Computers & Security

Cybersecurity Education, Awareness Raising, and Training Initiatives: National Level Evidence-Based Results, Challenges, and Promise

--Manuscript Draft--

Manuscript Number:	COSE-D-21-01697R2
Article Type:	Full Length Article
Keywords:	cybersecurity; education; training; Awareness; internet
Corresponding Author:	Ruth Shillair Michigan State University College of Communication Arts and Sciences East Lansing, MI UNITED STATES
First Author:	Ruth Shillair, Ph.D.
Order of Authors:	Ruth Shillair, Ph.D.
	Patricia Esteve-González, Ph.D.
	William H. Dutton, Ph.D.
	Sadie Creese, Ph.D.
	Eva Nagyfejeo, Ph.D.
	Basie Von Solms, Ph.D.
Abstract:	This paper assesses the impact of cybersecurity education, awareness raising, and training (CEAT) on the vitality of internet use and services at the national level. CEAT encompasses one of five dimensions of a larger cybersecurity capacity building model (CMM) that was developed by the Global Cybersecurity Capacity Centre. The paper describes this dimension of capacity building within the CMM, and its indicators of education, awareness, and training in cybersecurity capacity. The paper then presents a cross-national analysis of the outcomes of CEAT on internet use based on comparative data from 80 nations. Controlling for contextual variables, such as the wealth of the nations and scale of internet use, the analysis shows a positive and statistically significant impact of CEAT on the vitality of internet use and services, as well as a distribution of CEAT scores that indicates key issues for low-income and developing nations. A qualitative analysis of responses from these nations is used to identify key reasons for their levels of maturity in this area. While recognizing key limitations of these findings, it offers suggestions for policy and practice to meet the need for effective programs for education, awareness raising, and training. In addition, the research suggests the need for more detailed indicators of CEAT initiatives in more nations and over time to assess the validity of the findings and the recommendations for policy and practice in this area of capacity building offered in this paper.

MICHIGAN STATE
UNIVERSITY

To the Editors:

Thank you for your consideration of our manuscript *Cybersecurity Education, Awareness Raising, and Training Initiatives: National Level Evidence-Based Results, Challenges, and Promise*

In the face of ever increasing cybersecurity threats, there is a general consensus that cybersecurity education, awareness raising and training (CEAT) is important to counter these threats and build a safe and secure cyberspace. Yet, up to this point, there is limited empirical evidence to support this assumption. This manuscript makes progress towards addressing this deficit by detailing a multi-method analysis of data collected by the Oxford Martin Cyber Security Capacity Centre and the Organization of American States. This multinational effort sent research teams to interview top stakeholders in dozens of countries.

This manuscript represents the first time the data from this project has been empirically analyzed to focus on the impacts of CEAT on the use of the Internet for economic purposes. Also, we do a qualitative analysis of several dozen of the countries that our team members analyzed. We feel this research offers great value as it provides insights into efforts in developing nations as they seek to improve their cybersecurity education, awareness and training.

Sincerely,

College of Communication Arts and Sciences

Department of Media and Information

404 Wilson Road, Room 409
Michigan State University
East Lansing, MI 48824
USA

Phone: +1.517.355.8372
Fax: +1.517.355.1292
Web: mi.msu.edu

Dr. Ruth Shillair, Ph.D
Assistant Professor, Media & Information Studies
Director of Media & Information, Master's Program
Health and Risk Communication Center, Faculty Affiliate
Research Fellow, Quello Center
Michigan State University

Research Consultant
Global Cybersecurity Capacity Centre
Oxford Martin School, Department of Computer Science
University of Oxford
United Kingdom

Reviewer Comments with the Authors' Responses

Thank you so much to all the reviewers, your insights and guidance have greatly improved the manuscript.

Reviewer #1: Read it the first time and liked it. Now I like it more. The clarifications make this understandable to the casual reader and the points are well made an important - accept

Thank you for your review. We have sought to continue revisions that further clarify the study's findings.

Reviewer #4: This paper is very interesting and provides important insight into the role of cybersecurity education, awareness and training initiatives at a national level. However, it includes a lot of different analyses and because of this it is difficult to follow in places. I have tried to identify a few places where more explanation would help improve its accessibility.

We have made further minor revisions throughout the manuscript to make it easier to follow and better explain the study without making any substantive changes.

The term 'formative levels' is first mentioned on the 3rd page of the Introduction section with no explanation of what a formative level might be. Similarly, the next line refers to 'these three factors', but doesn't name them. More consistent use of terms and explanation is needed early in the paper to link this text to Table 1 - note they are referred to as 'concepts' in the paragraph before, and these concepts might or might not be the factors referred to in the next paragraph.

In page three of the introduction, we have clarified the measures and how they are operationalized. We also introduce the measurement levels. We cleaned up this section to make it more accessible to the casual reader. We also went through the paper to make sure terminology was consistent for construct measures and operationalization.

The derivation of the model in Figure 4 should be explained. Is there previous literature to support any of the hypotheses?

Yes, we have included previous literature as well as included more explanation of the logic for the model, how it has evolved, and the unique constructs and focus for this research.

An outline of the methodology used for the qualitative analysis should be provided - e.g. what data was used and how was it analyzed to identify the themes that are reported?

We included more specific terminology to describe the methodology of the qualitative research.

Focus groups are mentioned twice in the results but no explanation of them is provided.

We have added a brief explanation about what the focus groups were conducted for our country reports and our quantitative data, which is a basis for this paper. We are happy to feature these more prominently, given the value of ten focus groups per country and each group having about a dozen participants. We include citations that point to articles that provide even more detail.

The following issues should also be addressed:

1. Check use of the acronym CEAT as it is defined multiple times in the paper - doing it just once when it is first used (in the Introduction) would be standard practice.

We have revised the manuscript to define the acronym CEAT in the Introduction and from there forward only use the acronym. We have amended this acronym in Figure 3 as well, and homogenized the reference to the CMM dimension on CEAT on all tables and figures.

2. Introduction line 24 should say 'will amount to' not 'amounts to …' as it is not yet 2025.

Done.

3. The last sentence in Section 2 says 'Does CEAT matter' - it seems to be there by mistake.

We deleted this question.

4. In paragraph before Table 2, 'being 2015 the first ones' should say 'the first ones being 2015' or similar.

We have amended the sentence to read: "This study considers a sample of 80 nations, most of them reviewed since 2019, although some nations were reviewed earlier, beginning from 2015."

Biographical Sketch of Authors

Ruth Shillair is an assistant professor at Michigan State University in Media and Information Studies and director of the master's program. She is a research fellow at the Quello Center at Michigan State University, a faculty affiliate for the Health and Risk Communication Center also at Michigan State University. She is a research consultant for the Oxford Cybersecurity Capacity Centre. Her research includes communication strategies to improve cybersecurity practices, ways to increase digital literacy, and policies to reduce the digital divide.

Patricia Esteve-González is a Senior Research Associate at the Global Cyber Security Capacity Centre, University of Oxford. She has a PhD in Economics and her research interests focus on the role of institutions and the mechanism design of their policies. Her published and ongoing research uses theoretical and empirical methodologies in a variety of contexts, including cybersecurity capacity.

William H. Dutton is an Emeritus Professor at the University of Southern California. Bill was the founding Director of the Oxford Internet Institute (OII) and first Professor of Internet Studies at the University of Oxford, where Bill is now an OII Fellow and Martin Fellow with Oxford's Global Cybersecurity Capacity 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.

Eva Nagyfejeo is a Research Fellow at the Global Cyber Security Capacity Centre, University of Oxford, supporting the delivery of global cybersecurity capacity-building expertise by promoting the Centre's CMM through country reviews. She obtained her PhD in Politics and International Studies from the University of Warwick (UK) and her thesis examined EU-US cooperation in cybersecurity focusing on the fight against cybercrime. Prior to joining the GCSCC, she worked at the EUISS, NATO, Europol/European Cybercrime Centre (EC3), the European Parliament and at the Center for Security Studies at ETH Zürich.

Prof SH (Basie) von Solms is a retired Research Professor in the Academy for Computer Science and Software Engineering at the University of Johannesburg in Johannesburg, South Africa. He is the Director of the Centre for Cyber Security at the University of Johannesburg as well as an Associate Director of the Global Cybersecurity Capacity Centre of the University of Oxford in the UK.

National Level Evidence-Based Results, Challenges, and Promise

Ruth Shillair[a], Patricia Esteve-González[b], William H. Dutton[c], Sadie Creese,[d] Eva Nagyfejeo,[e] and Basie Von Solms[f]

[a] Quello Center, Michigan State University, East Lansing, United States. ORCiD: 0000-0003-0341-9096; email address: shillai7@msu.edu.

[b] Global Cyber Security Capacity Centre, Department of Computer Science, University of Oxford, Oxford, United Kingdom. ORCiD: 0000-0003-3740-1396.

[c] Global Cyber Security Capacity Centre, Department of Computer Science, University of Oxford, Oxford, United Kingdom. ORCiD: 0000-0002-0141-6804.

