute for Policy Studies (2015)	Cyber Readiness Index	Index to assess countries' cyber readiness through indicators based on facts and primary resources (empirical research and documentation). <sup>f</sup>
World Bank (WB) (2016)	Combatting Cybercrime	Toolkit for emerging economies to assess their current capacity and a source of good international practices to combat cybercrime. <sup>g</sup>
World Economic Forum (WEF) (2001)	Networked Readiness Index	Aggregated indicator of the impact of ICT in countries based on the WEF's Executive Opinion Survey and data from international organisations (ITU, WB and UN agencies). <sup>h</sup>

<sup>a</sup>E-Governance Academy, founded in 2002, <https://ncsi.ega.ee/methodology/>, accessed on 28 April 2020.

<sup>b</sup>GFCE, launched through a Hague declaration in 2015, [https://thegfce.org/wp-content/uploads/2020/05/MaturityFrameworkforNationalCSIRTsv1.0\\_GFCE.pdf](https://thegfce.org/wp-content/uploads/2020/05/MaturityFrameworkforNationalCSIRTsv1.0_GFCE.pdf), accessed on 21 May 2020.

<sup>c</sup>ITU, issuing global cybersecurity index since 2014, <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>, accessed on 28 April 2020.

<sup>d</sup>MITRE, a US federally funded non-profit has given technical guidance since 1958, <https://www.mitre.org/publications/project-stories/mitre-strengthens-cyber-capacity-of-developing-nations>, accessed on 21 May 2020.

<sup>e</sup>GCSCC, founded in 2015 <https://gcsc.web.ox.ac.uk/the-cmm>, accessed on 21 May 2020.

<sup>f</sup>Potomac Institute for Policy Studies, started in 2015, <https://potomac institute.org/images/CRIndex2.0.pdf>, accessed on 28 April 2020.

<sup>g</sup>WB, the WB global cybersecurity capacity programme funded by the Korea-World Bank Group Partnership Facility started in 2016 issues the cybercrime reports, <http://www.combattingcybercrime.org/>, accessed on 21 May 2020.

<sup>h</sup>WEF, reports on global information technology issued since 2001, [http://www3.weforum.org/docs/GITR2016/GITR\\_2016\\_full%20report\\_final.pdf](http://www3.weforum.org/docs/GITR2016/GITR_2016_full%20report_final.pdf), accessed on 28 April 2020.

**Table 2.** CMM dimensions of cybersecurity capacity-building and associated factors.

Dimension	Factors that define specific indicators of capacity-building
1. Policy and strategy	National cybersecurity organisation, incident response, critical national infrastructure protection, emergency preparedness, cyber defence, communications redundancy
2. Culture and society	Cybersecurity mindset, cybersecurity awareness, confidence and trust online, privacy online
3. Knowledge-building	Cyber education, training, boardroom understanding of cybersecurity, skills, research and development
4. Legal and regulatory	Legal and regulatory frameworks, criminal justice system, responsible disclosure
5. Technology	Implementation of standards in ICT security, procurement, and software development, internet infrastructure resilience, cybersecurity products in the marketplace

While initiated at the GCSCC, the development and deployment of the model have been informed by international expert consultation and collaboration to review and advise the GCSCC on each aspect of the CMM. As explained in Creese et al. (2021), this

was part of a strategy to mitigate any risk of imposing an ethnocentric criteria of evaluation. For example, the design of each of its aspects has been informed by international expert consultation through two reviews of the CMM, the 2016 CMM edition being the latest review used in this study. Each of the five dimensions is defined by multiple factors, resulting in a total of twenty-four factors. The operationalisation of these factors entails data collection of over 200 indicators that are evaluated in each country assessment. To mitigate any risk of misinterpretation and ensuring that local knowledge is embedded in the reviews, the GCSCC review process involves governments and national stakeholders in reaching a mutual agreement and validating maturity levels. The report is then owned and published by the respective government.<sup>1</sup> This often adds up to a year for the completion of a review; however, this process increases the quality of the assessment as there has been mutual input and agreement. This process results in capacity being gauged for the nations in the sample over a small window of several years, rather than at the same point in time for all the nations.

Consultation and collaboration with international experts and stakeholders have resulted in the establishment of an assemblage of centres that has lead deployment of the CMM in their respective regions. This includes the Oceania Cyber Security Centre (OCSC), Melbourne, funded by the State Government of Victoria, and the Cybersecurity Capacity Centre for Southern Africa (C3SA), funded by an alliance of the UK government and the Norwegian Ministry of Foreign Affairs.

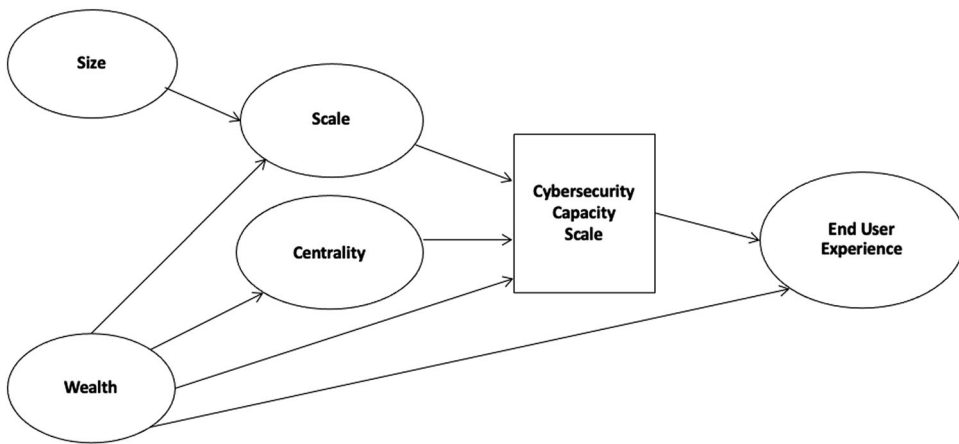
The first reviews of nations using the Oxford CMM were begun in 2015 (GCSCC 2019, 2). However, it was not until 2020 that the project had completed a sufficient number of reviews to undertake a strong empirical study of the impact of different levels of capacity-building. By 2020, CMM reviews had been conducted in over 70 nations across all regions of the world. In most countries, a review team from the university visited the country to conduct a set of interviews and modified focus groups involving multiple stakeholders from government, business and industry, and civil society. Each of these groups assembled different sets of stakeholders who were asked to describe the status of developments across selected dimensions of the model. Together, the groups informed the team on the status of all aspects of the CMM.

In some nations across Latin America and the Caribbean, a review based on the same CMM was conducted by the Organization of American States, in collaboration with Oxford University but through an online self-administered questionnaire which was an adapted version of the CMM. At the initial stage of these reviews in the region, given it was a new tool, this was coupled with in-country workshops to explain the CMM in a sample grouping of OAS member states (delivered in both English and Spanish).

