Cybersecurity Capacity Building: Cross-National Benefits and International Divides

Sadie Creese
Professor, Department of Computer Science, University of Oxford and Director of the Global Cyber Security Capacity Centre

William H. Dutton
Oxford Martin Fellow, Global Cyber Security Capacity Centre, and Senior Fellow, Oxford Internet Institute, University of Oxford

Patricia Esteve-González
Oxford Martin Fellow, Global Cyber Security Capacity Centre, Department of Computer Science, University of Oxford

Ruth Shillair
Assistant Professor, Quello Centre, Michigan State University & GCSCC Research Associate

Abstract

The growing centrality of cybersecurity has led many governments and international organizations to focus on building the capacity of nations to withstand threats to the online security of 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 are intuitively valuable, there is a lack of evidence on whether they achieve their intended objectives. This paper takes a cross-national comparative approach to determining 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 underscores a relatively low, formative status of cybersecurity capacity in most of the nations studied, but also shows that relatively higher levels of maturity translate into positive outcomes for nations. The analysis also reveals a capacity divide between countries based on income levels, that reinforces economic divides. The study provides empirical support to international efforts aimed at building cybersecurity capacity, and mitigating gaps based on the wealth of nations.

Keywords: Cybersecurity, Policy, Capacity, Internet, Divides, End Users

Introduction

The global diffusion and growing centrality of information and communication technologies (ICTs), such as the Internet, social media, and related digital technologies has raised concerns over the vulnerabilities to the security of digital devices, data, networks, platforms, and ICT services — what has been broadly referred to as digital security or 'cybersecurity'. Cybersecurity is about '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 et al. 2014: 9). How vulnerable are nations to such malevolent actions and what can be done?

Security issues are not new. However, in the early years of computing, 'computer security' was addressed in most circumstances by an organization'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 organization. As computing has moved toward what was initially called 'resource sharing systems' that allowed many people to use the same system, security issues became more complex (Ware 1970: xv). With the advance of this system online over the Internet and related social media and online platforms, responsibility for security has moved well beyond the reach of any single organization's IT team. It can involve a wide array of actors across the world, including over four and one-half billion Internet users, representing over half of 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 in order to be more resilient 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 to best enhance cybersecurity capacity, which has led to a number of different approaches in business and 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, based on these prescriptive models of cybersecurity capacity, are designed to enable nations to raise their maturity level, such as by prioritizing investment in initiatives designed to improve capacity by identifying strengths and weaknesses. But do such reviews and the investments they support actually payoff for nations? Do higher levels of maturity in cybersecurity capacity building translate into real benefits and fewer security problems for end-users? This is the central question addressed by the present analysis reported in this paper.

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 in order to guide further development of capacity in each nation, the field research data collected for these reviews also yields a rich set of 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 (CCS) that we then use to examine the impact of capacity building on expected outcomes, and the set of factors shaping national capacity building, and affecting its impact, such as the wealth of nations.

The Oxford Project on Cybersecurity Capacity Building: Snapshots of the Security of Nations

The Oxford GCSCC developed one of the earliest and most prominent models of what is entailed in achieving different levels of maturity in capacity building – the CMM. This was first published in late 2014 by the GCSCC at the University of Oxford 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 1).

The first reviews of nations using the Oxford CMM were begun in 2015 (GCSCC 2019: 2). Since launching national reviews of capacity building, CMM reviews have been conducted in over 70 nations across all regions of the world. This paper is based on 73 nations that have been reviewed to date. In most countries, a two to four-person review team from the university visited the country for three to four days to conduct a set of interviews and ten 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. Across the ten groups, each dimension was the topic of at least two modified-focus groups. Together, the groups informed the team on the status of all aspects of the CMM. In some nations, such as those across Latin America and the Caribbean, a review based on the same CMM was conducted by the Organization of American States (OAS), in collaboration with Oxford University, but through questionnaires rather than field visits to key contacts in each nation.

Table 1. CMM Dimensions of Cybersecurity Capacity Building and Associated Factors

	Dimension	*Factors that Define Specific Indicators of Capacity Building*
1.	Policy and Strategy	National Cybersecurity Organization, 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 & 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

The telecommunications sector of the ITU (ITU-T 2008: 2) defined cybersecurity broadly as ‘the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.’ 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 1).

GCSCC and OAS reviews of cybersecurity capacity building across these five dimensions of the CMM have enabled this research to capture indicators of the maturity level on each of these dimensions in the 73 nations, ranging from start-up to formative to established to

strategic and finally to dynamic, the highest level of maturity. Does their level of maturity matter?

Theorising and Establishing the Impact of Capacity Building

Cybersecurity capacity building is a relatively new arena for research, but one in which there has been a growing level of work. There have been major efforts in this area, including the development of a Cyber Readiness Index designed to 'evaluate a country's maturity and commitment to cybersecurity' (Spidalieri 2015: 4), 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 & Alsaleh 2017). Fully a dozen frameworks have been developed and reviewed (Azmi et al 2018).

Despite the development of cyber security frameworks, there has been a lack of systematic empirical research on the actual impact of cybersecurity capacity building. A primary reason lies in the recency of the very concept of capacity building in this area, and the early stages of the GCSCC review process, which has been one of the first. The CMM was only launched in 2015. It was not until 2020 that our team had completed a sufficient number of reviews to undertake a strong empirical study of the impact of different levels of capacity building.

A related reason is the inherent difficulty of measuring cybersecurity capacity (Rosenzweig 2019) and obtaining empirical evidence of its impact, given the many factors involved and reporting, given the reluctance of organizations to share such information (Vaidya, R. et al 2018). One critical aspect of the review process was allowing nations to review all of our judgements of maturity levels and reach a mutual agreement on their validity. The report was then owned and published by the respective government.[1] This often added up to a year to the completion of a review, but also added an additional albeit constructive stage of review and discussion to ensure that there was mutual agreement on its validity. Given these limitations, there have been a limited number of reviews of capacity building initiatives and their impacts (**Error! Reference source not found.**). These initiatives consider different frameworks to measure different issues related to cybersecurity, and they differ as well on

[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.

the sample of countries, the methodologies, and the availability/publication of their outcomes.

Box 1. Cybersecurity capacity building initiatives

Combatting Cybercrime (World Bank) is a toolkit for emerging economies to assess their current capacity and a source of good international practices to combat cybercrime.