[d] Global Cyber Security Capacity Centre, Department of Computer Science, University of Oxford, Oxford, United Kingdom. ORCiD: 0000-0002-2414-9657

[e] Global Cyber Security Capacity Centre, Department of Computer Science, University of Oxford, Oxford, United Kingdom. ORCiD: 0000-0002-1767-2642

[f] Director of the University of Johannesburg (UJ) Centre for Cyber Security, Johannesburg, South Africa. ORCiD: 0000-0003-3586-6632

Abstract

This paper assesses the impact of cybersecurity education, awareness raising, and training (CEAT) on the vitality of internet use and services at the national level. CEAT encompasses one of five dimensions of a larger cybersecurity capacity building model (CMM) that was developed by the Global Cybersecurity Capacity Centre. The paper describes this dimension of capacity building within the CMM, and its indicators of education, awareness, and training in cybersecurity capacity. The paper then presents a cross-national analysis of the outcomes of CEAT on internet use based on comparative data from 80 nations. Controlling for contextual variables, such as the wealth of the nations and scale of internet use, the analysis shows a positive and statistically significant impact of CEAT on the vitality of internet use and services, as well as a distribution of CEAT scores that indicates key issues for low-income and developing nations. A qualitative analysis of responses from these nations is used to identify key reasons for their levels of maturity in this area. While recognising key limitations of these findings, it offers suggestions for policy and practice to meet the need for effective programs for education, awareness raising, and training. In addition, the research suggests the need for more detailed indicators of CEAT initiatives in more nations and over time to assess the validity of the findings and the recommendations for policy and practice in this area of capacity building offered in this paper.

Keywords: cybersecurity, education, training, awareness, internet

Funding for this research provided by: 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.

1. Introduction

Access to the internet is continuing to expand, along with its use for a wider variety of purposes. There are estimates that close to 4.7 billion people are active users of the internet – close to 60% of the world's population (Johnson, 2021). However, many users have limited knowledge or awareness of the risks of being online, and have never been involved in educational or training programs on cybersecurity (Aiken, 2019). A relative lack of education, awareness, and training could be contributing to increased problems with cybersecurity, vulnerability to rising levels of cybercrime and poor password practices. By one estimate, the global costs of cybercrime (including the damage and destruction of data) amount to over US$10.5 trillion per year by 2025 (Morgan, 2020). Thus, initiatives to improve cybersecurity education, awareness and remediation of threats, and training to mitigate these harms are of importance at the national level.

The potential value of these initiatives might be taken for granted, given that safe, reliable, and accessible information and communication technologies (ICTs) are at the heart of local and global economic growth. This growth is not without risks, as individuals, households, businesses, industries, and critical infrastructures are increasingly connecting people and things online, as with the Internet of Things (IoT), these new connections can turn into new security vulnerabilities. Security problems vary from compromised passwords to ransomware attacks or stolen databases. These risks raise questions about approaches to enhancing security, with one major response being the need for building the cybersecurity capacity of nations, which includes advances in cybersecurity education, awareness raising, and training at multiple levels, from nations to organizations to households and individuals.

With the global diffusion of the internet, social media, and mobile smartphones, increasing responsibilities end up with the individual user. Many individuals online are sufficiently informed to protect themselves and help protect others (Shillair et al., 2015), but

many others do not know how these attacks occur or how to protect themselves. For example, a survey of US households found that three-quarters (75%) of respondents could recognise a strong password, but less than a quarter (13%) knew what a virtual private network (VPN) does and even fewer (10%) could recognise an example of multi-factor authentication (Olmstead & Smith, 2017). Given such low awareness of basic security precautions, it is likely that improving educational offerings, raising awareness, and providing opportunities for training in cybersecurity are needed around the world. For such reasons, there have been several long-term national efforts, including initiatives of the Computer Science and Telecommunications Board (CSTB) in the US, and the National Cyber Security Centre in the UK to model the potential of what can be done at the national scale (Clark et al., 2014; Coventry et al., 2014).

Nevertheless, cybersecurity policy largely assumes, but has not yet developed, systematic empirical evidence on such basic questions as: what are the impacts of policies at the national level for cybersecurity education, awareness, and training programs? Do these policies help improve internet use and commerce? Alternatively, would a deeper awareness of online threats have a chilling effect, even causing a decline in use of the internet for commerce, communications, and governmental functions?

The present research provides empirical support that national level efforts to improve cybersecurity education, awareness raising, and training (CEAT) have made a positive difference. We use evidence of CEAT initiatives in 80 nations that were analysed using the Cybersecurity Capacity Maturity Model for Nations (CMM)[1], a framework to estimate the maturity stage of different national cybersecurity capacities (GCSCC, 2021). The CMM is

[1] The concept of a maturity framework follows the seminal work of Humphrey (1988) on software maturity, on which many maturity models have subsequently been based.

based on five dimensions of cybersecurity capacity: cybersecurity policy and strategy; cybersecurity culture and society; building cybersecurity knowledge and capabilities; legal and regulatory frameworks; and standards and technologies. The CMM was developed with over 200 experts from technological, academic, and policy sectors.[2] Over multiple iterations and data collections by international teams, these assessments probed into key aspects of cybersecurity capacity at the national level.

Each dimension is evaluated using a mix of factors that were determined the by CMM contributors to be essential to that dimension. Factors are further segmented by measurable aspects that allow close examination of factors for actionable response. Aspects are further operationalized by observable indicators. These indicators are used to gauge the maturity stages across all five dimensions of capacity building and the factors that comprise each dimension. Stages of maturity range across five levels, from start-up to formative, established, strategic, and a dynamic stage. More details about the CMM and measures are in the data and analysis section. The CMM allows researchers to take a broad and rather abstract concept and break it into more concrete measurable indicators. The CMM review process produces content-rich qualitative evaluations and transforms it into quantitative measures that allow analysis and evaluation of cybersecurity capacity building efforts.

Based on the CMM dimension focused on building cybersecurity knowledge and capabilities, CEAT is evidenced by several factors. The first is focused on the provision and administration of educational programs on cybersecurity. Secondly, awareness raising, which includes programmes aimed at the internet user community at large but also initiatives in executive awareness raising. Thirdly, training is indicated by the provision and uptake of

[2] The development and evolution of the CMM are at https://gcscc.ox.ac.uk/development-and-evolution-of-the-cmm

training programs. More details and the operationalization of these concepts are described in Table 1 and in the data and analysis section of this article.

However, as this analysis will demonstrate, levels and approaches to cybersecurity education, awareness raising, and training are too often only at the initial maturity levels of start-up or formative, given a preponderance of low-income nations. In our analysis, factors of cybersecurity education, awareness raising, and training are combined for an overall indication of the maturity of CEAT in each nation. Empirical analysis demonstrates that CEAT makes a positive difference, but this impact might be limited in that many nations have low maturity levels on CEAT. To better understand this problem, we also conducted a qualitative analysis of the full CMM reports of 23 selected nations, as described in a later section. This yielded descriptions of what each of these nations were and were not doing for CEAT, enabling us to more concretely show the ways in which cybersecurity education, awareness, and training were being deployed.

Table 1. Brief description of the indicators in those aspects in the CMM dimension on CEAT.

Factor	*Aspect*	Summary of *indicators*
Education	Provision of education	Availability of cybersecurity education offerings and educator qualification programmes.
	Administration of education	Coordination and resources for developing cybersecurity education frameworks based on national demand.
Awareness	Awareness raising programmes	Existence of a national programme for cybersecurity awareness raising; range of demographics and issues covered; engagement of different stakeholders.
	Executive awareness raising	Efforts to raise the executive's awareness of cybersecurity issues in different sectors.
Training	Provision of training	Availability of cybersecurity professional training programmes for enhancing skills and capabilities.
	Uptake of training	Certified employees trained in cybersecurity through cybersecurity training programmes and knowledge transfer.

2. Theoretical framework and related literature

Most pundits and practitioners would expect a high level of consensus on the need for programs to educate internet users and service providers on issues tied to cybersecurity, raise everyone's awareness of the risks, and to provide training in how to enhance the capacity of individual internet users and organisations to protect themselves from cyber-attacks. In line with this, aspects of CEAT are part of nearly every credible cybersecurity capacity building model being supported by nations and NGOs, such as the World Bank (Azmi et al., 2018). However, there is a serious level of uncertainty over the value of investing in cybersecurity education, awareness raising, and training – which we have summarized as CEAT investments. Often this results in under-investment, particularly in low-income countries (Nagyfejeo & Solms, 2020). However, this could be the case more generally, and could help explain the shortage of cybersecurity skills worldwide. In addition, approaches to mitigating such deficiencies are not easy to study because governments do not use metrics or any consistent systems to evaluate the impact of such policies (De Zan, 2019; De Zan & Di Franco, 2019).

Experts in cybersecurity capacity building are divided over the efficacy of putting substantial resources into CEAT. For example, cybersecurity involves legal, technical, and societal protections that require broader and deeper educational initiatives than can be easily packaged and offered to a wide range of individuals. Moreover, awareness raising has had a history of challenges in discovering how to raise awareness across a broad public without instilling fear and undermining use. In addition, awareness raising often fails to guide people on what to do in situations involving specific software and problems. Finally, the most effective training programs are those that can reach all users, not just the technologically savvy. They also need to entail a significant range of material and interaction with trainers

and learning materials, such as practice with confronting and identifying phishing emails or problematic attachments.

Given these challenges, top cybersecurity executives and policy communities might aspire to delivering effective education, awareness raising, and training, but also be unable to resource these activities at the levels required for them to be truly effective. In addition, there is a more basic confrontation between experts arguing that solutions should focus on technology, since people are the problem, and those who posit that we need to see people as the key to solutions.

The people are the problem position, maintains the need to place more resources into technical advances that obviate the need for human awareness at the level of internet users. Advances in spam filters and antivirus protection software illustrate the potential for such an approach. In contrast, if users are less exposed to attacks because of software detection improvement, they will be less prepared to recognise them (Mc Mahon, 2020). The people are the solution position maintains that every technical fix is a partial solution, requiring humans to identify and respond to problems, and that most, if not all, 'technical fixes' create new problems, such as shifting attacks to new targets (Kassner, 2020). In this sense, Von Solms (2021) supports the idea that investing in the level of cybersecurity awareness and knowledge of workers can reduce the probability of a cyberattack, supporting the assumption that educational, awareness, and training courses can be effective as tools to prevent and fight cybercrime.