To capture levels of maturity across such a wide range of elements, interviews and modified-focus groups sought to elicit indications of maturity of over fifty aspects of multiple factors across the five dimensions of cybersecurity capacity-building (Table 2). GCSCC and OAS reviews of cybersecurity capacity-building across these five dimensions of the CMM have enabled this research to gauge the maturity level of each of these dimensions in 73 nations when the national CMM reviews were conducted.

### *A framework for the empirical analysis of cybersecurity capacity*

Using surrogate indicators of capacity-building, Dutton et al. (2019) found evidence of capacity-building having an independent and positive impact on the end-user's



**Figure 1.** Theoretical framework. Adapted from Dutton et al. (2019).

experience, including positive impacts on overall utilisation of the internet, controlling for key variables such as the wealth of nations. In that analysis, a model was used that considered societal and structural forces as part of the overall ecosystem that impacts the experiences of cybersecurity threats by end-users. That study found evidence of a positive role for capacity-building over a wider number of end-users' experiences. (Figure 1).

In this current analysis, for the first time, we use the GCSCC CMM field-based indicators along with the external secondary data to provide an empirical analysis of the impacts of capacity-building on ICT usage across sectors of users. The central question is whether indicators of cybersecurity capacity, derived from field research in 73 nations, will have a direct and positive impact on the utilisation of ICTs when controlling for key antecedent and moderating variables.

The key antecedents are size, wealth, scale and centrality of internet-use in the country.<sup>2</sup> The size of a nation is its overall population, and its wealth is indicated by GDP per capita. These factors are shown in the model to impact the scale and centrality of internet use. Scale is the number of internet users in a nation and centrality is the percentage of the population using the internet. The higher the centrality, the more likely the internet can be used for more significant activities, such as banking or shopping. A higher scale of internet use does not necessarily translate into greater centrality – the number of internet users in a nation does not mean that a larger percentage of the population use the internet. Larger nations will have more internet users (scale), and wealthier nations will be expected to have larger proportions of internet users (centrality). When controlling for size, wealth, scale and centrality, will capacity have a positive and significant impact on patterns of internet use and impact?

### Comparative data collection

The present analysis is based on cross-sectional data collected from capacity reviews conducted in 73 nations, all reviewed based on the CMM. As explained above, the CMM framework gauges the maturity of a country in relation to its cybersecurity capacity across five different dimensions (Table 2). Each dimension consists of different factors, and each factor has multiple 'aspects' which are the most granular units for which maturity is

calibrated by a set of direct indicators of cybersecurity capacity. According to the increasing maturity scale in GCSCC (2016), these five maturity stages are: (1) start-up, (2) formative, (3) established, (4) strategic and (5) dynamic. The maturity stage of each aspect is characterised by different indicators of capacity, but the indicators of maturity at each maturity stage follow a common definition across aspects allowing for their comparison (GCSCC 2016, 7). This paper considers each aspect as an ordinal variable that can take a value between 1 and 5.

As noted above and described in Creese et al. (2021), two different approaches to data collection were used to gauge the national cybersecurity capacity maturity of all aspects in the CMM. The main approach involved field research and the second was based on questionnaires.

### ***Field research through modified-focus groups and interviews***

The field research approach was based on the GCSCC team conducting selected in-depth interviews and employing modified-focus groups using mixed methods to assess maturity stages for each aspect based on qualitative coding (Williams 2003; Knodel 1993; Krueger and Casey 2014). The GCSCC team sought to open discussion and gain information about each dimension of cybersecurity capacity from multiple groups of stakeholders. Rather than trying to generate an overly wide range of answers, the groups were selected and moderated to focus on information that would enable them to determine the best rating for each aspect of the CMM model.

This process involved a review team from Oxford (or a partner institution)<sup>3</sup> travelling to each country to conduct about ten modified-focus group sessions with representatives of national stakeholder clusters (see Box 1).<sup>4</sup> These representatives were identified before the field visit and clustered into modified focus group sessions based on their expertise in each dimension of the CMM.

#### **Box 1. Stakeholder clusters participating in the modified-focus groups.**

Academia, civil society groups, and internet governance; Criminal justice and law enforcement; Cyber task force or representatives responsible for developing cybersecurity strategy; Cybersecurity incident response teams (CSIRT); Defence and intelligence community; Government ministries; Information technology leaders from government and the private sector; International partners; Legislators and other policy owners, such as appointed experts; Private sector and business; Representatives of critical national infrastructures

Each session of stakeholders focused on one or two dimensions of the model. Sessions were recorded, with the consent of all participants, and used solely to write the review.<sup>5</sup> For more details on the sessions, see Creese et al. (2021). Across all 10 modified focus groups, indicators tied to over 50 aspects of all the factors related to the 5 dimensions were covered. The evidence provided in the different sessions was triangulated with a separate desk research phase. The resulting maturity stages are used as data in the present research analysis.

### ***Online tool administered by the Organization for American States***

The GCSCC at Oxford University collaborated with the Organization of American States (OAS) and the Inter-American Development Bank (IDB) to develop measurements that

could be administered online. These were based on the CMM and adapted to fit the specific regional context and concerns in the Latin American and Caribbean countries. The online tool provided questions to be completed by OAS member states, asking their national point of contact in each country to distribute the survey to relevant national experts with the knowledge to provide the most reliable information about cybersecurity in the country, such as references in support of their response (including links to websites and documents). Multiple experts and knowledgeable officials in each country participated, but the questionnaire was a fact-finding questionnaire rather than a sample survey of opinion. The OAS team reviewed the responses that were collected and used domain experts to research and complete any uncertain or missing values from the data provided. The generated scores were then sent to each member state for further validation, and the results were published by the IDB and OAS and used for analysis of cybersecurity preparedness (IDB 2020).

### **Combined data set**

Before combining the data from IDB (2020) with the GCSCC dataset, the research team at GCSCC looked for anomalies that might be attributed to the different methodological approaches or the process followed in particular national studies. This led to the identification of only one nation as an outlier. In that nation, outlying scores on maturity levels could not be validated by additional interviews and documentation, leading observations for this country to be removed from the cross-national data set. With that one exception, there was remarkable coherence, such as that based on the analysis of inter-item reliability and construct validity across the nations in the sample. The clear and reliable patterns indicated that the data from the two methods (42 countries reviewed once by the GCSCC during the period 2015–2020 and 31 countries surveyed by OAS and IDB, 2020) could be validly combined.

Table 3 describes the 73 countries in the study's sample by region and income classification, as defined by the World Bank (2019) during the year of each nation's CMM review.