Cyber Readiness Index (Potomac Institute for Policy Studies) assesses the cyber readiness of countries through indicators based on facts and primary sources (empirical research and documentation).[2]

Cybersecurity Capacity Maturity Model for Nations (Oxford's GCSCC) assesses countries' cybersecurity capacity maturity based on field interviews, focus groups, and desk research.[3]

Global Cybersecurity Index (ITU) measures the commitment of countries to cybersecurity based on a question-based online survey.[4]

National Cyber Security Index (E-governance Academy) measures preparedness of countries to prevent cyber threats and manage cyber incidents based on public evidence on legal acts, official documents, and official websites.[5]

National Cyber Strategy Development & Implementation (MITRE) assesses cyber capacity building through a field forum (interviews, seminar or workshops).[6]

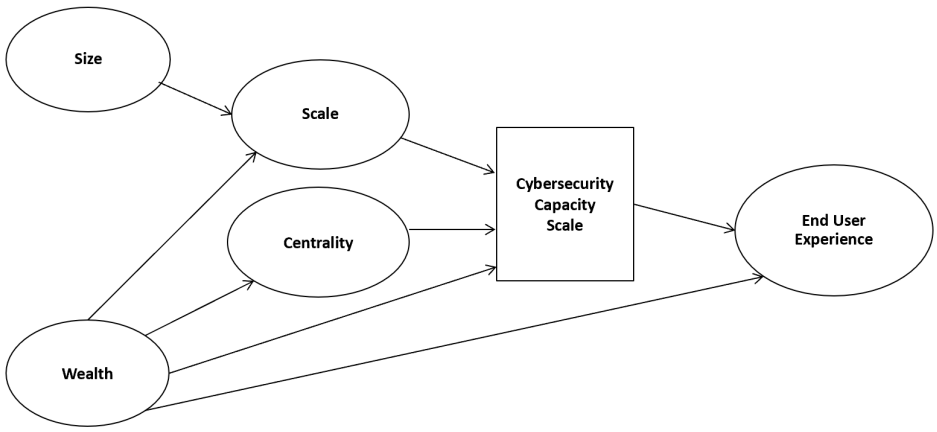
The Global Forum on Cyber Expertise is a multi-stakeholder community that aims to strengthen cyber capacity building globally by international cooperation.[7]

Networked Readiness Index (WEF) is an aggregated indicator of the impact of ICT in countries based on the WEF's Executive Opinion Survey and data from international organizations (ITU, WB, and UN agencies such as the UNESCO).[8]

[2] See https://potomacinstitute.org/images/CRIndex2.0.pdf, accessed on 28 April 2020.
[3] See https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf, accessed on 28 April 2020.
[4] See https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, accessed on 28 April 2020.
[5] See https://ncsi.ega.ee/methodology/, accessed on 28 April 2020.
[6] See https://www.mitre.org/publications/project-stories/mitre-strengthens-cyber-capacity-of-developing-nations.
[7] See https://thegfce.org/, accessed on 1 May 2020.
[8] See http://www3.weforum.org/docs/GITR2016/GITR_2016_full%20report_final.pdf, accessed on 28 April 2020.

An exception is one empirical study of our own that employed surrogate indicators of cybersecurity maturity based on available secondary data (Dutton et al 2019). This analysis found evidence of capacity building having an independent and positive impact on the end-user's experience, including positive impacts on overall utilization of the Internet, controlling for key variables such as the wealth of nations. Its major shortcoming was not having more direct empirical indicators of cybersecurity capacity maturity – only more indirect surrogate indicators. However, from this study, we found evidence of a positive role for capacity building over a wider number of end-users experiences, and were able to develop and test a simplified theoretical framework of the key dynamics shaping the end-user experience (Figure 1).

Figure 1. Theoretical Framework*



*Adapted from Figure in Dutton et al (2019) to align with variables in this analysis.

This framework (Figure 1) provides a basis for the present analysis which is anchored in more direct, field research data on cybersecurity capacity building. It seeks to assess the impact of capacity building by gauging its consequences for the behaviour and problems faced by end-users, what we call 'End User Experiences'. This expands on the negative experiences analysed in Dutton et al (2019) by also considering positive experiences such as freedom of expression and ICT usage by end-users. The central question is whether indicators of cybersecurity capacity, derived from our field research in 73 nations, will have a direct and positive impact on end-user experiences when controlling for key antecedent and moderating variables.

Dutton et al (2019) examined a large set of potential control variables, which were re-examined in the context of the present analysis. The key antecedents in both studies were determined to be the scale and centrality of Internet use in the country.[9] How many people use the Internet reflects the scale of use, and the proportion of the public online reflects its centrality to the nation. The larger the proportion, the more likely the Internet can be used for more significant activities, such as banking or shopping. In turn, the scale and centrality of Internet use are hypothesized to be shaped primarily by the size and wealth of the nation. 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 the studied end-user experiences?

Data

As noted above, the analysis is based on cross-sectional data drawn from capacity reviews conducted in 73 nations, all reviewed on the basis of the CMM. The CMM is a framework to assess the maturity of a country regarding its cybersecurity capacity across five different dimensions (Table 1 above). Each dimension is split into different factors, and each factor includes multiple 'aspects' which were calibrated by a set of indicators defined for each aspect. Each aspect contains direct indicators of cybersecurity capacity within five maturity stages: (1) Start-Up, (2) Formative, (3) Established, (4) Strategic, and (5) Dynamic. Although the maturity stage of each aspect is characterized by different indicators, the meaning of each maturity stage has a common definition across aspects allowing for their comparison (GCSCC, 2016: 7). Therefore, within the dataset, each aspect is considered an ordinal variable that can take a value between 1 and 5 according to the increasing maturity scale defined in the CMM (GCSCC, 2016).

As noted above, two different approaches to data collection were used to gauge the maturity stage of all aspects in the CMM. Each used somewhat different methodologies. The main approach involved field research and the second was based on questionnaires.

Field Research Through Modified-Focus Groups and Interviews

[9] 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.

The field research approach was based on the GCSCC employing modified-focus groups using mixed methods to generate ordinal scores for each dimension based on qualitative coding (Williams, 2002; Knodel, 1993; Krueger and Casey, 2014). They used 'modified-focus groups' rather than traditional focus group facilitation. For example, facilitators in the field sought to open discussion and gain information about each dimension of cybersecurity capacity from multiple groups of stakeholders. Rather than trying to generate a wide range of answers, the groups were moderated to home in on information that would enable them to determine the best rating for each aspect of the CMM model. For example, the research team did not weigh all expressions equally, but instead sought to determine and prioritize the most credible and valid answers based on the totality of the information obtained.

This process involved a review team from Oxford (or a partner institution)[10] traveling to each country and conducting about ten group sessions in the field with key representatives of national stakeholder clusters, enumerated in Box 2. Participants in the discussions were identified prior to the field visit and clustered into groups based on their expertise in each dimension of the CMM. Each of the ten sessions ran for about 2 hours and had between 5 to 15 participants – all stakeholders in the nation's cybersecurity, who represented different institutions and different kinds of expertise (Box 2).

Box 2. Stakeholder Clusters Participating in the Modified-Focus Groups

Academia, Civil Society groups, and Internet Governance
Criminal Justice and Law Enforcement
Cyber Task Force
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

[10] Given the increasing demand of CMM reviews, some country reviews have been implemented joint with strategic partners (ITU, NRD Cyber Security, Oceania Cyber Security Centre, and the World Bank) but following the same methodology with modified-focus groups and interviews to national stakeholders.

Each session focused on one or two dimensions of the model to ensure that each dimension was discussed by more than one modified-focus group. During each session, the review team asked questions to guide discussions around indicators of relevance to the dimensions being considered by that group of stakeholders. Each session was recorded with the consent of all participants, assuring the participants that the recordings would be used solely for the purpose of writing the review, and accurately representing their views.[11] This meant for example that no one would be quoted without their express permission. It did allow for the resulting ratings of maturity to be used as data in our research. Across all ten modified-focus groups, indicators tied to over fifty aspects of all the factors related to the five dimensions were covered.