3. Data and Analysis

The present study sought to establish whether those countries that have more mature levels of capacity building in CEAT will see demonstrable gains accruing to users, such as in the vitality of internet-enabled governmental and business services and growing commercial use of the internet. We examine this by analysing cross-national data from up to 80 countries that

have been reviewed through the lens of the Cybersecurity Capacity Maturity Model for Nations (CMM) of the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford. Using the indicators from the CEAT factor, we compare nations at different levels of maturity, controlling for their context, such as national wealth, which enables us to determine what impact – if any – is achieved through greater maturity in CEAT.

3.1. Indicators of cybersecurity

The CMM (GCSCC, 2021) is a theoretical framework that help nations to estimate their level of maturity in five *dimensions* of cybersecurity: cybersecurity policy and strategy; cybersecurity culture and society; building cybersecurity knowledge and capabilities; legal and regulatory frameworks; and standards and technologies. Each dimension contains different *aspects* that are grouped by topic or *factor*. Aspects are the units of study whose maturity is benchmarked in the CMM. The model considers five maturity stages that define different actions in capacity building for each aspect. To move from one maturity stage to another, there is an evaluation of indicators (specific operationalizations) of aspects which build together to form the factors. The *start-up* maturity stage indicates no observable evidence of cybersecurity capacity in that aspect; the *formative* maturity stage shows evidence of ad hoc activity; the *established* maturity stage has evidence of indicators in place with little decision-making on their choices; the *strategic* maturity stage shows evidenced mechanisms with choices according to the needs of the nation or organisations; and the *dynamic* maturity stage indicates that such mechanisms can be altered depending on the changing environment with rapid decision-making.

Since the CMM launch in 2014, the GCSCC and its implementation partners have used this model to review the cybersecurity capacity in more than 80 nations.[3] This study

[3] The implementation partners of the GCSCC that have conducted CMM reviews are the World Bank, Organization of American States, Oceania Cyber Security Centre, NRD Cyber Security, the International

considers a sample of 80 nations, most of them reviewed since 2019, although some nations were reviewed earlier, beginning from 2015. Table 2 summarises some key characteristics of the nations studied in this paper. The sample has representative nations from all the regions in the world and different income groups as defined by the World Bank (2021c). However, some regions are particularly overrepresented (for example, Latin America and the Caribbean) while others are underrepresented (for example, Middle East and North Africa). Similarly, high-income countries are underrepresented compared to the other income groups. The reason behind this is that the countries in the sample are not selected randomly. A government organisation in a nation interested to implement the CMM contacts the GCSCC to start the review process, not vice versa. Moreover, for all the sample countries in the Latin America and the Caribbean region, we considered the data in IDB & OAS (2020) as secondary data.

Table 2. Descriptive information on the nations in the sample.

Year of CMM[4]	N	Region (WB, 2021c)	N	Income (WB, 2021c)	N
2015:	6	East and Pacific:	10	High:	14
2016:	4	Europe and Central Asia:	14	Upper middle:	31
2017:	5	Latin America and the Car.:	32	Lower middle:	26
2018:	10	Middle East and North Afr.:	1	Low:	9
2019:	18	South Asia:	3		
2020:	37	Sub-Saharan Africa:	20		
Total:	*80*	*Total:*	*80*	*Total:*	*80*

The process of a CMM review involves field data-gathering from consultations with national stakeholders and desk research, collecting direct information on cybersecurity capacity in the nation, and being a national CMM report the evidence-based outcome of such review. A national CMM report contains qualitative information on the cybersecurity

Telecommunication Union, the Commonwealth Telecommunications Organisation, and Cybersecurity Capacity Centre for Southern Africa.

[4] This information is available at the website of the Global Cyber Security Capacity Centre. https://gcscc.ox.ac.uk/, accessed on 4 November, 2020.

capacities of the nation in the CMM framework, expanding on the cybersecurity indicators found when the CMM review was done. While the researchers write the CMM report, they synthesise this qualitative information into the maturity stage of each aspect. Once the report is finished, the maturity stages of all aspects are joined to the dataset, allowing to consider each aspect in the CMM as an ordinal variable that can take a value between 1 (start-up maturity stage) and 5 (dynamic maturity stage). For more detailed information about the data collection and the CMM review processes, see Creese et al. (2021a, 2021b).

This paper focuses on the CMM dimension related to building cybersecurity education, awareness, and training. This dimension was particularly modified from the first edition of the CMM in 2014 to the second edition in 2016 (GCSCC , 2016) to incorporate lessons learnt from the deployment of the model. With the aim of incorporating all the nations feasible in the analysis, the data of the seven countries reviewed under the 2014 CMM edition was converted to the 2016 edition;[5] the remaining 73 countries were reviewed under the 2016 CMM edition. As shown previously in Table 1, the 2016 CMM edition considers that the CEAT dimension contains three factors, and each factor contains two aspects. The aspects are formed from multiple indicators, that are specific operationalizations of the aspect as determined by the teams of experts developing the scales. More details about cybersecurity indicators that define the maturity stages of each aspect can be found in GCSCC (2016, p. 32-38).

Table 3 contains some descriptive statistics of the six aspects or variables in the CEAT dimension. Taking all the countries together, the average maturity stage did not achieve the formative maturity stage (corresponding to a value of 2) because there were many

[5] The newest edition of the CMM (GCSCC, 2021) has been used to review two nations. However, at the moment this paper is written, these national CMM reports were in a preliminary phase and this data could not be included in this study.

countries in the sample with a start-up maturity stage (corresponding to a value of 1) when they were reviewed. For example, the awareness raising of executives was the most mature aspect on average, but with only an average value of 1.90. The least mature aspect on average for our sample of countries corresponded to the administration of education, with an average maturity stage of 1.52. However, some nations achieved maturity stages above the established level (corresponding to a value of 3) on all the aspects of this dimension, illustrating the variability within the sample.

The relationships among the aspects within the CEAT dimension were positive and strong, indicating that these six variables were likely to be positively and linearly related.[6] While all the relations between aspects were positive, some were stronger, such as between the provision and uptake of training, than others, such as between the executive awareness raising and administration of education.

Table 3. Descriptive statistics on aspects in the CMM related to CEAT.

Variable	Obs.	Mean	S. D.	Min	Max
CEAT	80	1.79	0.55	1.00	3.33
Education	80	1.67	0.61	1.00	3.80
Provision of education	80	1.82	0.76	1.00	3.80
Administration of education	80	1.52	0.61	1.00	3.80
Awareness	80	1.84	0.61	1.00	3.50
Awareness Raising Programmes	80	1.77	0.74	1.00	4.00
Executive Awareness Raising	80	1.90	0.67	1.00	3.00
Training	80	1.85	0.64	1.00	4.00
Provision of training	80	1.87	0.71	1.00	4.00
Uptake of training	80	1.84	0.65	1.00	4.00

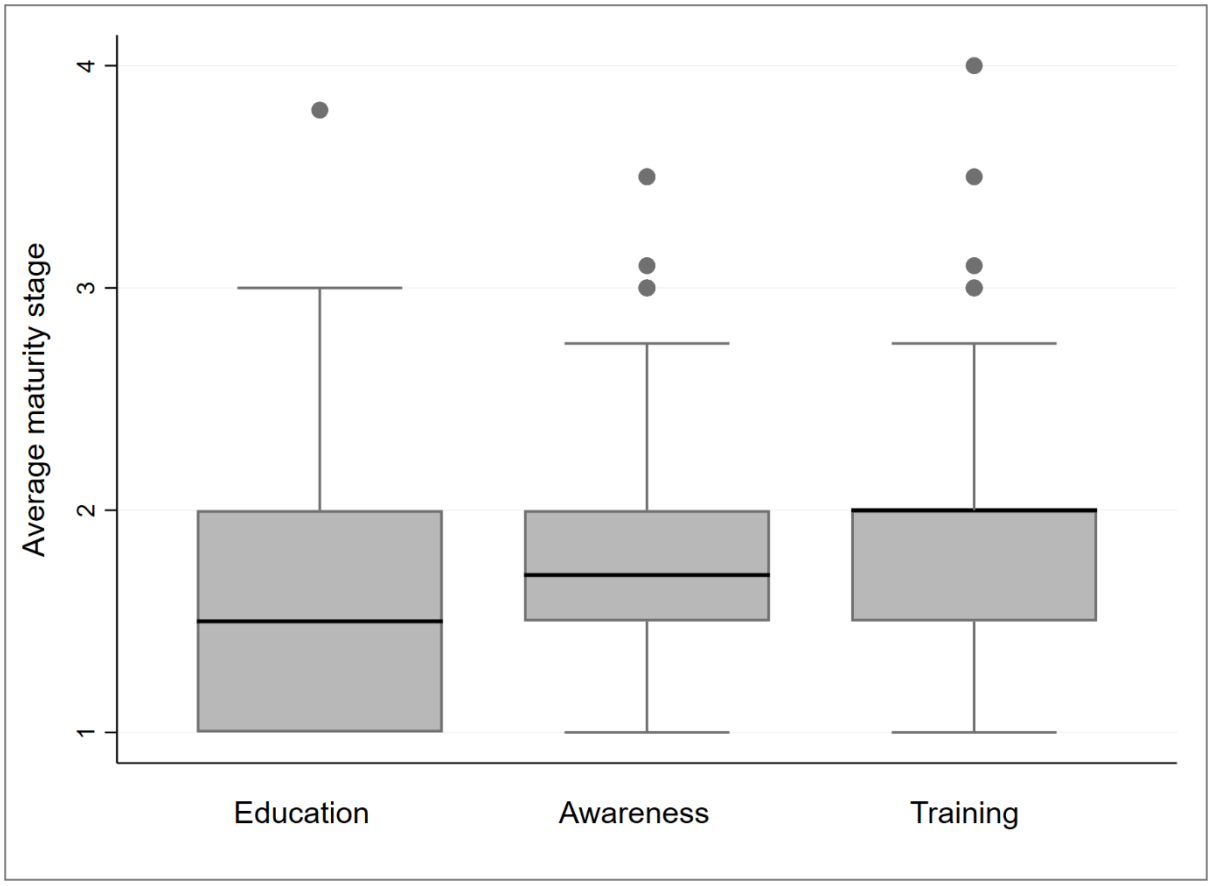
The factors calculated as the average maturity stage of their corresponding *aspects* are coloured in grey.