### **Creating maturity scores for each level of analysis for a national score**

This analysis used multivariate approaches to determine whether each aspect in a given factor was sufficiently correlated with other aspects to reliably be combined. With a few rare exceptions, the aspect scores within each factor were correlated at a sufficiently high level to justify combining them into a single average for each factor. Given reliable scales

**Table 3.** Description of the 73 countries in the sample.

Region	Obs.	Income	Obs.
Sub-Saharan Africa	15	Low and Lower-Medium	29
Middle East and North Africa	1	<i>Low: 8</i>	
Europe and Central Asia	14	<i>Lower-Medium: 21</i>	
South Asia	3	Upper-Medium	33
East Asia and Pacific	9	High	11
Latin America and the Caribbean <sup>a</sup>	31		
Total	73	Total	73

<sup>a</sup>Collected by the Organization of American States, based on the GCSCC's CMM.

for each factor, we then analysed all factors by their respective dimension. Again, the factors were highly correlated with other factors in their respective dimension of the CMM. This justified combining the factors to create an average maturity score for each dimension. Averages were used rather than other measures, such as the minimum maturity stage for each dimension, in order not to lose meaningful variance in maturity levels – variance that would be lost in rounding to a whole number representing the judged maturity level.

Following the aspect-factor-dimension hierarchy of our data, we then created an average score across all five dimensions, given they were also sufficiently correlated to create a reliable single indicator of a nation's nationally weighted average maturity stage (Table 4). The average maturity stage based on all five dimensions thus led to a single metric to represent a nation's capacity – the Cybersecurity Capacity Scale (CCS). This CCS is the variable that we use as a summary indicator of each nation's overall level of cybersecurity capacity.

To test the external validity of this single CSS indicator, the relationships between CCS and other alternative indicators of national cybersecurity were analysed. As Table 5 shows, there was a positive and significant correlation with other reputable measures of cybersecurity: the Global Cybersecurity Index from ITU, the Networked Readiness Index from WEF, and the number of secure servers from Netcraft.<sup>6</sup> These correlations support the external validity of our scale of cybersecurity capacity – CCS.

### *The distribution of cybersecurity maturity*

A guiding question of our comparative research was whether nations were developing strong cybersecurity capacity. The distribution of maturity scores suggests that much work remains to be done across all the nations studied. Figure 2 represents the distribution of CCS with its histogram. The countries in the sample have a low average score (1.67), indicating that these nations have a maturity stage below formative in the average of all the cybersecurity dimensions included in the CMM. As the histogram shows, 58 countries (almost 80% of the sample) have a CCS value below 2 (this is a formative maturity stage). However, there is variability across nations as the minimum and maximum observations range between the maturity stages 'start-up' (1.03) and slightly above 'established' (3.28). In summary, most nations were below a formative stage of capacity development.

### *A digital divide in capacity-building*

CCS maturity levels were analysed using a scatter plot that examined the relationship between wealth, measured by GDP per capita, and CCS. The figure shows both the

**Table 4.** Pearson's correlation coefficients between the CMM dimensions.

Dimensions	D1	D2	D3	D4	D5
D1 Policy and strategy	1.00	–	–	–	–
D2 Culture and society	0.83	1.00	–	–	–
D3 Knowledge-building	0.77	0.84	1.00	–	–
D4 Legal and regulatory	0.78	0.88	0.78	1.00	–
D5 Technology	0.85	0.81	0.75	0.79	1.00

All coefficients  $p < 0.001$ .

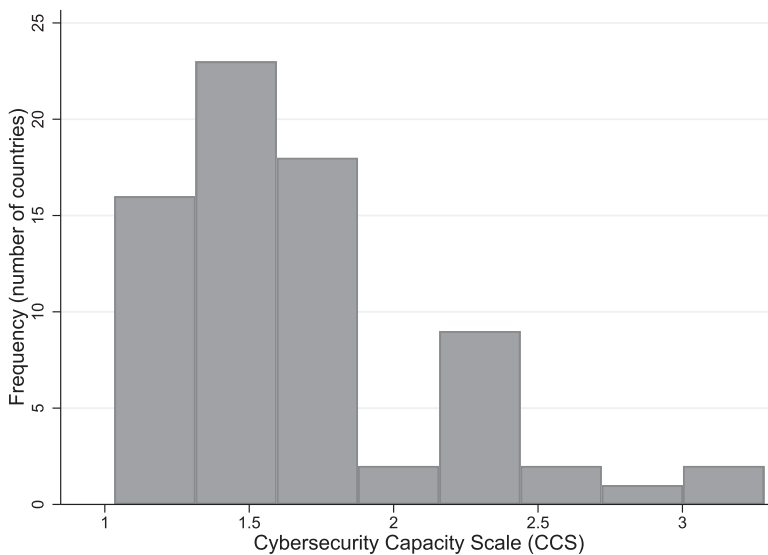
**Table 5.** Pearson's correlation coefficients between CCS and alternative indicators.

Indicators	CCS	Countries <i>n</i>
Global Cybersecurity Index (ITU)	0.67***	72
Networked Readiness Index (WEF)	0.80***	58
Number of secure servers, log (Netcraft)	0.82***	72

\*\*\* $p < 0.001$ .

relatively low levels of maturity across all nations, as discussed above, but also a relationship of CCS with wealth. There is a clear digital divide in capacity-building where economic resources shape cybersecurity capacity in ways that might reinforce the advantages of wealthier nations. However, it appears that wealth alone was not a sole determinant, as there is a wide range of CCS development in the mid GDP per capita level. This might demonstrate, as Calderaro and Craig (2020) found, that other factors, such as scientific development and educational efforts, are influencing CCS development.

However, in contrast to our findings, Makridis and Smeets (2019) did not find a significant relationship between the wealth of nations, an aspect of what they called 'institutional capacity', and cyber readiness, which they used as an indicator of cybersecurity capacity. The relationship between wealth and capacity-building found in this study could be a consequence of our use of different indicators, or of using path analysis that captures direct and indirect effects of wealth on the centrality of internet use. Given our sample size, we also use a minimal number of variables, eliminating those that are essentially redundant to (i.e. highly correlated with) our strongest variables, such as wealth, as a means to reduce any issues of collinearity. Makridis and Smeets (2019) were also focused on shifts in readiness over time periods rather than its absolute level at a specific point in time, which could also explain the fact that wealth did not