Prior to the field research, desk research was conducted to ensure that the moderators and research team were aware of basic information about the nation, including governance, business and industry, and cybersecurity operations and officers in the country. After the field work, the evidence provided in different sessions was triangulated with a separate desk research phase, sometimes requiring further documents or interviews to fill any gaps, such as an aspect that could not agree to the appropriate maturity level.

Online Questionnaire Administered by the Organization for American States

The GCSCC collaborated with the Organization of American States (OAS) and the Inter-American Development Bank (IDB) to develop an online survey for their member states. Based on the CMM model, adapted to the particular context of Latin America and the Caribbean countries, the survey was available in English and Spanish. OAS sent the survey to their member states, asking their point of contact in each nation to distribute the survey to those in their nation with the expertise to provide the most reliable information about cybersecurity in the country. Multiple respondents in each country returned their questionnaires to OAS, which aggregated responses to arrive at maturity scores for each dimension. The aggregated scores were then sent to each member state for validation, leading to the final maturity stages of each aspect, which were published in IDB and OAS (2016).

Combined Data Set

[11] During the sessions, the Chatham House Rule was used to promote the openness of a discussion, leading to the non-attribution of specific statements. See https://www.chathamhouse.org/chatham-house-rule, accessed on 28 April 2020.

The research team at GCSCC subsequently reviewed the data to identify outliers. This led to only one nation being removed from the data set. Generally, there was remarkable coherence, such as inter-item reliability, and construct validity, across the nations that participated in the study. Throughout the analysis phase, the team continued to look for anomalies that might be attributed to the different methodological approaches but found clear and reliable patterns indicating that the data from the two methods could be validly combined.

The present paper is based on data at the aspect level of 42 countries reviewed once by the GCSCC during the period 2015-2020, and 31 countries surveyed by OAS (IDB and OAS, 2016). Table 2 describes the 73 countries in the study's sample by region and income classification, as defined by the World Bank (2019b) during the year of the CMM review.

Table 2. 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	*Low: 8*	
Europe and Central Asia	14	*Lower-Medium: 21*	
South Asia	3	Upper-Medium	33
East Asia and Pacific	9	High	11
Latin America and the Caribbean*	31		
Total	73	Total	73

*Collected by the Organization of American States, based on the GCSCC's CMM.

Creating Maturity Scores for Each Level of Analysis for a National Score

The research team analysed data at the aspect level, since this was the finest level of detailed data collected through both methods. Over time, the CMM has included new aspects to adapt the model to the changing topic of cybersecurity capacity. For backward comparison reasons, this article considers only those aspects included in the first countries assessed under the CMM. Thereby, the same aspects are used for all nations, even though more recent reviews collected data on new aspects added from later revisions of the model.

Multivariate approaches were used 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 level that they could be combined in a single average for each factor.[12] Given reliable scales for each factor, we then analysed all factors by their respective dimension. Again, the factors were well 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.

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 3). 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 is the variable that we use as a summary indicator of each nation's average level of cybersecurity capacity.

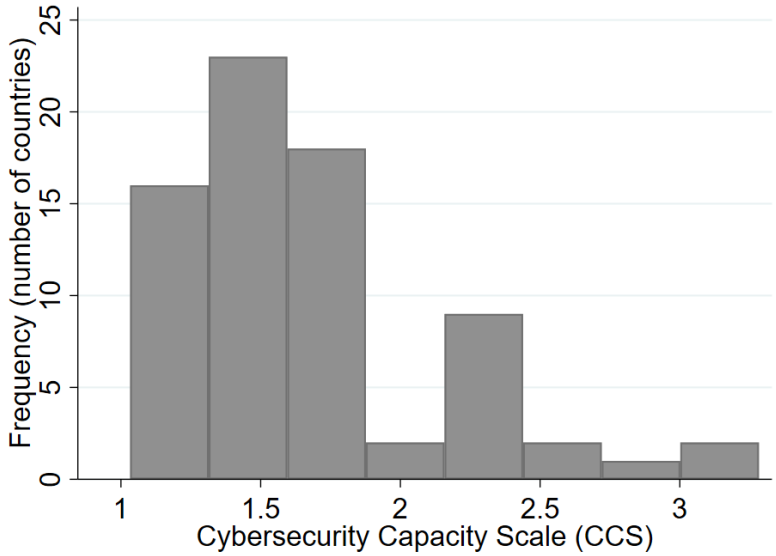
Table 3. Pearson's correlation coefficients between the CMM dimensions for the sample of countries. All coefficients are significant at 0.001 level.

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 & Regulatory	0.78	0.88	0.78	1.00	-
D5 Technology	0.85	0.81	0.75	0.79	1.00

Error! Reference source not found. displays the descriptive statistics of CCS, graphically presented in Figure 2. On average, the countries in the sample have a low score (1.67) indicating that it is hard for these nations to have a maturity stage higher than formative in 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).

[12] The formal review process resulted in factor maturity scores ranging from 1 to 5, determined by whether the nation met all the criteria defined as critical to its stage of maturity; that is, a factor's maturity stage is the minimum maturity stage of all aspects contained in this factor. In this study, we did not round down to the fully achieved level of cybersecurity. Instead, we calculated the average maturity stage and kept the actual number of indicators achieved in order to capture the actual variance across nations that were rated at the same overall level of maturity.

Figure 2. Histogram of CCS. The 73 observations in the sample were divided into 8 bins with a width of 0.28 units of the variable CCS.



To help determine the validity of this single indicator, the relationships between the CCS variable and other alternative indicators of national cybersecurity were analysed. As Table 4 shows, there was a positive and significant correlation (Pearson's correlation coefficient significant at 0.001 level) to alternative variables on cybersecurity, including the Global Cybersecurity Index from ITU, the Networked Readiness Index from WEF, and the number of secure servers from Netcraft.[13] These correlations support the validity of our indicator of cybersecurity capacity – CCS.

Table 4. Pearson's correlation coefficients between CCS and alternative indicators. Number of observations in parentheses. All coefficients are significant at 0.001 level.

Indicators	CCS
Global Cybersecurity Index (ITU)	0.67 (72)
Networked Readiness Index (WEF)	0.80 (58)
Number of Secure Servers, log (Netcraft)	0.82 (72)

[13] 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 this country sample. To address these issues, we applied the natural logarithm of the number of secure servers.

Table 5: Variable definitions and descriptive statistics.

Variable	Definition	N	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
Encounter Rates	Percentage of computers running Microsoft real-time security products that report a malware encounter (Microsoft).	41	22.85 (8.90)	3.70	52.90	Own calculus with data from Microsoft (2015; 2016; 2017)[14]
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)[15]
Centrality	Percentage of population that has used the Internet in the last 3 months (ITU).	73	48.59 (23.62)	4.71	98.26	WB (2020a)[16]
Scale	Natural logarithm of the number of Internet users; Internet users calculated with *Internet Users* and *Total Population.*	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)[17]
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)[16]
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)[16]
Piracy	Unlicensed software units as a percentage of total software units installed on personal computers (WEF).	40	69.15 (15.93)	24.00	90.00	WB (2019a)[16]
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)[14]
Voice and Accountabili-ty	Citizens' perceptions of their participation in selecting their government, freedom of expression, freedom of association, and freedom of media; units of a standard normal distribution (Kaufmann et al., 2010).	73	0.23 (0.61)	-1.14	1.62	WB (2020b)[14]

[14] These sources provide the encounter rates for the first three months of 2017, the average encounter rate of the first quarter of 2016, and the average encounter rate of the third and fourth quarters of 2015. We calculated the average encounter rate for the first quarter of 2017, and the average encounter rate of the third and fourth quarters of 2015. We used the most recent value available for missing years.
[15] Data available until 2018; we used the most recent value available for missing years.
[16] 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).
[17] Data available until 2016; we used the most recent value available for missing years.