After calculating the average maturity stage at the factor level, taking the average maturity stage of the two aspects within each factor, we obtained a value that was not categorical and had more variance than the single variables. The correlation between the three

[6] The corresponding correlation matrices are available upon request.

factors was positive, with correlation coefficients more uniform and closer to one. Table 3 displays the descriptive statistics of the average maturity stage for the three factors in grey. In average, the countries in the sample showed a lower maturity in the education framework than in the other two factors (awareness and training). Figure 1 displays the box plot with the distributions of the three factors. Education was the factor with the highest proportion of countries with low maturity, with the median observation having an average maturity stage of 1.50. However, the median observation of the Training factor had a formative maturity stage (value 2), indicating that, in general, the framework for cybersecurity education was slightly behind the capacity offered by the professional training framework. The Awareness factor had a similar distribution to Training but with a lower median (value 1.71).

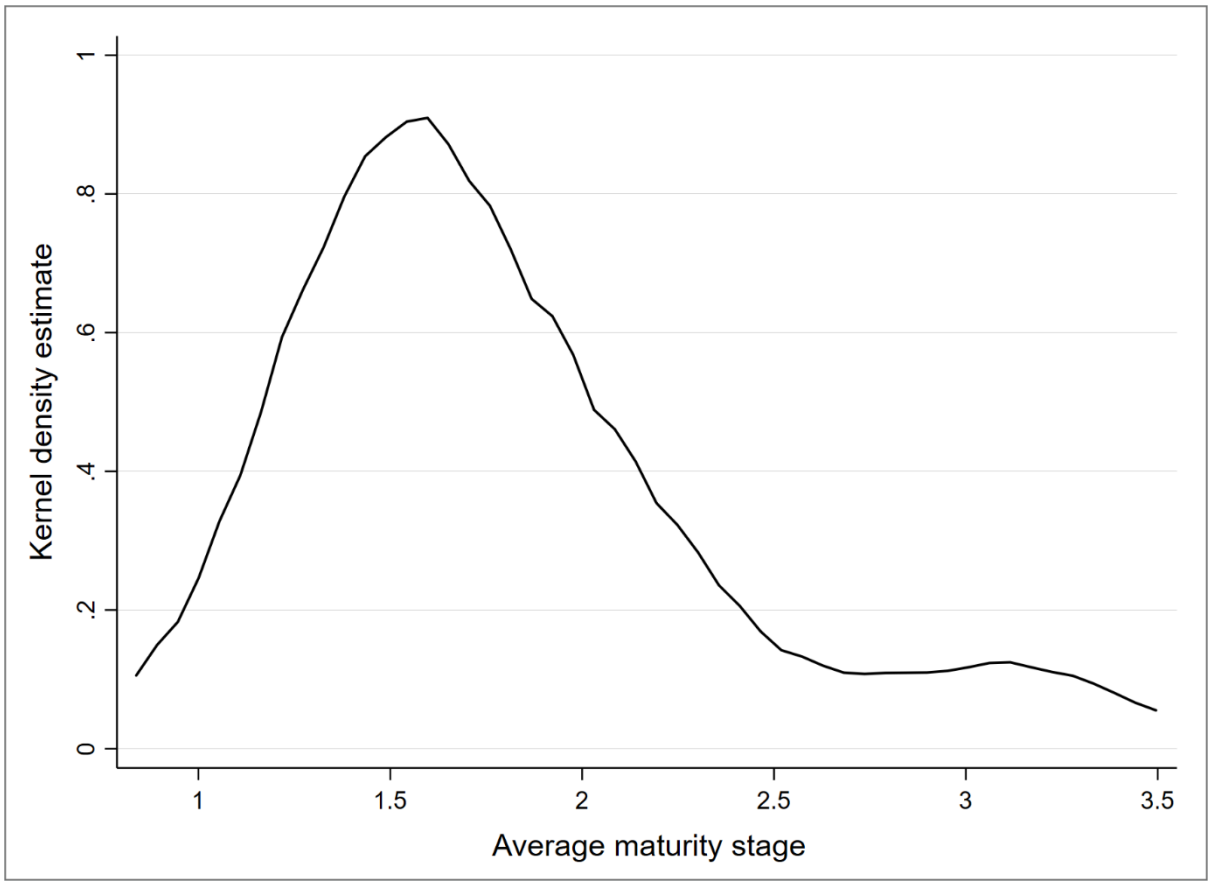
Figure 1. Box plot with the distribution of the three factors in the CMM dimension on CEAT.



The median position is signalled with a black thick line and the values inside the box correspond to the values in the interquartile range (percentiles 25th to 75th).

In order to have a single variable capturing the maturity of the sample countries in the CEAT dimension, we used the average of the three factors. Table 3 displays the descriptive statistics of this variable and Figure 2 shows its distribution. The mean and median values of CEAT, 1.79 and 1.67 respectively, indicate that most of the countries in the sample had around the start-up and formative maturity stages. Concretely, only 24 nations out of 80 had an average maturity stage equal or above formative, accounting for the 30 percent of the sample. Similarly, only 5 nations out of 80 had an average maturity stage equal or above established (6.25% of the sample).

Figure 2. Distribution of maturity levels for CEAT.

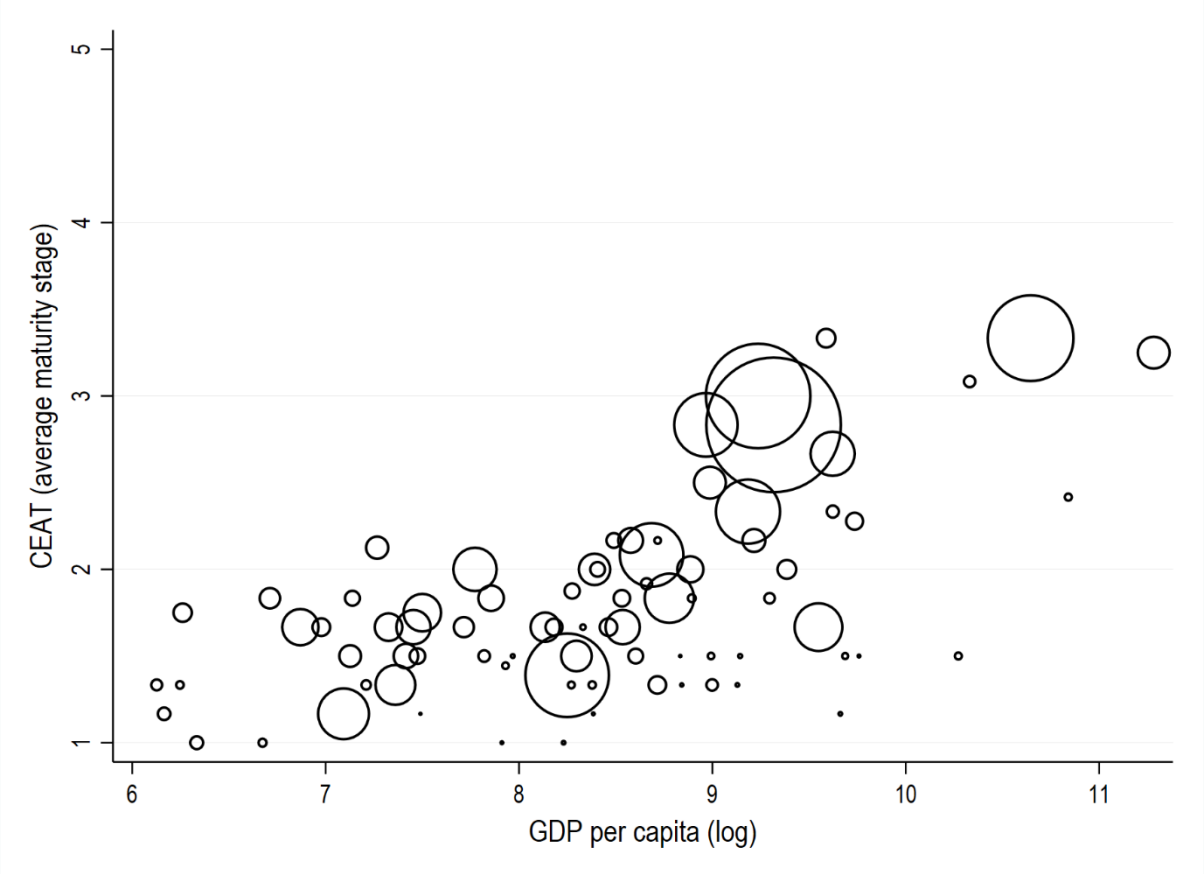


3.2. Secondary data

The literature has shown that the wealth of countries has a relevant role in determining the cybersecurity capacity of nations, jointly with the scale and centrality of internet (Creese et al., 2021a, Creese et al., 2021b, Dutton et al., 2019). We included these determinants to explain the level of maturity in the CEAT *dimension*. As explained in Table 4, we measured national *wealth* as the GDP per capita, *centrality* as the percentage of internet users, and *scale* as the number of internet users in the nation. We considered the *size* of the country as an indirect determinant of CEAT, measuring it by the nation's total population. Given that GDP per capita, number of internet users, and total population have a different scale to CEAT and a highly skewed distribution given our country sample, we applied the natural logarithm of the value for these three variables.