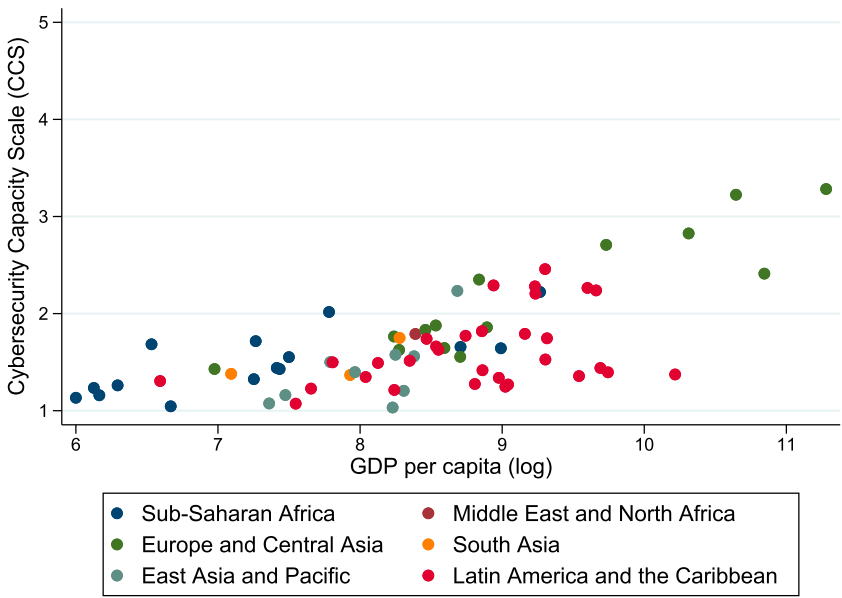
**Figure 2.** Histogram of CCS. The 73 observations in the sample were divided into eight bins with a width of 0.28 units of the variable CCS.

clearly explain changes in readiness. That said, we are confident in the robustness of our analysis linking wealth with levels of capacity-building (Figure 3).

*The empirical fit with the theoretical framework*

The theoretical framework described in Figure 1 conceptualises the important determinants of cybersecurity capacity to be size and wealth of a country, the scale of the national cyberspace infrastructure, and the centrality of this infrastructure. We use the variables GDP per capita (wealth), total population (size), number of internet users (scale), and percentage of internet users (centrality) as proxies of these determinants. Three of these variables (size, wealth and scale) are highly skewed as the country sample includes many low-income nations. To correct for potential error, we used the natural logarithm of these three variables.

The outcomes of the model focus on the impact of cybersecurity capacity. For these outcomes, we consider three indicators of ICT adoption and usage by the private sector (NRI: business usage), government (NRI: government usage), and individuals (NRI: individual usage). Employing the Network Readiness Usage Indexes<sup>7</sup>, private-sector online usage includes ‘firms with a Web site’, ‘ease of doing business’, ‘professionals, technicians and associate professions’, ‘business use of digital tools’ and ‘R&D expenditure by business’. Governmental usage includes indicators: ‘government online services’, ‘publication and use of open data’, ‘government promotion of investment in emerging technologies’ and ‘R&D expenditure by governments and higher education’ (ITU 2019). Individual use includes ‘number of internet users’,<sup>8</sup> ‘active mobile-broadband subscriptions’<sup>9</sup>, ‘use of virtual social networks’<sup>10</sup>, ‘tertiary enrolment’, ‘adult literacy rate’ and ‘ICT skills’ (Dutta and Lanvin 2020, 202)<sup>11</sup>. Finally, we consider voice and accountability from the World Bank GovData360 (WB, 2020b) to capture the citizens’ perception of



**Figure 3.** Scatter plot relating CCS and GDP per capita.

freedom as another relevant experience of end-users. Table 6 describes all the variables used in this empirical analysis.

### Data Analysis methods

We used complementary approaches to the quantitative analyses to determine the fit of our data with the hypothesised framework in Figure 1. The first was multivariate linear regressions to determine whether the CCS had a direct relationship with outcomes, controlling for possible moderating variables. The second was the testing of path models for each of our dependent outcome variables to more fully capture the dynamics of any relationship between CCS and its outcomes.

### Linear regressions

The first method employed is Ordinal Least Square (OLS) regressions with heteroscedasticity-robust standard errors. An OLS regression takes the form (1) and estimates the dependent variable ( $y_i$ ) for each observation  $i$  as a linear function of  $J$  independent variables ( $x_{ji}$ ), each one with its corresponding coefficient ( $\beta_j$ ) and an additive error ( $u_i$ ). Coefficients  $\beta_j$  correspond to the marginal effect of each independent variable. When

**Table 6.** Variable definitions and descriptive statistics.

Variable	Definition	<i>N</i>	Mean (S.Dv.)	Min	Max	Data source
CCS	Weighted mean of the maturity stage of all aspects in the CMM, following the aspect/factor/dimension hierarchy; values between 1 and 5 (GSCC and IDB and OAS 2016)	73	1.67 (0.48)	1.03	3.28	Own calculus
Wealth	Natural logarithm of the Gross Domestic Product divided by population; constant 2010 US dollars (WB and OECD)	73	8.42 (1.11)	6.00	11.28	Own calculus with data from WB (2020a) <sup>9</sup>
Centrality	Percentage of population that has used the internet in the last three months (ITU)	73	48.59 (23.62)	4.71	98.26	WB (2020a) <sup>10</sup>
Scale	Natural logarithm of the number of internet-users; internet-users calculated with <i>internet-users</i> and <i>total population</i>	73	14.34 (2.11)	9.73	18.65	Own calculus with data from WB (2020a)
NRI: business usage	Index number measuring the business usage pillar of the Networked Readiness Index (NRI); values between 1 and 7 (WEF)	58	3.56 (0.58)	2.60	6.13	WEF (2019) <sup>11</sup>
NRI: government usage	Index number measuring the government usage pillar of the NRI; values between 1 and 7 (WEF)	58	3.62 (0.68)	2.24	5.20	WEF (2019)
NRI: individual usage	Index number measuring the individual usage pillar of the NRI; values between 1 and 7 (WEF)	58	3.54 (1.25)	1.62	6.60	WEF (2019)
Size	Natural logarithm of the number of residents in a county regardless of legal status or citizenship (UN)	73	15.23 (2.13)	10.85	19.37	Own calculus, WB (2020a)
Voice and accountability	Citizens' perceptions of their participation in 'selecting their government, freedom of expression, freedom of association, and freedom of media'	73	0.23 (0.61)	−1.14	1.62	WB (2020b)

we consider the natural logarithm of an independent variable, the interpretation of coefficient  $\beta_j$  corresponds to the change in  $E[y|x]$  as a proportionate change in  $x_{ji}$  (see, e.g., Cameron and Trivedi 2010, 85).

$$y_i = \beta_1 x_{1i} + \beta_2 x_{2i} + \dots + \beta_j x_{ji} + u_i \quad (1)$$

To estimate the model through OLS regressions, we need to divide the model into two parts and estimate separately the determinants of cybersecurity capacity, where CCS is the dependent variable, and the impact of cybersecurity capacity on its outcomes, where CCS is an independent variable.