The theoretical framework described in Figure 1 conceptualizes 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, total population, number of Internet users, and percentage of Internet users, correspondingly, as proxies of these determinants. Following the model, we use total population as a demographic variable hypothesized to shape the scale of the national cyberspace infrastructure. Three variables (Size, Wealth, and Scale*)* have a different scale to the rest of variables and a highly skewed distribution given this country sample, which includes a sizeable proportion of low-income nations, as discussed later in this article. To address these issues, we applied the natural logarithm of the value of these variables.

The second part of the model considers the impact of cybersecurity capacity on some key outcomes or experiences of cybersecurity for end-users. The experiences of end-users are likely to vary according to the context of their online activities, such as in using the Internet for work, shopping or social communication. Therefore, we consider different available sources that approximate different outcomes of cybersecurity for end-users. As in Dutton et al (2019), we consider Piracy and Encounter Rates as negative outcomes and, in addition, we consider as positive outcomes three indicators of ICT adoption and usage by the private sector (NRI: Business Usage), government (NRI: Government Usage), and private individuals (NRI: Individual Usage). Finally, we consider Voice and Accountability to capture the citizens' perception of freedom as another relevant experience of end-users. Table 5 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 hypothesized 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, such as wealth. 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 heteroskedasticity-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 (β_j), and an additive error (u_i). Coefficients β_j correspond to the marginal effect of each independent variable. When we consider the natural logarithm of an independent variable, the interpretation of coefficient β_j correspond to the change in $E[y|\mathbf{x}]$ as a proportionate change in x_{ji} (see, for example, Cameron and Trivedi, 2010, p.85).

$$y_i = \beta_1 x_{1i} + \beta_2 x_{2i} + \cdots + u_i \qquad (1)$$

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 in order 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, 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 correct for attenuation (Dijkstra & Hensler, 2015). As stated by Dijkstra and Hensler (2015), "for every pair of latent variable scores $\tilde{\mathrm{n}}_i$ and $\tilde{\mathrm{n}}_j$, the consistent correlation cor($\tilde{\mathrm{n}}_i, \tilde{\mathrm{n}}_j$) is calculated as follows:"

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

Results of the Analyses

OLS regressions

Table 6 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 explain 68 percent 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 equal, a 1 percent 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 5 dimensions of the CMM. Similarly, ceteris paribus, a 1 percent increment in Scale would increase CCS by 0.11 units.

Table 6: OLS regressions to explain cybersecurity capacity scale (CCS). Robust standard errors in parentheses. Symbols ***, **, *, + indicate, correspondingly, levels of significance <0.001, <0.01, <0.05, and <0.1.

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

Table 7 displays the estimations of the second part of the model that shifts to explaining the impact of CCS on six different outcomes. Columns (1) and (2) show the estimations to explain two negative outcomes, Piracy and Encounter Rates. The level of Piracy roughly indicates the proportion of computers that do not have licenses and are therefore not automatically updated, such as with security updates. Encounter Rates are provided by information sent Microsoft from licensed computers that provide an indication of how subject these systems have been to malicious users. Both indicate bad experiences for users, but are quite different, such as Encounter Rates providing no information about users with pirated software.

The only significant variable that explains Piracy is CCS; all things equal, an increment of a unit in CCS is estimated to reduce the percentage of unlicensed software by 18 percentage points. In contrast, however, while CCS has a negative relationship with Encounter Rates, the relationship it is not statistically significant. The only variable with a significant impact in (2) is Centrality*;* ceteris paribus*,* an increment of one percentage point of Centrality would

reduce Encounter Rates by 26 percentage points. The model seems to better explain Piracy than Encounter Rates although the results of both estimations are characterised by the low level of significance of coefficients. This might be driven by the low number of observations available for both outcome variables, and the narrow overlap of countries in the different datasets of the variables – a different set of countries have data on Piracy than have data on Encounter Rates.

Columns (3), (4), and (5) estimate the impact of CCS on the vitality of ICT usage in three sectors: individual Internet users, private sector, and 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 (NRI: Business Usage) is an index number 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 mute. Wealth has a positive impact on the vitality of ICT usage by the private sector; ceteris paribus, a 1 percent 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 (6) show that the model explains 67 percent 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 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. As number of users is highly correlated to population, this result could be related to the difficulty of individual impact on the political outcomes of larger countries. For example, consider the country with the highest number of Internet users (18.65 corresponds to 125,500,000 users approximately).

Ceteris paribus, a 1 percent increment in the number of users of this country would reduce Voice and Accountability by 0.17 units of a normal standard deviation. The sign of the coefficient of Centrality moves in the same negative direction, although it is not significant.

Table 7. OLS regressions to explain cybersecurity outcomes. Robust standard errors in parentheses. Symbols ***, **, *, + indicate, correspondingly, levels of significance <0.001, <0.01, <0.05, and <0.1.

	Piracy (1)	Encounter Rates (2)	NRI: Individual Usage (3)	NRI: Business Usage (4)	NRI: Government Usage (5)	Voice and Account. (6)
CCS	-18.02**	-5.04	0.61**	0.60*	0.69**	0.56**
	(6.54)	(4.84)	(0.19)	(0.28)	(0.26)	(0.18)
Scale	-0.21	1.82+	-0.03	-0.03	0.02	-0.17***
	(1.03)	(0.97)	(0.04)	(0.04)	(0.05)	(0.03)
Centrality	0.04	-0.26*	0.03***	-0.01*	0.00	-0.01+
	(0.12)	(0.13)	(0.01)	(0.01)	(0.01)	(0.00)
Wealth	-6.26+	3.09	0.24+	0.37**	0.04	0.31***
	(3.60)	(3.35)	(0.13)	(0.13)	(0.15)	(0.08)
Constant	159.59***	-8.65	-0.50	0.58	1.73	-0.57
	(31.16)	(28.19)	(0.95)	(0.88)	(1.15)	(0.78)
N	40	41	58	58	58	73
R^2	0.76	0.42	0.88	0.53	0.39	0.67

These results are consistent with the linear estimations and with the results in Dutton et al. (2019).

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 a number of steps to check goodness of fit and overall validity of measures (Fornell & Larcker, 1981).

The model was tested using four different outcomes to better understand the impact of cybersecurity capacity on: piracy; encountering malware and viruses; use by business and government; and the confidence to participate in online forums (voice).

Discriminant Validity

Validity measures were run on all the models to check discriminant validity, collinearity (VIF) and goodness of fit measures. Most of the constructs were single item measures, so

construct reliability was not an issue. The one construct, Outcomes: Use Factors, consisted of three variables with a Cronbach's alpha of .840 and the loadings are in Table 8.