Figure 3 shows a positive relationship between CEAT and GDP per capita for the countries in the sample, while we cannot see a clear pattern for internet scale. The countries in the sample with a higher GDP per capita were more likely to be more mature in CEAT, but it is noticeable that many of the wealthier countries were not investing in CEAT, showing maturity levels below formative. Some countries with lower levels of GDP per capita are at a formative stage or above in CEAT. However, these last observations are exceptional, making it evident there is a need to invest economic resources in building CEAT. Given that the centrality of internet use is highly correlated to wealth (with a Pearson's correlation coefficient of 0.87), this scatterplot looks very similar when we replace GDP per capita with percentage of internet users.

Figure 3. Scatter plot with the average maturity stage of the CEAT dimension of the CMM and GDP per capita (log). The bubbles are weighted by the number of users in each country.



As explained in Section 2, the level of maturity in CEAT may have an impact on the vitality use of the internet and social media. We expect that countries with more maturity of CEAT have more digitalised societies, with digital technologies incorporated into daily business and social activities. We looked at seven outcome variables related to the digitalisation of countries. The variable *access account* captures how many users in a country access financial accounts through their mobile phone or the internet. The variables *firms with web* and *business use of digital tools* capture how businesses use digital tools for their internal and external activities. The variable *gig economy* considers the prevalence of jobs related to online platforms in a country, usually freelance jobs or flexible jobs that strictly depend on the demand of the online platforms. The variables *e-government* and *e-participation* are more related to the online services provided by governments and their quality. The last outcome variable we consider is the number of *secure servers* that countries

have, as countries more mature in CEAT would use and request more secure connections to the internet.[7] Table 4 shows the sources of these variables and the descriptive statistics for the countries in our sample.

Table 4. Descriptive statistics and sources of the secondary variables.

Variable	Description and source	N	Mean (S. D.)	Min	Max
Centrality	Individuals using the internet as a percentage of population (World Bank, 2021d)	80	48.96 (25.31)	4.71	98.25
Scale	Natural logarithm of the number of users calculated with the total population of each country and Centrality, both variables from World Bank (2021d)	80	18.95 (2.05)	14.35	23.42
Wealth	Natural logarithm of the Gross Domestic Product (GDP) per capita in constant 2010 US$ (World Bank, 2021d)	80	8.39 (1.11)	6.12	11.28
Size	Natural logarithm of total population (World Bank, 2021d)	80	15.25 (2.12)	10.87	19.37
Firms with web	Percentage of firms having their own website (World Bank, 2021a)	78	44.16 (21.76)	1.80	91.74
Access account	Percentage of respondents who used a mobile phone or the internet to access a financial institution account in the past year (World Bank, 2021b)	55	11.44 (11.54)	0.66	56.04
Secure servers	Natural logarithm of the number of secure internet servers (World Bank, 2021d)	79	6.94 (2.77)	0.00	13.62
E-Government	E-Government Development Index (from 0 to 1) including the provision of online services, telecommunication connectivity, and human capacity; index multiplied by 100 (UN DESA, 2021)	79	54.36 (17.14)	13.78	89.44
E-Participation	E-Participation Index (from 0 to 1) including the use of online services to facilitate information by governments to citizens, interaction with stakeholders, and engagement in decision-making processes; index multiplied by 100 (UN DESA, 2021)	79	52.39 (21.50)	11.86	98.04

[7] We considered the natural logarithm of the number of secure servers in each country to mitigate the problems related to its skewed distribution and the different scale compared to the rest of variables in the model.

Gig economy	Normalised score (between 0 and 100) included as an indicator of the Inclusion sub-pillar (Network Readiness Index, 2020)	52	36.21 (17.64)	3.78	93.80
Business use of digital tools	Normalised score (between 0 and 100) included as an indicator of the Businesses sub-pillar (Network Readiness Index, 2020)	52	53.07 (17.45)	13.89	88.91
Internet use	Composite variable made up of seven secondary variables.	47	0.00 (0.96)	-1.78	2.47

As showed in Table 5, the seven outcome variables were all positively correlated, with e-government and e-participation having the strongest correlation with a Pearson's coefficient above 0.8, and gig economy and firms with web the weakest correlation coefficient close to zero. A factor analysis confirmed that the seven outcome variables could be combined in a composite variable, which we simply called *internet use*.[8] Notice that our sample of 80 countries was highly affected by the availability of secondary data, reducing the number of observations to 47.

4. Methodology and analysis

This study used both linear regressions and path analysis to test the determinants of CEAT and its impact the internet use.[9] The results of these two quantitative approaches were aligned, finding that investing in CEAT had a positive and significant impact on the vitality of the internet use, although this result was mainly driven by the impact of CEAT on e-governance, an outcome variable measuring the promotion of citizen participation into national governance.

[8] This factor analysis is available under request.

[9] In particular, we used ordinal least square regressions with heteroscedasticity-robust standard errors.

Table 5. Pearson´s correlation matrix.

	CEAT	Wealth	Scale	Central.	Firms	Access	Secure	E-Gov.	E-Part.	Gig E.	Business
EAT	1.00***										
Wealth	0.57***	1.00									
Scale	0.52***	0.01	1.00								
Centrality	0.58***	0.87***	0.10	1.00							
Firms with web	0.57***	0.55***	0.31**	0.61***	1.00						
Access account	0.57***	0.68***	0.07	0.49***	0.46***	1.00					
Secure servers	0.68***	0.54***	0.68***	0.56***	0.59***	0.49***	1.00				
E-Government	0.68***	0.85***	0.25*	0.88***	0.63***	0.48***	0.69***	1.00			
E-Participation	0.71***	0.53***	0.48***	0.62***	0.59***	0.32*	0.66***	0.83***	1.00		
Gig economy	0.31*	0.33*	0.13	0.22	0.07	0.48***	0.26+	0.23+	0.13	1.00	
Business usage	0.61***	0.65***	0.34*	0.51***	0.46***	0.54***	0.63***	0.58***	0.44***	0.65***	1.00

+ $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

4.1. Regressions

Table 6 displays the regression results of testing our first hypotheses that wealth, scale, and centrality are determinants of the maturity of countries in CEAT. When we have the three variables in the model, only wealth and scale have a significant positive impact on CEAT. A 1 percent increment of the number of users is estimated to have an impact on the average maturity stage of CEAT by 0.14 units, and a 1 percent increment of the GDP per capita would increase CEAT by 0.22 units. Centrality does not have a significant impact on CEAT; this is partially explained by the strong correlation between variables centrality and wealth (see Table 5).[10]

Table 6. Regression to explain CEAT capacity.

	CEAT	CEAT	CEAT
Centrality	0.01***	0.01***	0.00
	(0.00)	(0.00)	(0.00)
Scale		0.13***	0.14***
		(0.02)	(0.02)
Wealth			0.22**
			(0.08)
Constant	1.17***	-1.16**	-2.81***
	(0.09)	(0.39)	(0.73)
N	80	80	80
R-sq	0.33	0.55	0.60

Robust standard errors in parenthesis below the corresponding coefficient.
*p< 0.05, **p< 0.01, ***p< 0.001

Table 7 displays the results of testing the second hypothesis that CEAT has a positive impact on internet use. The results show that CEAT does have a significant and positive impact on internet use even when we use control variables that are the same variables that determine CEAT (centrality, scale, and wealth). However, a close analysis shows that the

[10] This result was already found in Creese et al. (2021b).

relation between CEAT and internet use is relatively weak and mainly explained by the outcome variable e-participation.

Table 7. Regressions to explain internet use.

	Internet use	Internet use	Internet use	Internet use	Internet use
CEAT	1.31***	0.74***	0.53***	0.43*	0.38*
	(0.17)	(0.15)	(0.20)	(0.19)	(0.17)
Centrality		0.02***	0.02***		0.01**
		(0.00)	(0.00)		(0.00)
Scale			0.18***	0.16**	0.18***
			(0.05)	(0.05)	(0.05)
Wealth				0.57***	0.37**
				(0.10)	(0.13)
Constant	-2.65***	-2.59***	-6.00***	-8.98***	-8.09***
	(0.34)	(0.31)	(0.97)	(1.16)	(1.17)
N	47	47	47	47	47
R-sq	0.57	0.74	0.80	0.82	0.84

Robust standard errors in parenthesis below the corresponding coefficient.
+ p < 0.10, *p < 0.05, **p< 0.01, p< 0.001.

Table 8 displays the estimation of the same model as in Table 7, but it explains each individual outcome variable used to construct internet use. While the results show that CEAT would have a positive impact on these outcomes, these results are not statistically significant except for E-participation. Increasing one maturity stage in CEAT would increase e-participation (variable that ranges from 0 to 100) around 14.5 units. To illustrate the size of this impact, consider for example the country with the lowest e-participation index in our sample with a value 11.86. An identical country, but with an average maturity stage in CEAT one unit larger, would have an estimated value in its e-participation index of 26.35 (more than double). Centrality was the other explanatory variable in our model that had a significant and positive impact on e-participation, although the size of this impact was smaller.

Our model explains particularly well the outcome variables e-government, secure servers, and e-participation, explaining the 85%, 75%, and 63% of the variance of these three variables respectively. Notice that, for these three outcomes variables, there was availability of data for almost all the countries in our sample (our initial the sample had 80 countries reviewed under the CMM). While the number of observations for explaining the percentage of firms with web was close to 80, the model did not explain this variable very well. Only centrality seems to have a positive impact on the percentage of firms on the web. The model did not explain well the remaining three outcome variables, gig economy, business usage, and access account, with R-squares 0.16, 0.54, and 0.56, respectively. Moreover, the number of observations was particularly low for these three last estimations.