### Path analyses

In the second approach, we used path analysis to take account of the more complete model of multivariate relationships. For this, we used structural equation modelling as a method to incorporate latent variables and test the larger theoretical model, techniques that move beyond the limitations of traditional OLS models. This is a method that is growing in use in many fields, such as information systems research, as it allows for a more robust analysis of complex systems (Henseler, Hubona and Ray 2016). We use the consistent partial least squares (PLSc) as it provides additional levels of correction to estimate the path coefficients for endogenous latent variables and to correct for attenuation (Dijkstra and Hensler 2015). As stated by Dijkstra and Hensler (2015), 'for every pair of latent variable scores  $\tilde{n}_i$  and  $\tilde{n}_j$ , the consistent correlation  $\text{cor}(\tilde{n}_i, \tilde{n}_j)$  is calculated as follows:'

$$\text{cor}(n_i, n_j) = \frac{\text{cor}(\tilde{n}_i, \tilde{n}_j)}{\sqrt{\rho_A(\tilde{n}_i) \rho_A(\tilde{n}_j)}}$$

## Results of the analyses

### OLS regressions

Table 7 displays the estimations of the first part of the model on determining cybersecurity capacity. Variables are entered one by one in the regression, through columns (1) to (3), and the three variables together explain 68% of the variance of CCS. The results show that, given the sample of countries, all the variables in the model have a positive impact on CCS, although the significance of centrality is too low to interpret its coefficient. This is probably driven by the strong correlation between this variable and wealth (0.86 Pearson's correlation coefficient, level of significance below 0.001). Wealth has the largest coefficient of the variables related to CCS. The model estimates that, all things being equal, a 1% increment in wealth would increase CCS by 0.22 units. The size of this increment is quite important considering that CCS is the average maturity stage of the five dimensions of the CMM. Similarly, *ceteris paribus*, a 1% increment in scale would increase CCS by 0.11 units.

Table 8 displays the estimations of the second part of the model that shifts to explaining the impact of CCS on four different outcomes. As the CCS includes smaller and poorer countries that are not covered by some of the NRI measures there was a lower count, yet we were able to include countries that are often overlooked in other studies.

**Table 7.** OLS regressions to explain CCS.

	(1)	(2)	(3)
Scale		0.11*** (0.01)	0.11*** (0.02)
Centrality			0.00+ (0.00)
Wealth	0.29*** (0.05)	0.29*** (0.04)	0.22*** (0.06)
Constant	−0.78 (0.40)	−2.36*** (0.40)	−1.93*** (0.53)
N	73	73	73
R <sup>2</sup>	0.44	0.68	0.68

Robust standard errors in parentheses

\* $p < 0.05$ , \*\* $p < 0.01$ , \*\*\* $p < 0.001$ .

Columns (1), (2) and (3) estimate the impact of CCS on a higher ICT usage in three sectors: individual internet users, the private sector and the public sector. CCS has a significant positive impact on each of these three dependent variables. *Ceteris paribus*, we would expect NRI: individual usage and NRI: business usage to increase by 0.60 units when CCS increases by one unit. The size of this effect is relatively important given that NRI: individual usage and NRI: business usage are index numbers that can take values between 1 and 7. The impact of CCS on NRI: government usage is even larger. For example, consider the country with the lowest value for NRI: government usage (2.24). For an identical country, but with a value of CCS exactly one unit larger, we would estimate it to have a value for NRI: government usage around 2.93.

Regarding the other independent and moderating variables, scale does not seem to have any statistically significant impact on the three usage variables; the coefficients of centrality are more statistically significant, but the size of these relationships is so small that their impacts are moot. Wealth has a positive impact on higher ICT usage by the

**Table 8.** OLS regressions to explain cybersecurity outcomes.

	NRI: individual usage (1)	NRI: business usage (2)	NRI: government usage (3)	Voice and account (4)
CCS	0.61** (0.19)	0.60* (0.28)	0.69** (0.26)	0.56** (0.18)
Scale	−0.03 (0.04)	−0.03 (0.04)	0.02 (0.05)	−0.17*** (0.03)
Centrality	0.03*** (0.01)	−0.01* (0.01)	0.00 (0.01)	−0.01+ (0.00)
Wealth	0.24+ (0.13)	0.37** (0.13)	0.04 (0.15)	0.31*** (0.08)
Constant	−0.50 (0.95)	0.58 (0.88)	1.73 (1.15)	−0.57 (0.78)
N	58	58	58	73
R <sup>2</sup>	0.88	0.53	0.39	0.67

Robust standard errors in parentheses

+  $p < 0.01$ , \* $p < 0.05$ , \*\* $p < 0.01$ , \*\*\* $p < 0.001$ .

private sector; *ceteris paribus*, a 1% increment in wealth increases NRI: business usage by 0.37 units. The model seems to explain particularly well NRI: individual usage, while the R-squared of the model is low when explaining NRI: business usage and NRI: government usage.

Finally, the results in column (4) show that the model explains 67% of the variability of the data on voice and accountability for the countries in the sample. CCS is the variable with the highest impact; all things being equal, an increment of one unit of CCS is estimated to increase voice and accountability in 0.56 units of a normal standard deviation. The size of this impact is relatively large considering that the dependent variable ranges between values  $-2.5$  and  $2.5$ . Wealth has a similar impact. However, the positive impact of CCS and wealth on voice and accountability is smaller in those countries with a larger scale, when controlling for CCS and wealth. We can only speculate that as the number of internet users increases, it is possible that individual users feel less empowered by the internet – somewhat less able to be heard and make a difference in politics.

### **Path analyses**

Structural equation modelling, and the specific instance of path analysis, is often used in testing more complex models as it helps with interpreting causality (Duncan 1966). To examine the structure and strength of variable relationships, there are several steps to check goodness-of-fit and the overall validity of measures (Fornell and Larcker 1981). The model in Figure 1 was tested under the path analysis, where the determinants of CCS and its impact can be estimated more globally.

### **Collinearity and discriminant validity tests**

Validity measures were run on all the models to check discriminant validity, collinearity (VIF) and goodness-of-fit measures. VIF levels of 1.00 would indicate no collinearity and as the number increases, collinearity increases. Although models may vary in tolerance of various VIF levels, Craney and Surles (2002) suggest that levels over 5 be treated with caution and over 10 be rejected. All our VIF measures were below 2.0.

Construct reliability for our multi-variable construct, 'outcomes: use factors', had a Cronbach's alpha of .840, along with strong loading (see Table 9), indicating high internal consistency.

### **Model fit measures**

Standardized Root Mean Square Residual (SRMR) is an absolute measure of fit, the lower the value, the better the fit. A value of zero would indicate a perfect fit. Generally speaking, a value of less than .08 of the saturated model is considered a good fit (Hu and Bentler 1999). Table 10 presents the results of the SSMR goodness-of-fit measures.

### **Path analysis of ICT use**

Internet-use in households, private industry and government are all positively shaped by higher levels of CCS. There is a strong, positive relationship between CCS and the use

factors (Figure 4). Wealth also has a strong and direct relationship with use factors, as well as indirect effects resulting from its positive association with CCS. Interestingly, when controlling for other variables, including wealth and CCS, the scale and centrality of internet use are negatively related to the vitality of usage factors. This might well indicate greater importance of CSC in nations where the internet is used on a greater scale and is more central.