Table 8: 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<.001

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 & Bentler,1999). Table 9 is the results of the SSMR goodness of fit measures.

Table 9: All Models Goodness of Fit Measures

Model Fit Measures SSMR	Saturated Model	Estimated Model
SSMR Piracy	0.000	0.048
SSMR MS Encounter Rate	0.000	0.051
SSMR Use	0.059	0.098
SSMR Voice	0.000	0.026

Given the size of the sample and the kurtosis of one item in the Use model, the goodness of fit measures indicates the models are acceptable.

Collinearity

SEM and path analysis are founded on regression analysis, where the goal is to isolate the relationship between the independent variable and the dependent variable. Variance inflation factors (VIF) help measure collinearity. 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. We tested out models for both outer and inner VIF measures.

Table: 11 VIF measures

Inner VIF Factors	Outcomes: Piracy	Outcomes: ER	Outcomes: Use	Outcomes: Voice
Centrality /Cybersecurity Capacity Scale	3.641	3.867	4.010	4.010
Centrality /Outcomes	3.801	3.985	4.103	4.103

Cybersecurity/Capacity Scale/Outcomes	4.314	4.500	3.158	3.158
Scale / Cybersecurity Capacity Scale	1.048	1.053	1.035	1.035
Scale /Outcomes	1.357	1.302	1.727	1.727
Size/ Scale	1.082	1.118	1.069	1.069
Wealth/ Centrality	1.000	1.000	1.000	1.000
Wealth/ Cybersecurity Capacity Scale	3.559	3.765	3.969	3.969
Wealth/ Outcomes	5.611	6.228	4.799	1.069
Wealth/ Scale	1.082	1.118	1.069	4.799

Outer VIF Factors	**Outcomes: Piracy**	**Outcomes: ER**	**Outcomes: Use**	**Outcomes: Voice**
Centrality (% users)	1.000	1.000	1.000	1.000
Cybersecurity Capacity Scale (csc avr)	1.000	1.000	1.000	1.000
Scale (users)	1.000	1.000	1.000	1.000
Size (population)	1.000	1.000	1.000	1.000
Wealth (GDP pc)	1.000	1.000	1.000	1.000
Piracy	1.000	*	*	*
ER (MS encounter rate)	*	1.000	*	*
Use (nri business use)	*	*	2.202	*
Use (nri gov use)	*	*	1.851	*
Use (nri individual use)	*	*	1.994	*
Voice	*	*	*	1.000

* not applicable

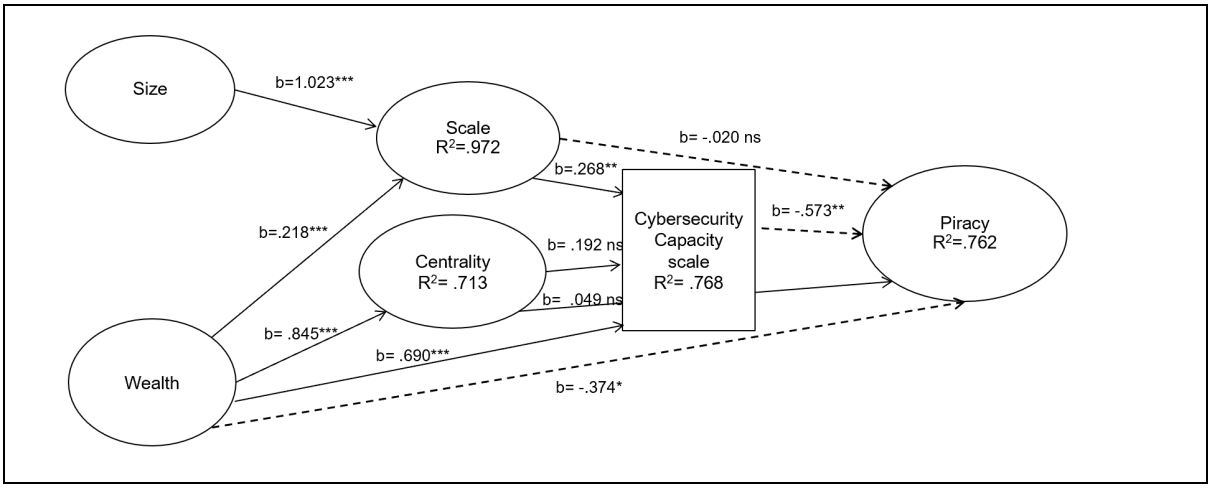
All the relationships but two in all the models were well within the acceptable measures for VIF. The two items of concern, Wealth→Piracy (5.611) and Wealth→Outcome: ER (6.228) were low enough to be acceptable, especially since the rest of the items in each model had low VIF level.

Shaping Piracy

CCS has a direct and independent negative impact on Piracy, controlling for other variables in the path model. Scale has no direct relationship with Piracy, but it does have a strong positive effect on Size, which in turn, has a positive and significant impact on CCS. Larger countries, with a larger Size, have the scale to have greater support for CCS. Wealth is also positively related to Size, but has even stronger relationships with Centrality, and the CCS. Other things equal, Wealth actually has a positive relationship with Piracy, but this is counterbalanced by its positive impact on CCS that mitigates Piracy. Generally, the path results described in Figure 3 support the results of the regression analyses and the

theoretical model for this study. CCS is likely to diminish Piracy, which in turn, should support better user experiences.

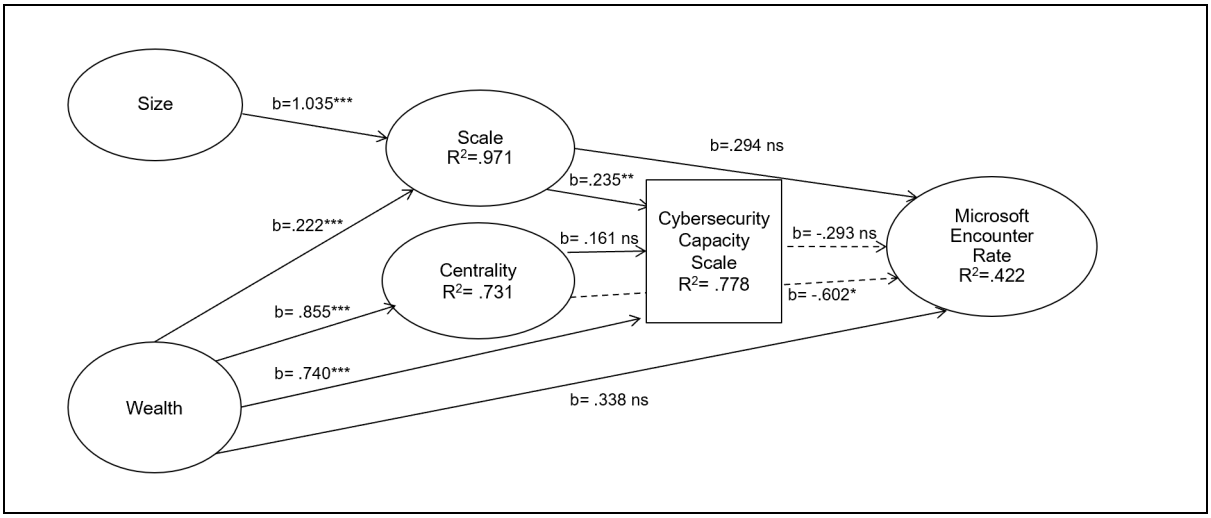
Figure 3. Cybersecurity Capacity and Impact on Piracy



Path Results for Encounter Rates

The path analysis of Encounter Rates squares with the regression analyses, showing a negative but nonsignificant relationship with CCS (Figure 4). The major factors shaping Encounter Rates tends to be Wealth and the percentage of the population using the Internet – Centrality. Both Wealth and Centrality are likely to make these nations more important targets of malicious users. While the statistical relationship between CCS and Encounter Rates is not significant, it is negative, and the very fact that individuals and institutions have licensed software is in some respects an indication of having built a higher cybersecurity capacity. In other words, it is very likely these countries would suffer more attacks if they had lower levels of licensed software.