Table 8. Regressions to explain outcome variables.

	Firms with web	Access account	Secure servers	E-Government	E-Participation	Gig economy	Business usage
CEAT	7.20+	5.75+	0.16	3.85	14.49**	5.13	6.70
	(4.25)	(3.23)	(0.42)	(2.66)	(5.38)	(7.43)	(4.76)
Centrality	0.38*	-0.25**	0.01	0.33***	0.39**	-0.29	-0.23
	(0.16)	(0.08)	(0.01)	(0.07)	(0.13)	(0.20)	(0.14)
Scale	2.05+	-1.59+	0.87***	1.15+	2.53+	0.24	2.29+
	(1.10)	(0.86)	(0.12)	(0.62)	(1.42)	(1.93)	(1.32)
Wealth	1.18	10.24***	1.02**	5.42**	-1.65	8.87	11.66**
	(3.53)	(2.45)	(0.30)	(1.81)	(3.60)	(5.70)	(3.97)
Constant	-36.74	-41.11*	-18.94***	-35.80*	-26.50	-38.95	-92.69*
	(32.29)	(18.55)	(3.27)	(16.44)	(37.50)	(55.35)	(34.91)
N	78	55	79	79	79	52	52
R-sq	0.47	0.56	0.75	0.85	0.62	0.16	0.54

Robust standard errors in parenthesis below the corresponding coefficient.
+ $p < 0.10$, * $p< 0.05$, **$p< 0.01$, *** $p < 0.001$.

4.2. Path analysis

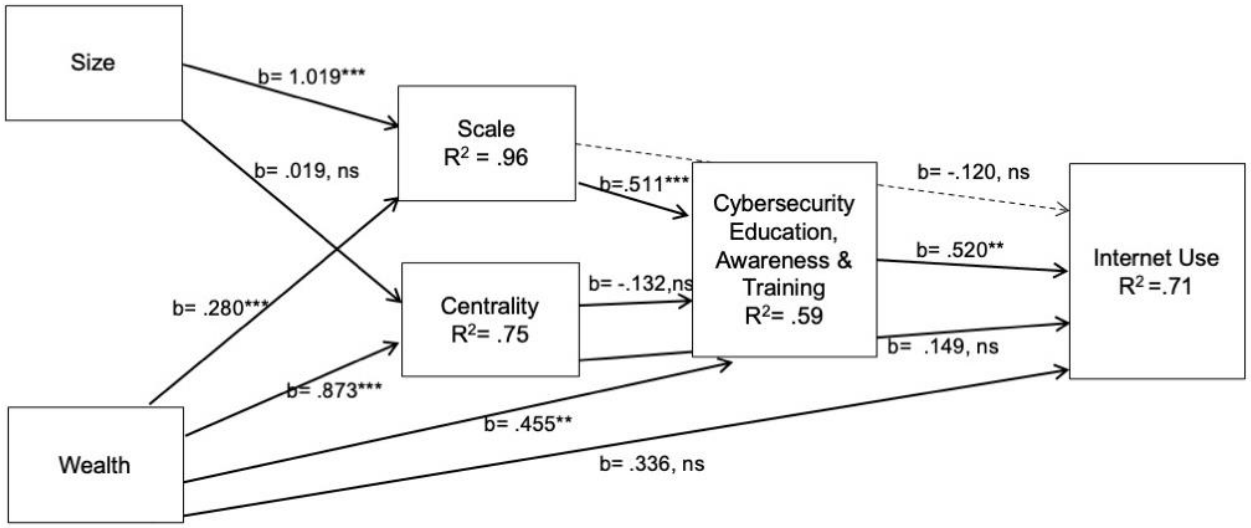
A latent variable structural model was used to test the dimension of education, awareness and training and how it is associated with our indicators of the centrality and scale of internet use, given the other external variables of scale, scope and wealth . By using this model, it allows us to better understand the construct of CEAT and how it impacted internet use, given the other external variables that are also impacting internet use. This model of key factors shaping cybersecurity capacity building impacts evolved over a series of studies (Dutton et al, 2019; Creese, Dutton, Esteve-Gonzalez, & Shillair, 2021b).

The data was analysed using SmartPLS software (Ringle et al., 2015). The model fit measures were good with Standardized Root Mean Square Residual (SRMR) of 0.046 in the saturated model and 0.048 in the estimated model. Acceptable models are conservatively less than 0.080 (Bentler & Bonett, 1980). The Normed Fit Index (NFI) also indicated a good fit with .951 for the saturated model, as measures over 0.90 being considered acceptable when considering incremental fit (Bentler & Bonett, 1980). All items were tested for collinearity and all measures had a VIF of less than 5.0. The results of the analysis are in Figure 4.

The CEAT construct was overall significant for internet use. The construct of wealth, while having a strong beta (b= 0.336) had a high standard deviation (st. dev. 0.245), which is not surprising since our sample has a large proportion of lower income countries. The significance of wealth to CEAT (b=0.455, $p< 0.01$) demonstrates how having greater financial resources for education, awareness and training led to more use of the internet for commercial purposes. The scale of use to CEAT (b=0.288, $p<0.001$) indicates that perhaps the sheer numbers of users would lead governments to increase CEAT if possible.
These quantitative analyses left questions about why the levels of CEAT were so low across so many of the nations and why the relationship between CEAT and internet use was not

more prominent. For this purpose, we turned to a more qualitative look at the indicators of CEAT within each nation in our sample, which is discussed in the next section.

Figure 4: SEM analysis results



* p < 0.05, ** p < 0.01, p< *** .001. ns= not significant

5. Qualitative Insights on Factors Contributing to Low Levels of CEAT

Behind the empirical analysis we have just presented, there were in-depth expert analyses, desk research, and discussions with country experts within each nation. All this information can be found in the national evidence-based reports produced after reviewing countries through the CMM. To prepare a country report, researchers from the Global Cybersecurity Capacity Building Centre arrange focus group meetings with teams of up to a dozen people from ten different stakeholder groups. These focus groups meet and discuss the dimensions of the CMM, giving their evaluations as insiders of what steps the country is taking. Their responses enable the team to rank the maturity of indicators that form the aspects and factors of that dimension. Each country has an average of ten stakeholder clusters from: academia, civil society, and the Internet government representatives; criminal justice and law enforcement, defence, and intelligence communities: legislators and policy makers; CSIRT and IT leaders; critical national infrastructure workers; private sector; cyber task force; and international non-government agencies. The focus group feedback is coded by the research team and the results are shared with the host country along with the publication of a country report.

This section includes a qualitative analysis of national CMM reports for a subsample of our 80 countries to look at any common patterns that may explain the challenges in building capacity in CEAT. Each report was iteratively reviewed to look for common themes and patterns related to CEAT initiatives. These were further clustered, and comments were examined for evidence that would give further insights. To ensure comparability of responses, we selected those nations where at least one member of the GCSCC participated in the national CMM review (conducting desk research, consultations with representatives of national stakeholders, and writing the national report). All these steps were to improve internal validity and rigor of the observations (Miles, Huberman, & Saldaña, 2018).

Therefore, this qualitative component is based on a subset of CMM reviews conducted in 23 countries throughout Europe, Africa and the Oceania region as part of the GCSCC programme.[11] We included five extra countries with non-published reports to make sure we were not biasing the analysis with our criteria. The following challenges to the development of CEAT were observed: 1) the lack of a coordinated cybersecurity awareness programme at the national level; 2) a limited level of awareness at the executive or board level; 3) inadequate national budgetary allocations for cybersecurity education; 4) a limited number of qualified educators in cybersecurity; 5) the migration of skilled cybersecurity professionals; 6) the high-cost of professional cybersecurity certificates; 7) a lack of knowledge transfer across nations; 8) language barriers; 9) a limited role of community leaders. These areas will be discussed in the following sections in more detail, but it was apparent that there is no one single problem to remedy but a set of challenges facing greater CEAT.

5.1. National awareness raising programmes

In several countries, some ad-hoc initiatives in cybersecurity awareness-raising from public and private entities were available. However, these campaigns were not coordinated and were often run without a government-led agency that would have the sufficient authority and resources to develop and implement a national cybersecurity awareness raising programme. In addition, many countries lacked a national online cybersecurity awareness portal that would serve as a single point of contact on awareness and disseminate all possible programmes. These results are in line with the findings of Nagyfejeo & Solms (2020).

[11] This qualitative analysis includes the following countries, with the year of finalisation of the corresponding CMM report in parentheses: Albania (2018), Bangladesh (2018), Bhutan (2015), Bosnia and Herzegovina (2019), Brazil (2018) (2019), Cyprus (2017), Gambia (2018), Ghana (2018), Iceland (2017), Indonesia (2015), Kiribati (2019), Kosovo (2019), Kyrgyzstan (2017), Lithuania (2017), Madagascar (2016), Niger (2019), Samoa (2018), Senegal (2016), Serbia (2019), Sierra Leone (2016), Switzerland (2019), Tonga (2018), and Tunisia (2019).

5.2. Board-level cybersecurity awareness

Ensuring that cybersecurity is a top management, board-level concern is critical as they play a vital role in determining the response to cyber threats in the organisation. Results from the CMM reports indicate that board-level understanding of cybersecurity is relatively limited and reactive rather than pro-active. The participants of focus group discussions suggested the need for more targeted awareness campaigns for executives regarding how cybersecurity risks affect their organisations. However, executives of multinational companies and from the finance sector, such as in banking, appeared to be more aware of cybersecurity risks. Another challenge raised was that IT staff lacked the ability to demonstrate the value of cybersecurity to the management and the boards, such as not speaking the same "business language". In addition, CEOs worry of the financial burdens of cybersecurity for the organisation.