### *Path analysis of voice and accountability*

The CMM defines law and policy concerning freedom of expression and other human rights as critical to building cybersecurity capacity. As Figure 5 shows, there is a strong positive association between CCS and cross-national indicators of citizen perceptions of having voice and accountability, even when controlling for all the other variables in the model. This is not inherent in the indicators used, as the elements of voice and accountability in the CCS are based on law and policy, while the dependent variable is anchored in citizen perceptions of freedom of speech (Table 6). However, we cannot know whether law and policy on expression shapes actual freedom of speech, only citizen perception.

As with respect to the vitality of use, voice is also related directly to the wealth of the country, but when controlling for other variables, there is a negative relationship between the scale of internet use and voice. People may feel that they have less voice in countries with a larger number of internet users – a small fish in a larger pond. This indicates that controlling for other variables, such as wealth, voice is lower than expected based on only the number of internet users as tapped by scale. This is also the case with the centrality of use, but the relationship between centrality and voice is not statistically significant.

## **Conclusion and discussion**

Governments and international organisations are focusing increasing attention on building the capacity of nations to withstand threats to the security of their citizens and their digital resources. These cybersecurity capacity-building initiatives entail a multidimensional range of actions to address problems, ranging from awareness-raising to technological innovations. Capacity-building at the national level offers the potential to develop a proactive approach to investing in cybersecurity. However, there are major questions surrounding the efficacy of measuring cybersecurity capacity and judging its impact on end-users.

This study was based on field research in 73 nations, which collected data across the multiple dimensions of cybersecurity capacity-building and analysed whether capacity-building had an independent effect on internet usage by individuals, governments and

**Table 9.** Item loadings for model: use outcomes.

Outer loadings: Outcome – use	Sample mean (M)	STDEV	T Statistics
nri_businusage <- Outcomes	0.747***	0.092	8.290
nri_govusage <- Outcomes	0.659***	0.079	8.310
nri_indivusage <- Outcomes	0.964***	0.039	24.750

\*\*\* $p < 0.001$ .

**Table 10.** All models' goodness-of-fit measures.

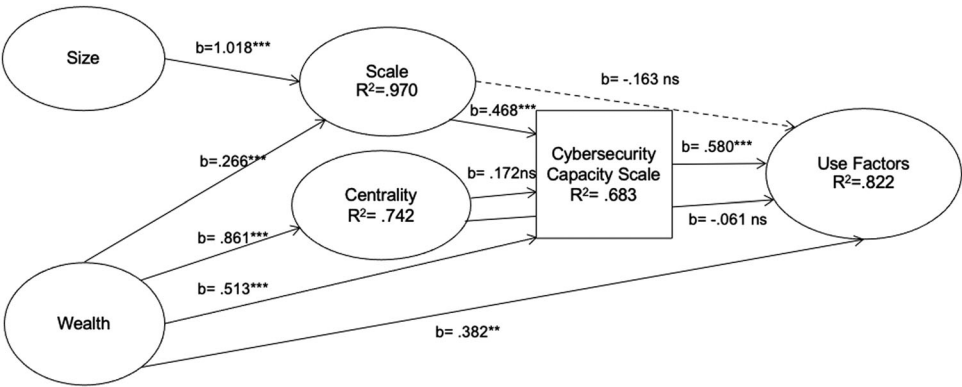
Model fit measures SRMR	Saturated model	Estimated model
SRMR Use	0.059	0.098
SRMR Voice	0.000	0.026

business. This enabled our study to use a cross-national comparative approach to understanding the impact of cybersecurity and the factors shaping it with one of the strongest data sets yet available on this phenomenon. Data focus on the status of cybersecurity capacity-building, its determinants and consequences. The findings were fourfold.

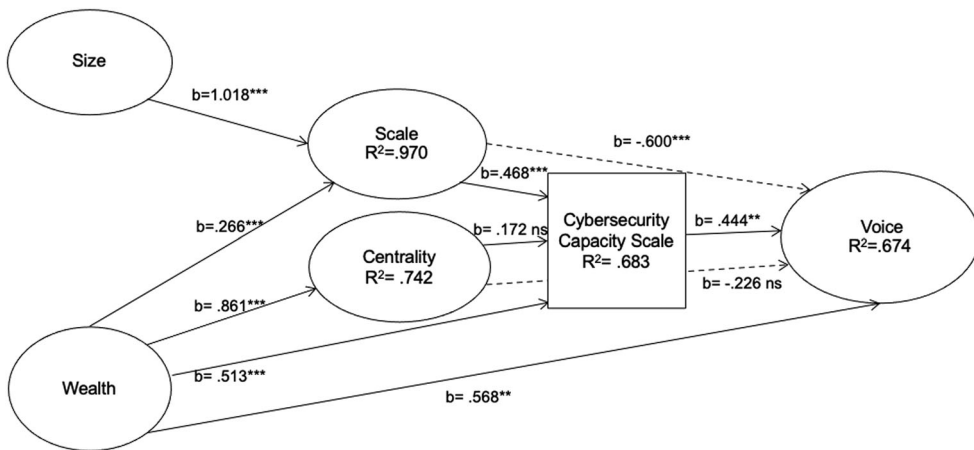
First, in describing capacity-building across the 73 nations, it was apparent that the level of capacity-building in most nations is at the very early stages of development, what was called a start-up or formative stage in the maturity model on which these assessments were based. This is critical in that it demonstrates the general need for initiatives to raise capacity, particularly in light of our findings on its positive impact on usage.

Secondly, we found a digital divide in capacity-building. There is no binary division between those with and without capacity, but there are incremental differences in capacity that are tied to the wealth of nations, as well as the scale and diffusion of the internet. However, wealth, as indicated by GDP per capita, plays a role directly and indirectly in our analysis, such as in shaping the centrality and scale of internet development. Wealth supports capacity-building but also reaps more beneficial outcomes of the internet. In such ways, the economic development of nations reinforces inequalities in capacity-building and its outcomes for nations.

That said, while the wealth of nations reinforces capacity-building and the related economic and opportunity benefits of internet usage, it is not deterministic of these outcomes. Some nations reach levels of capacity-building that are higher than would be predicted based on their wealth, and others lower. These findings build on other research, such as the World Bank development report, that explores the potential digital dividends that come from reducing the digital divide in access. In addition to improving access to the internet, there is evidence of a need to improve cybersecurity capacity as it positively shapes the outcomes of internet use (World Bank 2016). Therefore, national and



**Figure 4.** Cybersecurity capacity and impact on ICT use factors.



**Figure 5.** Cybersecurity capacity and impact on voice and accountability.

international efforts to support cybersecurity capacity-building can complement more traditional work on diminishing digital divides.