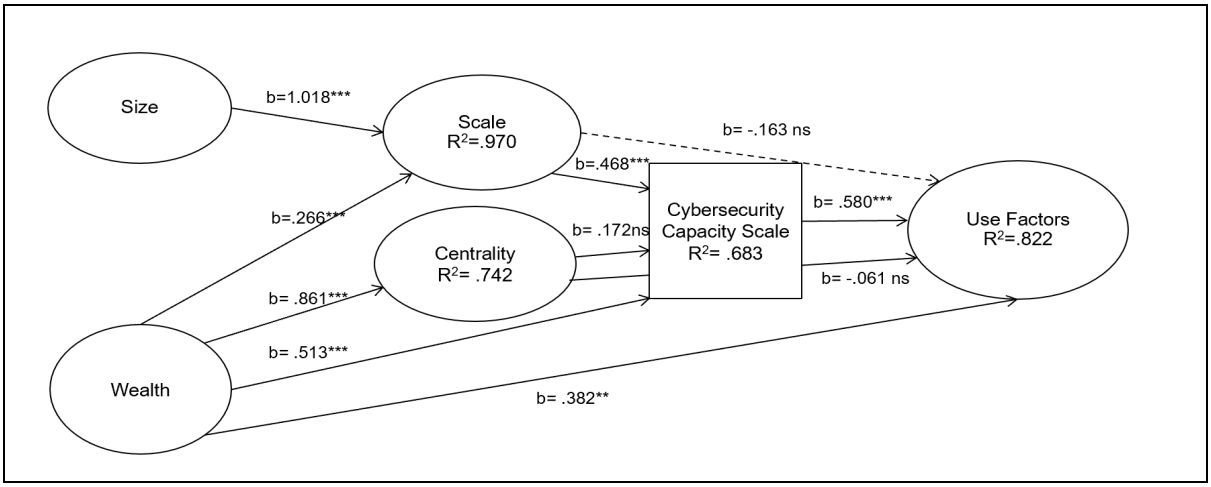
Figure 4. Cybersecurity Capacity and Impact on Encounter Rates



Path Analysis of Internet Use

Internet use in households, private industry and government are all positively shaped by higher levels of CCS. There is a strong, positive relationships between CCS and the Use Factors (Figure 5). 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 is negatively related to the Use Factors (Figure 5). This might indicate the great importance of CSC in nations where the Internet is used at a greater scale and is more central.

Figure 5. Cybersecurity Capacity and Impact on ICT Use Factors



Path Analysis of Voice and Accountability

Conventional wisdom often links higher levels of security with lower levels of freedom of expression, transparency and accountability. However, central aspects of the CMM define law and policy with respect to freedom of expression and other human rights as critical to building cybersecurity capacity. As Figure 6 shows, there is in fact a strong positive association between CCS and cross-national indicators of Voice and Accountability, even when controlling for all the other variables in the model. As with respect to the vitality of use, Voice is also related directly with the Wealth of the country, but when controlling for other variables, there is a negative relationship between the scale of Internet use and Voice. This is also the case of the centrality of use, but the relationship between Centrality and Voice is not statistically significant.

Figure 6. Cybersecurity Capacity and Impact on Voice and Accountability

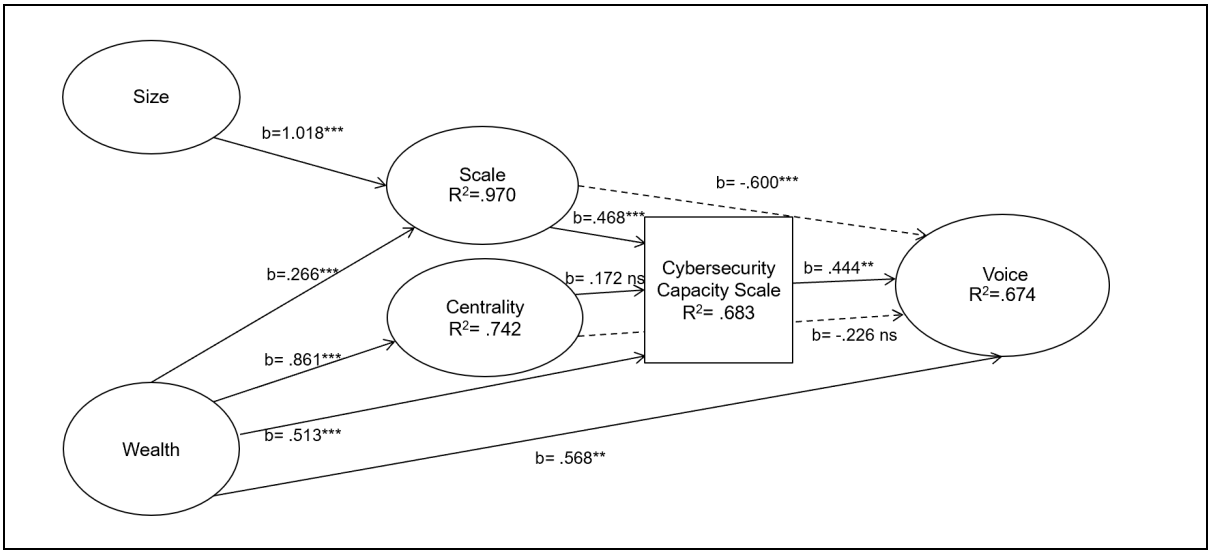
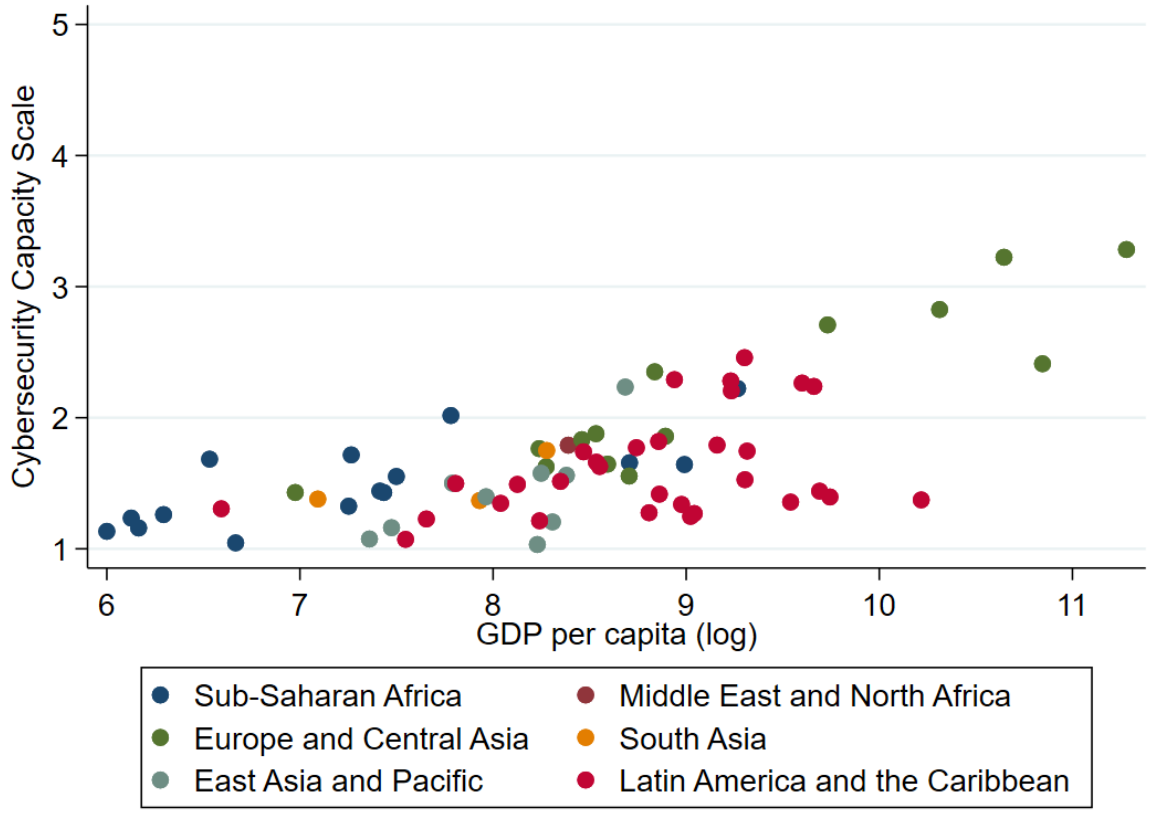