5.3. Language barriers

Overcoming cybersecurity communications barriers between cybersecurity professionals and non-technical users (e.g. government officials, company's senior executives, average citizen) remains a challenge and creates a disconnect. Moreover, some CMM reports highlighted the lack of appropriate local language options to explain new technological concepts for the citizens therefore creating another language barrier in the effectiveness of cybersecurity awareness raising programmes.

5.4. Cybersecurity budgets

Even though integrating cybersecurity on the national curriculum is seen as essential to develop cybersecurity skills and awareness-raising throughout the formal education systems (ITU, 2018), it is a struggle to get budgetary support to achieve those goals. The CMM reports noted that many countries allocated no or limited budgets for cybersecurity

education and the national curriculum due to resourcing and capacity constraints. As a result, there is often no resourced formal national curriculum for cybersecurity training or degree. In exceptional cases, the government, schools and industry collaborated in an ad-hoc manner to supply the resources necessary for CEAT. Given the rapid transformation and expansion of the cyber domain, academic institutions are struggling to keep their curricula up-to-date.

5.5. Qualified educators in cybersecurity

Globally, the demand for cybersecurity skills far exceeds the current supply of traditionally qualified individuals (TechRepublic, 2021). This problem was confirmed during the focus group discussions for the CMM reports, describing that the market requires technical and professional cybersecurity skills that are often not obtained through rigorous theoretical programmes offered by universities and other institutions. Given a shortage of qualified cybersecurity educators/staff and limited expertise to teach cybersecurity, university level supply is limited. Also, these assessments highlighted that women were dramatically underrepresented in cybersecurity, a problem that might need university level recruitment, outreach and retention initiatives.

5.6. The cybersecurity brain drain

Generally, government representatives discussed the struggle to find and keep skilled cybersecurity talent due to strict budgetary concerns, working with legacy technologies, and often cannot pay as well as the private sector, which was also found by other research (e.g., Crumpler & Lewis, 2019). We found that qualified IT staff often leave the country and go abroad to seek better opportunities in the European Union or North America. Graduates are often recruited by international companies directly at the university. Also, some organisations are not allowed by law to hire new IT staff due to some budget restrictions. Those ICT professionals who remain in the country usually move into the private sector to earn higher

salaries and find jobs for more specialised staff. Many companies opt for outsourcing ICT work.

5.7. Cybersecurity certifications

Cybersecurity job responsibilities are complicated and span across all organisations, requiring continuous learning and on-the-job training. The CMM reports revealed that professional training certificates were often prohibitively expensive and often available only abroad, therefore many experts were self-educated or gained their expertise on the job. Another challenge mentioned was the lack of transparency concerning qualifications, resulting in many job holders not having the training and professional qualifications to meet the demands of their roles. Also, training initiatives within the public and private sector are still largely focused on IT professionals.

5.8. Barriers to knowledge transfer

The CMM reports highlighted the need to have more knowledge transfer within both the public and private sector. In some countries, the private enterprises usually train their own staff internally. One major challenge that came out of the reviews was that due to the high rate of staff turnovers, government agencies and companies do not spend enough time on introducing knowledge and properly sharing it, resulting in new employees being not fully briefed on their tasks. This is a concern for future economic growth as organisations can benefit greatly from knowledge and skills acquired by their employees after completing previous cybersecurity training (Kroll et al., 2016).

5.9. Role of community leaders

Participants from some regions in Africa and Oceania highlighted the vital role that community leaders, such as chiefs of local village councils and religious leaders, play within

society. They could play a crucial role in shaping citizens' perspectives on cybersecurity and awareness on cyber risks but are seldom enrolled in this effort (Nagyfejeo & Solms, 2020).

6. Discussion

Common sense might support the value of cybersecurity education, awareness, and training; however, up to this point, there has been little systematic empirical evidence to support its impact, especially in developing nations. This research demonstrates the importance of CEAT to the increased use of the Internet for economic purposes. Current levels of CEAT reflect the knowledge gaps between the relatively poor and wealthy nations, and the resulting impacts on potential economic gains that countries could experience. This empirical analysis demonstrates the close ties to scale of Internet access and growth in CEAT. This would suggest that as the digital divide is reduced, CEAT should also increase in developing nations. However, this prospect is offered with the caveat that an increase of cybersecurity education, awareness and training will not necessarily happen organically. Just as the famous Coleman Report of 1966 on education in the US found it is controversial to assert any impacts without being challenged. Conditions, such as the education level of parents, or social norms may encourage "safe" online practices rather than insecure use.

First, the internet has been found to be an "experience technology" in many respects (Dutton & Shepherd, 2006). For example, you can tell someone that you can find anything online using search, but until someone experiences the use of search, they often do not quite understand the power of search. Therefore, it is common for many to learn for themselves through experience online. While this suggests that awareness and skills will improve over time, many internet users across all nations are relatively inexperienced and require more focused CEAT.

Secondly, other users are often helpful in teaching friends, colleagues, and family how to use the internet and social media, including how to be safe online. Social learning is

potentially as important if not more than organized instruction. Let us call this a rational theory of CEAT – that greater education, awareness, and training will enable safer internet use and therefore enhance the vitality of internet and social media use. Even if learning from experience and through social interaction can benefit users, CEAT should make a difference in capacity building.

Thirdly, the level of CEAT required to make a difference for individuals and organisations require multi-stakeholder commitment and resources to implement effective, and culturally aware programs to meet increasingly sophisticated threats. The qualitative findings discussed in section 5 provide detailed examples of the problems created by a lack of the economic and financial resources to provide CEAT.

The empirical findings of this research add support to conventional wisdom about the need for cybersecurity education, awareness raising, and training. However, the findings also document the relatively low levels of CEAT initiatives across the nations of our sample. In short, CEAT can make a positive impact, but such initiatives are being under-utilized in developing the cybersecurity capacity of nations. This research adds empirical support to demonstrate the need for national investment in CEAT even as they invest in reducing the digital divide.

The implications of this analysis for policy and practice are critical. It is not simply a few case studies of CEAT that underscore the problematic levels at which these initiatives are currently pursued. In fact, this may be a far broader problem with most national implementations of education, awareness raising, and training in cybersecurity requiring more investment and higher levels of maturity.

The qualitative analysis underscored the multiple factors undermining CEAT across our nations. That said, one key problem is that building community awareness of online risks was not always a priority. For several decades, governments and multi-stakeholder

organizations in many countries have focused on getting internet access to as much of their population as possible, especially in developing countries (Hargittai, 1999; Viard & Economides, 2014). Internet access was shown to increase multiple economic indicators, with a robust telecommunications policy being crucial to national connectivity (Hargittai, 1999). National policies often supported distribution, and efforts to get internet access to marginalized groups (Cullen, 2001) as the internet allowed access to educational materials, health information (Cline & Haynes, 2001), economic opportunities (Manyika & Roxburgh, 2011), and governmental services (Rice, 2002). Efforts were often focused on getting individuals engaged online, even for sensitive transactions like banking, as these had many advantages for consumers and businesses alike (Jiang et al., 2022). Furthermore, the internet opened up opportunities for individuals to become more than just consumers of information, it was a medium that was allowed individuals to creatively participate in issues of importance (Dutton, 2009). Despite the focus on positive impacts of engaging populations online, the awareness of a need for CEAT is long-standing.

As early as 1986, the Organization for Economic Cooperation and Development (OECD) published *Computer-related Crime: Analysis of Legal Policy* that explored the need for comprehensive education and awareness policies to protect emerging economic development that was based on the internet (Development Committee for Information, Computer, & Communications Policy, 1986). Since 1998 the United Nations has issued General Assembly resolutions calling for international norms in using ICTs securely and setting up open ended working groups and groups of governmental experts (GGE) to explore how global efforts can support innovation and improve economic conditions peacefully (United Nations, 2021). Groups of researchers and practitioners started to meet to address the need emerged for better cybersecurity protections. In 2002 the annual Workshop on the

Economics of Information Security (WEIS) met that brought together technologists, security professionals, academics, economists, legal, and policy experts (Moore et al., 2009).

Some notable national level efforts to improve cybersecurity education include the US National Initiative for Cybersecurity Education (NICE) that lays out a structure for formal cybersecurity educational efforts (Newhouse et al., 2017). Businesses and organizations also work to build effective cybersecurity awareness programs (Bada & Nurse, 2019). And those OECD countries that are more mature in cybersecurity combine policies led by governments and partnerships between universities and private corporations interested in strengthening local expertise (Radunović & Rüfenacht, 2016). Despite these laudable efforts to improve cybersecurity resilience, as this research shows, there are many challenges ahead, especially for developing nations.

7. Summary and Conclusions

The quantitative findings of this paper provide added empirical support for the effectiveness of CEAT initiatives across a sample of 80 of countries. This is in line with related research that shows that overall cybersecurity capacity building has had an independent impact on key outcomes (Dutton et al., 2019; Creese et al., 2021b). This suggests that CEAT programs, as developed across our population of 80 nations, have demonstrated an independent impact on key outcomes of internet use, as detailed in the previous sections. However, the countries in our sample showed a low maturity in CEAT. The results of a qualitative analysis related this finding to a weak coordination of cybersecurity awareness programmes, a limited level of awareness among executives, insufficient budgetary allocations for CEAT, and a cybersecurity brain drain, among other reasons. Thus, the utility of this research that is focused on CEAT empirically demonstrates the value of efforts to improve education, awareness, and training as there are measurable returns on internet use and its associated economic growth.