Thirdly, national choices on building capacity have implications for ICT adoption and usage as well as citizens' perceptions of freedom and accountability. Even when controlling for antecedent variables that might provide alternative explanations for the vitality of individual, business and governmental usage of ICTs, such as the wealth of nations, cybersecurity capacity-building had a strong, statistically significant and positive effect on overall use. This was supported by multivariate analyses using simple linear regressions and more complete path modelling of all the variables in our theoretical model. The patterns of relationships paint a clear case for the value of capacity-building, which might well be even more critical in nations with a greater centrality and scale of internet use.

Finally, the results of this study reinforce the case that more initiatives are needed to bolster cybersecurity capacity around the world. Cybersecurity capacity-building needs to be prioritised by international and national policymakers to address the global cybersecurity gaps identified in this study. Moreover, local outcomes are not immune to global problems in cybersecurity. All nations can be jeopardised by any diminished capacity in other nations.

### **Directions for research**

These findings provide a basis for several directions for further research. First, it is important to continue refining indicators of all the dimensions of cybersecurity capacity-building. For example, the project team has been developing an approach to what we have called 'structured field coding' to support the replicability and reliability of using multiple indicators from focus groups, interviews and desk research, and multiple observers in the field to establish the maturity of each aspect of the model (Dutton et al. 2021). This effort can support innovation in comparative research but is critical also to continuing to refine our analysis of the implications of capacity-building. The reliability and integrity of our findings are fundamental to the research leading to trusted recommendations on policy and practice.

Secondly, in refining the model and moving to more structured field coding, it is possible to have more granular data at the indicator level. This will enable comparisons on any given indicator of the maturity model and thereby greatly enrich the range and quality of the comparisons that can be drawn from our studies.

Thirdly, given the value of our model (Figure 5) in estimating the expected level of maturity across dimensions, it is possible to locate nations that under- or over-perform – having less or greater maturity in capacity-building that one would expect based on the variables in our model. This enables the team to focus on factors observed in the field or in desk research that could explain unusually low or high scores relative to what would be expected given their environment, scale and centrality of internet use. These targeted examinations into particular nations could lead to new aspects of and insights into capacity-building.

## Notes

1. Only three nations did not wish their review to be publicly available, although the corresponding data is included in the studied sample respecting their anonymity throughout this article.
2. Throughout the study, the research team explored a large set of potential control variables. Some were omitted because they were unrelated to security or end-user experiences, and others were dropped when they were essentially redundant to key variables included, such as size and wealth of the nation.
3. To address the increasing demand for CMM reviews, some country reviews were done by strategic partners (the World Bank, the International Telecommunication Union, NRD Cyber Security, and the Oceania Cyber Security Centre). They follow the same methodology as the CMM reviews.
4. The conduct of modified-focus groups often led to the identification of particularly well-informed individuals who were interviewed in more depth.
5. To promote open and unhindered discussion, the Chatham House Rule was used, which led to non-attribution of some statements. <https://www.chathamhouse.org/chatham-house-rule>, accessed on 28 April 2020.
6. The number of secure servers has a different scale to CCS (in our sample, the number of secure servers goes from 5 to 580,292) and a highly skewed distribution given the country sample. To address these issues, we applied the natural logarithm of the number of secure servers.
7. A full description of the Network Readiness Indicators of usage are available at: [https://networkreadinessindex.org/wp-content/uploads/2020/11/NRI-2020-V8\\_28-11-2020.pdf](https://networkreadinessindex.org/wp-content/uploads/2020/11/NRI-2020-V8_28-11-2020.pdf)
8. This one indicator of individual usage overlaps with our indicator of the scale of internet-use. However, it is one of a large number of indicators, and tests for any collinearity issues suggested that this was not an issue.
9. Data available until 2018; we used the most recent value available for missing years.
10. Data available until 2018; we used the most recent value available for missing years. For Kosovo, we obtained the percentage of internet-users from STIKK and KANTAR (2019).
11. Data available until 2016; we used the most recent value available for missing years.

## Notes on contributors

**William H. Dutton** is Emeritus Professor, University of Southern California, an Oxford Martin Fellow, supporting the Global Cyber Security Capacity Centre at the University of Oxford, Senior Fellow at the Oxford Internet Institute (OII), and Visiting Professor, Media and Communication, University of Leeds. Bill was OII's Founding Director and first Professor of Internet Studies at Oxford before his

appointment as the James H. Quello Professor of Media and Information Policy at Michigan State University, where he directed the Quello Center.

**Sadie Creese** is Professor of Cyber Security in the Department of Computer Science at the University of Oxford. She teaches operational aspects of cybersecurity including threat detection, risk assessment and security architectures. Sadie is the founding Director of the Global Cyber Security Capacity Centre (GCSCC) at the Oxford Martin School, where she continues to serve as a Director conducting research into what constitutes national cybersecurity capacity, working with countries and international organisations around the world. She was the founding Director of Oxford's Cybersecurity network launched in 2008 and now called CyberSecurity@Oxford. She was a member of the World Economic Forum's Cyber Security Centre's Strategic Advisory Board.

**Patricia Esteve-Gonzales** is a Research Fellow at the Global Cyber Security Capacity Centre. She has a PhD in Economics from Universitat Rovira i Virgili (Spain) and her research interests are in Applied Microeconomic Theory, with a special focus on institutions, mechanism design and competitions. Her published and ongoing research uses theoretical and empirical methodologies in a variety of contexts - public procurement, affirmative action, European integration, and cyber security.

**Ruth Shillair** is an assistant professor at Michigan State University in Media and Information Studies and director of the master's program. Her research covers a range of work looking to maximise the benefits of technology while minimising harm. This includes communication strategies to improve cybersecurity practices, ways to increase digital literacy, and policies to reduce the digital divide.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## Funding

The UK Foreign, Commonwealth and Development Office and the State Government of Victoria, Australia with in-kind support from the Organization of American States and the Inter-American Development Bank.

## ORCID

S. Creese  <http://orcid.org/0000-0002-2414-9657>

W. H. Dutton  <http://orcid.org/0000-0002-0141-6804>

P. Esteve-González  <http://orcid.org/0000-0003-3740-1396>

R. Shillair  <http://orcid.org/0000-0003-0341-9096>

## References

- Almuhammadi, S., and M. Alsaleh. 2017. "Information Security Maturity Model for NIST Cyber Security Framework." Sixth International Conference on Information Technology Convergence and Services. February. doi:10.5121/csit.2017.70305
- Azmi, R., W. Tibben, and K. T. Win. 2018. "Review of Cybersecurity Frameworks: Context and Shared Concepts." *Journal of Cyber Policy*, doi:10.1080/23738871.2018.1520271.
- Baram, G., D. Paikowsky, T. Pavel, and I. Ben-Israel. 2017. "Trends in Government Cyber Security Activities in 2016." *SSRN*, January. [https://www.researchgate.net/publication/323331634\\_Trends\\_in\\_Government\\_Cyber\\_Security\\_Activities\\_in\\_2016](https://www.researchgate.net/publication/323331634_Trends_in_Government_Cyber_Security_Activities_in_2016)
- Calderaro, A., and A. J. Craig. 2020. "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building." *Third World Quarterly* 41 (6): 917–938. doi:10.1080/01436597.2020.1729729.