Table 12: Total Effects	Outcome: Piracy		Outcome: ER		Outcome: Use		Outcome: Voice	
	Mean	(SD)	Mean	(SD)	Mean	(SD)	Mean	(SD)
Centrality -> Cybersecurity Capacity Scale	.192	(.137)	.161	(.133)	.172	(.113)	.172	(.114)
Centrality -> Outcomes	-.062	(.159)	-.649	(.254)*	.039	(.121)	-.150	(.128)
Cybersecurity Capacity Scale -> Outcomes	-.573	(.208)**	-.293	(.311)	.580	(.129)***	.444	(.144)**
Scale -> Cybersecurity Capacity Scale	.268	(.090)**	.235	(.086)**	.468	(.076)***	.468	(.074)***
Scale -> Outcomes	-.173	(.098)	.225	(.130)**	.108	(.076)	-.392	(.083)***
Size -> Cybersecurity Capacity Scale	.274	(.094)**	.243	(.090)**	.476	(.081)***	.476	(.080)***
Size -> Outcomes	-.177	(.100)	.233	(.135)	.110	(.078)	1.018	(.028)***
Size -> Scale	1.023	(.037)***	1.035	(.037)***	1.018	(.028)***	-.399	(.085)***
Wealth -> Centrality	.845	(.045)***	.855	(.042)***	.861	(.036)***	.861	(.036)***
Wealth -> Cybersecurity Capacity Scale	.911	(.067)***	.930	(.064)***	.785	(.055)***	.785	(.055)***
Wealth -> Outcomes	-.859	(.085)***	-.383	(.149)***	.741	(.059)***	.266	(.042)***
Wealth -> Scale	.218	(.039)***	.222	(.037)***	.266	(.042)***	.563	(.101)***

* p<.05, **p<.01, ***p<.001

The significance of GDP Per Capita is one strong theme of the analyses. It is an important determinant of CCS, but also of the various outcome indicators. Figure 7 shows the simple relationship between Wealth, as measured by GDP Per Capita, and CCS. The figure shows both the relatively low levels of maturity across all nations, as discussed above, but also the clear relationship of CCS with Wealth. In essence, the analyses indicate that there is a digital divide in access to cybersecurity capacity. Wealthier nations are not only like to have higher levels of capacity, measured by CCS, but independent of all other factors, the positive outcomes of the Internet are associated with the wealth of the nation.

Figure 7. Scatter plot relating variables CCS and GDP per capita



Conclusions and Discussion

Governments and international organizations 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 multi-dimensional 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 described the multiple dimensions of cybersecurity capacity building and analyzed whether capacity building had an independent effect on the experiences of end users. This allows our study to take a 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 four-fold.

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 could be called a start-up or formative stage. This is critical in that it demonstrates the need for initiatives to raise capacity, particularly in light of our findings on its impact.

Secondly, we found that capacity building does matter. Controlling for antecedent variables that might provide alternative explanations for user experiences, such as the wealth of nations, cybersecurity capacity building had a strong, statistically significant, and positive effect on user experiences. In the case of only one of dependent variables, encounter rates, was the relationship not statistically significant in part due to the lack of data on encounter rates for many nations in our sample. Nevertheless, the relationship was in the right direction – capacity building reducing encounter rates – and the remaining dependent variables demonstrated strong relationships in the hypothesized direction.

Our earlier research found that nations with a greater level of capacity building were more likely to create a better experience for Internet users, such as fewer problems with malware (Dutton et al 2019). With more specific and direct empirical indicators of capacity building, we can validate this finding: greater levels of maturity translate into better experiences for users. This was supported by multivariate analyses using simple linear regressions and more complete path modeling of all the variables in our theoretical model. The patterns of relationships paint a clear case for the importance of capacity building.

However, the findings also point out the significance of other national variations, particularly with the wealth of nations. Put simply, we find a cybersecurity capacity divide between the low- and higher-income nations. Wealth reaps more beneficial outcomes of the Internet but also supports capacity building, providing direct and indirect support for the vitality of the

Internet in the wealthier nations. While this is purely descriptive of existing relationships, it does lend support to international efforts to support cybersecurity capacity building. Local outcomes are not immune to global problems in security, and all nations can be jeopardized by any diminished capacity in some nations.

The results of this study reinforce the case that more initiatives are needed to bolster cybersecurity capacity across the world. In addition, there must be more attention to decreasing the cyber-capacity divides between low-, medium- and high-income nations.

References

Almuhammadi, S., and Alsaleh, M. (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

Baram, G., Paikowsky, D., Pavel, T., Ben-Israel, I. (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

Cameron AC. And Trivedi PK. "Microeconometrics Using Stata. Revised Edition". Texas: Stata Press (2010).

Cohen, D. (2017), 'The British Response to Threats in Cyberspace', *Cyber, Intelligence, and Security*, 1(3), December: 19-36.