That said, there are limitations of the present study. While we have reviews relevant to CEAT for 80 nations, we lack adequate secondary data to incorporate of all of these nations in our multivariate analyses. Secondly, while we have a statistically significant relationship between CEAT and internet use, it is largely driven by one or another component of the combined index, such as e-participation. Thirdly, and more importantly, the low level of CEAT across the low-income nations and the limited range of CEAT even among wealthier nations suggests that the adequacy of CEAT is a basic problem globally. The development of more precise indicators of CEAT, which is being developed through the use of 'structured field coding', and the expansion of our sample through additional reviews and better secondary data sources need to move forward to more definitely examine the validity of our findings.

References

Aikin, M. (2019). Life in Cyberspace. *European Investment Bank.* https://www.eib.org/attachments/eib_big_ideas_life_in_cyberspace_en.pdf

Azmi, R., W. Tibben, & K. T. Win. 2018. "Review of Cybersecurity Frameworks: Context and Shared Concepts." *Journal of Cyber Policy*, September. DOI: 10.1080/23738871.2018.1520271.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security.*

Bentler, P. M., & Bonett, D. G. (1980). Significance Tests and Goodness-of-Fit in the Analysis of Covariance Structures, *Psychological Bulletin*, 88: 588-600.

Cline, R. J. W., & Haynes, K. M. (2001). Consumer health information seeking on the Internet: The state of the art. Health Education Research, 16(6), 671–692. https://doi.org/10.1093/her/16.6.671

Coleman, J. S. (1966). *Equality of Educational Opportunity [summary Report* (Vol. 1). US Department of Health, Education, and Welfare, Office of Education. https://files.eric.ed.gov/fulltext/ED012275.pdf

Coventry, D. L., Briggs, Prof. P., Blythe, J., & Tran, Dr. M. (2014). Using behavioural insights to improve the public's use of cyber security best practices (p. 20). UK Government Office for Science. http://nrl.northumbria.ac.uk/id/eprint/23903/1/14-835-cyber-security-behavioural-insights.pdf

Creese, S., Dutton, W. H., & Esteve-Gonzalez, P. (2021a). 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., Dutton, W. H., Esteve-Gonzalez, P., & Shillair, R. (2021b). Cybersecurity

Capacity Building: Cross-National Benefits and International Divides. *Journal of Cyber Policy*, 6(2), 214-235. Available at: https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1979617

Crumpler, W., & Lewis, J. A. (2019). The cybersecurity workforce gap. Washington, DC, USA: Centre for Strategic and International Studies (CSIS). https://www.csis.org/analysis/cybersecurity-workforce-gap

Cullen, R. (2001). Addressing the digital divide. Online Information Review, 25(5), 311–320. https://doi.org/10.1108/14684520110410517

Development. Committee for Information, Computer, & Communications Policy. (1986). Computer-related crime: Analysis of legal policy. Organisation for Economic Co-operation and Development.

De Zan, T. (2019). *Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions.* Global Cyber Security Centre. https://gcsec.org/wp-content/uploads/2019/02/cyber-ebook-definitivo.pdf

De Zan, T., & Di Franco, F. (2019). *Cybersecurity Skills Development in the EU*. European Union Agency for Cybersecurity (ENISA). https://op.europa.eu/en/publication-detail/-/publication/f28aaf4c-7550-11ea-a07e-01aa75ed71a1

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cyber Security Capacity: Does It Matter? Journal of Information Policy, 9: 280-306

Dutton, W. H. (2009). The fifth estate emerging through the network of networks. Prometheus, 27(1), 1–15.

Dutton, W. H., & Shepherd, A. (2006), 'Trust in the Internet as an Experience Technology', *Information, Communication and Society*, 9(4): 433-51.

GCSCC, Global Cyber Security Capacity Centre (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM). Revised Edition*. http://dx.doi.org/10.2139/ssrn.3657116.

Accessed 1 October 2021

GCSCC, Global Cyber Security Capacity Centre (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM). 2021 Edition*. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf. Accessed 1 October 2021

Hargittai, E. (1999). Weaving the Western Web: Explaining differences in Internet connectivity among OECD countries. Telecommunications Policy, 23(10), 701–718. https://doi.org/10.1016/S0308-5961(99)00050-6

Humphrey, W. S. (1988). Characterizing the software process: a maturity framework. *IEEE software*, *5*(2), 73-79.

IDB & OAS, Inter-American Development Bank & Organization of American States (2020). Cybersecurity. Risks, Progress and the Way Forward in Latin America and the Caribbean. 2020 Cybersecurity Report. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf. Accessed 4 November 2020

ITU (2018). Guide to Developing a National Cybersecurity Strategy, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Jiang, M., Rifon, N. J., Cotten, S. R., Alhabash, S., Tsai, H. Y. S., Shillair, R., & LaRose, R. (2022). Bringing older consumers onboard to online banking: a generational cohort comparison. *Educational Gerontology*, 1-18.

Johnson, J. (2021). Worldwide digital population as of January 2021. *Statista: Internet Demographics and Use.* https://www-statista-com.proxy1.cl.msu.edu/statistics/617136/digital-population-worldwide/

Kassner, M. (2020). 'Cybersecurity Pros: Are humans really the weakest link?', TechRepublic, 21 December: available online at:

www.techrepublic.com/article/cybersecurity-pros-are-humans-really-the-weakest-link/

Kroll, J., Mäkiö, J., & Assaad, M. (2016). Challenges and practices for effective knowledge transfer in globally distributed teams. *In Proc. Int. Joint Conf. Knowl. Discovery, Knowl. Eng. Knowl. Manage (pp. 156-164). DOI: 10.5220/0006046001560164*

Manyika, J., & Roxburgh, C. (2011). The great transformer: The impact of the Internet on economic growth and prosperity (pp. 0360–8581) [1]. McKinsey Global Institute. http://ict-industry-reports.com.au/wp-content/uploads/sites/4/2011/11/2011-the-great-transformer-McKinsey-Oct2011.pdf

Miles, M. B., Huberman, A. M., & Saldaña, J. (2018). *Qualitative data analysis: A methods sourcebook.* Sage publications.

Mc Mahon, C. (2020). In Defence of the Human Factor. *Frontiers in Psychology*, *11:* 1390. https://doi.org/10.3389/fpsyg.2020.01390

Moore, T., Clayton, R., & Anderson, R. (2009). The Economics of Online Crime. Journal of Economic Perspectives, 23(3), 3–20. https://doi.org/10.1257/jep.23.3.3

Morgan, S. (2020). Cybercrime to cost the world $10.5 Trillion annually by 2025. *Cybercrime Magazine*, 13.

Nagyfejeo, E., & Solms, B.V. (2020). Why Do National Cybersecurity Awareness Programmes Often Fail?. *International Journal of Information Security and Cybercrime*, 9(2), 18-27. https://www.ceeol.com/search/article-detail?id=938012

Network Readiness Index (2020) Network Readiness Index 2020. https://networkreadinessindex.org/. Accessed 21 October 2020

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST special publication, 800(2017), 181.

Olmstead, K., & Smith, A. (2017). What the public knows about cybersecurity (pp. 18–18). http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Radunović, V., & Rüfenacht, D. (2016). Cybersecurity Competence Building Trends. DiPLO. https://www.rcc.int/p-cve/download/docs/Cybersecurity%20Competence%20Building%20Trends%20in%20OECD.pdf/9be68dfd9a803a0bcfcf76347d894916.pdf

Rice, R. E. (2002). Primary issues in Internet use: Access, civic and community involvement, and social interaction and expression. In Handbook of new media: Social shaping and consequences of ICTs (pp. 105–129). http://rrice.faculty.comm.ucsb.edu/C36Rice2002.pdf

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). "SmartPLS 3." Boenningstedt: SmartPLS GmbH, http://www.smartpls.com.

Shillair, R., Cotton, S. R., Tsai, H. Y., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. Computers in Human Behavior, 48, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

TechRepublic (2021). The cybersecurity skills gap persists for the fifth year running, https://www.techrepublic.com/article/the-cybersecurity-skills-gap-persists-for-the-fifth-year-running/

United Nations. (2021). Developments in the field of information and telecommunications in the context of international security. Office for Disarmament Affairs.

UNDESA. United Nations Department of Economic and Social Affairs (2021). Division for Public Institutions and Digital Government. https://publicadministration.un.org/egovkb/en-us/Data-Center. Accessed 7 July 2021

Viard, V. B., & Economides, N. (2014). The Effect of Content on Global Internet Adoption

and the Global "Digital Divide." Management Science, 61(3), 665–687. https://doi.org/10.1287/mnsc.2013.1875

Von Solms, B., & Du Toit, J.L. (2021). From Cybersecurity Awareness Programs to Cybercrime Fighting and Prevention Programs. Manuscript in preparation.

World Bank (2021a). Enterprise Survey. https://www.enterprisesurveys.org/en/enterprisesurveys. Accessed 23 June 2021

World Bank (2021b). Global Findex Database. https://globalfindex.worldbank.org/. Accessed 23 June 2021

World Bank (2021c). World Bank Country and Lending Groups. Historical classification by income. https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups. Accessed 22 July 2021

World Bank (2021d). World Development Indicators. https://datacatalog.worldbank.org/dataset/world-development-indicators. Accessed 24 June 2021

Declaration of interests

☒The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Credit Author Statement

Dr. Ruth Shillair: conceptualization, writing manuscript, literature review, methodology, data analysis.
Dr. Patricia Esteve-González: data analysis, writing, feedback.
Dr. William H. Dutton: writing, editing, conceptualization, team leader
Dr. Sadie Creese: director of the global cyber security capacity centre, getting funding and working with stakeholders
Dr. Eva Nagyfejeo: qualitative analysis, review of country review data
Prof SH (Basie) von Solms: qualitative analysis, revisions and feedback on country reviews, expert on Africa and developing nations cybersecurity capacity.