- Cameron, A. C., and P. K. Trivedi. 2010. *Microeconometrics Using Stata. Revised Edition*. Texas: Stata Press.
- Cohen, D. 2017. "The British Response to Threats in Cyberspace." *Cyber, Intelligence, and Security* 1 (3 December): 19–36.
- Clark, D., T. Berson, and H. S. Lin. 2014. "Computer Science and Telecommunications Board." In *At the Nexus of Cybersecurity and Public Policy*. 9 Washington, DC: The National Academy Press.
- Craney, T. A., and J. G. Surlles. 2002. "Model-dependent Variance Inflation Factor Cutoff Values." *Quality Engineering* 14 (3): 391–403.
- Creese, S., W. H. Dutton, and P. Esteve-Gonzalez. 2021. "The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions." *Personal and Ubiquitous Computing*. <https://doi.org/10.1007/s00779-021-01569-6>.
- Creese, S., W. H. Dutton, P. Esteve-Gonzalez, and R. Shillair. 2020. Cybersecurity Capacity Building: Cross-National Benefits and International Divides 22 July 2020. Paper accepted for presentation at the TPRC48, Washington DC, February 2021. Available at SSRN: <https://ssrn.com/abstract=3658350> or <http://dx.doi.org/10.2139/ssrn.3658350>.
- Dijkstra, T. K., and J. Henseler. 2015. "Consistent Partial Least Squares Path Modeling." *MIS Quarterly* 39 (2): 297–316.
- Duncan, O. D. 1966. "Path Analysis: Sociological Examples." *American Journal of Sociology* 72 (1): 1–16.
- Dutta, S., and B. Lanvin. 2020. *The Network Readiness Index 2020: Accelerating Digital Transformation in a Post-COVID Global Economy*. Portulans Institute. [https://networkreadinessindex.org/wp-content/uploads/2020/11/NRI-2020-V8\\_28-11-2020.pdf](https://networkreadinessindex.org/wp-content/uploads/2020/11/NRI-2020-V8_28-11-2020.pdf).
- Dutton, W. H., L. Axon, and C. W. Harris. 2021. *Structured Field Coding and Its Application to National Assessments*. Global Centre for Cybersecurity Capacity Building (GCSCC). January. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3781600](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3781600).
- Dutton, W. H., S. Creese, R. Shillair, and M. Bada. 2019. "Cybersecurity Capacity: Does It Matter?" *Journal of Information Policy* 9: 280–306.
- Fornell, C., and D. F. Larcker. 1981. "Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics." *Journal of Marketing Research* 18 (3): 382–388.
- GCSCC (Global Cyber Security Capacity Centre). 2016. "Cybersecurity Capacity Maturity Model for Nations (CMM). Revised Edition." <https://gcsc.ox.ac.uk/files/cmmrevisededition090220171pdf>
- GCSCC (Global Cyber Security Capacity Centre). 2019. "Global Impact. Knowledge and Policy Contributions from the First Five Years." [https://gcsc.ox.ac.uk/sites/default/files/gcsc\\_booklet\\_web.pdf](https://gcsc.ox.ac.uk/sites/default/files/gcsc_booklet_web.pdf)
- Hathaway, M. 2013. *Cyber Readiness Index 1.0*. Belfer Center for Science and International Affairs, Harvard Kennedy School. <https://www.belfercenter.org/publication/cyber-readiness-index-10>.
- Henseler, J., G. Hubona, and P. A. Ray. 2016. "Using PLS Path Modeling in New Technology Research: Updated Guidelines." *Industrial Management and Data Systems* 116 (1): 2–20. ISSN: 0263-5577.
- Hu, L. T., and P. M. Bentler. 1999. "Cutoff Criteria for fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus new Alternatives." *Structural Equation Modeling* 6 (1): 1–55. doi:10.1080/10705519909540118.
- IDB (Inter-American Development Bank, and Organization of American States). 2020. "2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean." <http://dx.doi.org/10.18235/0002513>.
- ITU (International Telecommunication Union). 2019. "Global Cybersecurity Index." Accessed 13 June 2019. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>.
- ITU-T (International Telecommunication Union Telecommunication Standardization Sector). 2008. "Series X: Data Networks, Open System Communications and Security: Telecommunication Security: Recommendation ITU-T X.1205."
- Knodel, J. 1993. "The Design and Analysis of Focus Group Studies: A Practical Approach." In Morgan, D. L. (ed.), *Successful Focus Groups: Advancing the State of the Art* (pp.35–50). Newbury Park: SAGE Publications, Inc., online <https://dx.doi.org/10.4135/9781483349008.n3>
- Krueger, R. A., and M. A. Casey. 2014. *Focus Groups: A Practical Guide for Applied Research*. India: SAGE Publications Asia-Pacific Pte. Ltd.

- Makridis, C. A., and M. Smeets. 2019. "Determinants of Cyber Readiness." *Journal of Cyber Policy* 4 (1): 72–89. doi:10.1080/23738871.2019.1604781.
- Maurer, T., and R. Morgus. 2014. *Compilation of Existing Cybersecurity and Information Security Related Definitions. Policy Paper*. DC, Washington: New America Foundation.
- Rosenzweig, P. 2019. "Preliminary Observations on the Utility of Measuring Cybersecurity." *Lawfare*. 6 August. <https://www.lawfareblog.com/preliminary-observations-utility-measuring-cybersecurity>.
- Solove, D. J., and D. K. Citron. 2017. "Risk and Anxiety: A Theory of Data-Breach Harms." *Texas Law Review* 96: 737.
- Spidalieri, F. 2015. *State of the States on Cybersecurity*. Pell Center for International Relations and Public Policy. <https://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/>.
- Ware, W. 1970. *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security*. Rand Corporation. <https://www.rand.org/pubs/reports/R609-1.html>.
- Williams, M. 2003. *Making Sense of Social Research*. London: SAGE Publications Ltd.
- World Bank. 2016. "World Development Report: Digital Dividends." Accessed 22 July 2021. <https://www.worldbank.org/en/publication/wdr2016>.
- World Bank. 2019. "World Bank Country and Lending Groups." Accessed 22 August 2019. <https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups>
- World Bank. 2020a. "World Development Indicators." Accessed 19 March 2020. <https://datacatalog.worldbank.org/dataset/world-development-indicators>
- World Bank. 2020b. "Worldwide Governance Indicators." Accessed 26 March 2020. <https://datacatalog.worldbank.org/dataset/worldwide-governance-indicators>
- World Economic Forum. 2019. "Networked Readiness Index." Accessed 13 June 2019. <http://reports.weforum.org/global-information-technology-report-2016/networked-readiness-index/>