Clark, D., Berson, T., Lin, H. S. (2014) (eds), Computer Science and Telecommunications Board, *At the Nexus of Cybersecurity and Public Policy*. Washington D.C.: The National Academy Press.

Craney, T. A., & Surles, J. G. (2002). Model-dependent variance inflation factor cutoff values. *Quality Engineering*, *14*(3), 391-403.

Dijkstra, T.K., Henseler, J. "Constistent Partial Least Squares Path Modeling." MIS Quarterly. 39 (2015),2, pp 297-316.

Duncan, O. D. (1966). Path analysis: Sociological examples. American journal of Sociology, 72(1), 1-16.

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

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics.

Henseler, J., Hubona, G., Ray, P. A. “Usuing PLS Path Modeling in New Technology Research: Updated Guidelines.” Industrial Management & Data Systems, 116, 1, pp 2-20. ISSN: 0263-5577

GCSCC (2016), Global Cyber Security Capacity Centre, “Cybersecurity Capacity Maturity Model for Nations (CMM). Revised Edition.” Available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf (11 November 2019, last accessed).

GCSCC (2019), Global Cyber Security Capacity Centre, Global Impact Knowledge and Policy Contributions from the First Five Years’, available online at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/GCSCC%20booklet%20WEB.pdf

Hathaway, M. (2013), Cyber Readiness Index 1.0. Belfer Center for Science and International Affairs, Harvard Kennedy School, November. https://www.belfercenter.org/publication/cyber-readiness-index-10

Hu, L.T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Inter-American Development Bank and Organization of American States (IDB and OAS). “Cybersecurity. Are we ready in Latin America and the Caribbean? Cybersecurity Report 2016.” (2016). Available at https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean (25 June 2019, last accessed).

International Telecommunication Union (ITU). “Global Cybersecurity Index”. (2019). Available at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (13 June 2019, last accessed).

ITU-T (2008), International Telecommunication Union Telecommunication Standardization Sector, Series X: Data Networks, Open System Communications and Security: Telecommunication Security: Recommendation ITU-T X.1205.

Kaufmann D., Kraay A., and Mastruzzi M. “The Worldwide Governance Indicators: Methodology and Analytical Issues.” World Bank Policy Research Working Paper No. 5430 (2010).

Kenny, D. (2015). Measuring Model Fit. http://www.davidakenny.net/cm/fit.htm (11 May, 2020, last accessed).

Knodel J. The Design and Analysis of Focus Group Studies: A Practical Approach; chapter 3 in Morgan D.L., “Successful Focus Groups: Advancing the State of the Art”. Newbury Park: SAGE Publications, Inc. (1993).

Krueger R.A., and Casey M.A. “Focus Groups: A Practical Guide for Applied Research”. India: SAGE Publications Asia-Pacific Pte. Ltd. (2015).

Microsoft. “Microsoft Security Intelligence Report”. Volume 20 (2015). Available at https://www.microsoft.com/en-us/security/operations/security-intelligence-report (23 May 2019, last accessed).

Microsoft. “Microsoft Security Intelligence Report”. Volume 21 (2016). Available at https://www.microsoft.com/en-us/security/operations/security-intelligence-report (23 May 2019, last accessed).

Microsoft. “Microsoft Security Intelligence Report”. Volume 22 (2017). Available at https://www.microsoft.com/en-us/security/operations/security-intelligence-report (23 May 2019, last accessed).

Rosenzweig, P. (2019), ‘Preliminary Observations on the Utility of Measuring Cybersecurity’, *Lawfare*, August 6. https://www.lawfareblog.com/preliminary-observations-utility-measuring-cybersecurity

Shoqata për Teknologji të Informacionit dhe të Komunikimit të Kosovës and Kantar Index Kosova (STIKK and KANTAR). “Internet Penetration and Usage in Kosovo.” (2019). Available at https://stikk.org/wp-content/uploads/2019/11/STIKK_IK_Report_Internet_Penetration_V3-final-1.pdf, (26 March 2020, last accessed).

Spidalieri, F. (2015), State of the States on Cybersecurity. Newport, RI: Salve Regina University, Pell Center for International Relations and Public Policy.

Vaidya, R. (2018), Department of Digital, Culture, Media & Sport, Ipsos MORI, and University of Portsmouth, *Cyber Security Breaches Survey 2018*. London: DCMS.

Ware, W. (1970), Head of Task Force on Computer Security, Defense Science Board, Security Controls for Computer Systems (U), Washington D.C.: Office of the Director of Defnse Research and Engineering, 11 February.

Williams M. “Making Sense of Social Research”. London: SAGE Publications Ltd (2003).

World Bank (WB). “TCdata360”. (2019a). Available at https://tcdata360.worldbank.org/ (6 August 2019, last accessed).

World Bank (WB). “World Bank Country and Lending Groups.” (2019b). Available at https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups (22 August 2019, last accessed).

World Bank (WB). “World Development Indicators”. (2020a). Available at https://datacatalog.worldbank.org/dataset/world-development-indicators (19 March 2020, last accessed).

World Bank (WB). “Worldwide Governance Indicators.” (2020b). Available at https://datacatalog.worldbank.org/dataset/worldwide-governance-indicators (26 March 2020, last accessed).

World Economic Forum (WEF). “Networked Readiness Index”. (2019). Available at http://reports.weforum.org/global-information-technology-report-2016/networked-readiness-index/ (13 June 2019, last accessed).

Appendix

Fornell-Larcker Criterion: Piracy Outcome

	Centrality	CCS	Outcomes	Scale	Size	Wealth
Centrality	1.000					
Cybersecurity Capacity Scale	0.731	1.000				
Outcomes	-0.683	-0.854	1.000			
Scale	-0.163	0.192	-0.114	1.000		
Size	-0.415	-0.006	0.062	0.963	1.000	
Wealth	0.845	0.835	-0.811	-0.064	-0.275	1.000

Fornell-Larcker Criterion: Microsoft Malware Encounter Rate Outcome

	Centrality	CCS	Outcomes	Scale	Size	Wealth
Centrality	1.000					
Cybersecurity Capacity	0.747	1.000				
Outcomes	-0.589	-0.420	1.000			
Scale	-0.198	0.119	0.339	1.000		
Size	-0.448	-0.082	0.460	0.963	1.000	
Wealth	0.855	0.851	-0.459	-0.114	-0.325	1.000

Fornell-Larcker Criterion Use Outcome

	Centrality	CCS	Outcomes	Scale	Size	Wealth
Centrality	1.000					
Cybersecurity Capacity Scale	0.661	1.000				
Outcomes	0.726	0.816	0.805			
Scale	0.101	0.490	0.135	1.000		
Size	-0.192	0.305	-0.057	0.951	1.000	
Wealth	0.861	0.665	0.816	0.008	-0.253	1.000

Fornell-Larcker Criterion Voice Outcome

	Centrality	CCS	Scale	Outcomes	Size	Wealth
Centrality	1.000					
Cybersecurity Capacity Scale	0.661	1.000				
Scale	0.101	0.490	1.000			
Outcomes	0.496	0.379	-0.401	1.000		
Size	-0.192	0.305	0.951	-0.532	1.000	
Wealth	0.861	0.665	0.008	0.664	-0.253	1.000