



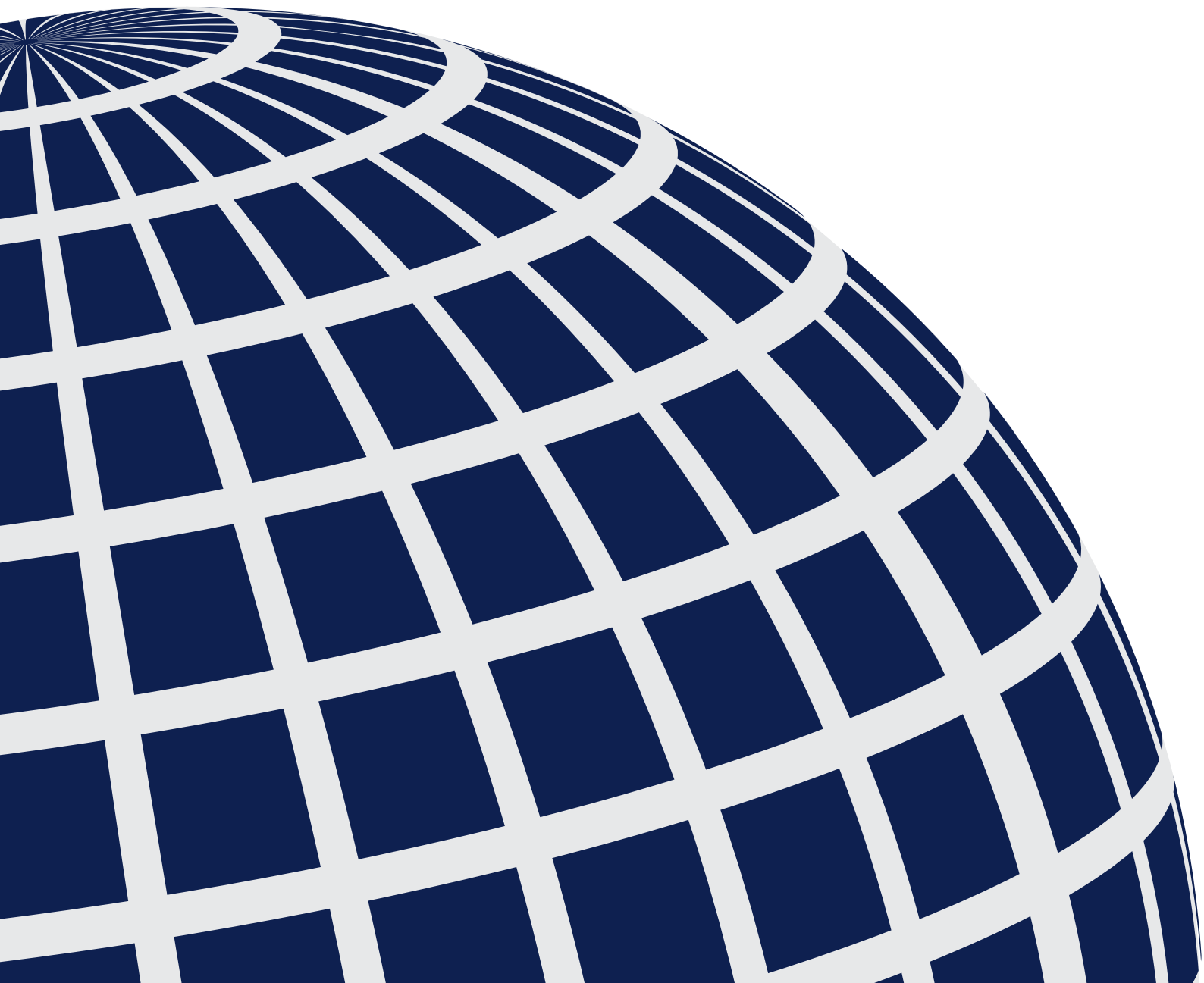
Global  
Cyber Security  
Capacity Centre

OXFORD  
MARTIN  
SCHOOL



# GLOBAL IMPACT

KNOWLEDGE AND POLICY  
CONTRIBUTIONS FROM  
THE FIRST FIVE YEARS





## UNDERSTANDING THE COMPLEXITIES OF CYBERSECURITY CAPACITY

In 2013 Oxford academics in collaboration with academics from UCL, Exeter and Royal Holloway Universities, established the Global Cyber Security Capacity Centre (GCSCC) with the mission to research what constitutes cybersecurity capacity for a nation and the nature of effective capacity-building practice. At that point in time indexes and metrics were being used to determine the presence of capacity in nations, however, they were not designed to take account of evolving knowledge and practice, nor could they consider the ability to respond and grow capacity in the face of a changing environment – be it due to trends in technology use, socio-political climate, or evolution of the threat.

We created the GCSCC and its research programme to initially develop an evidence-based Cybersecurity Capacity Maturity Model for Nations (CMM) that addresses these knowledge requirements, that could be used to underpin strategic investment decisions, and in so doing to help accelerate and optimise cybersecurity capacity-building efforts around the world. A key requirement being that the model took account of both the breadth and depth of what national cybersecurity capacity consists of, what it means to be effective at delivery, the wide spectrum of knowledge and practice, and of the interdependencies that exist between the factors that make up national cybersecurity capacity.

This mission has never been more important. The world's economies continue to develop with ever-increasing dependence on technology. If we do not ensure that cybersecurity capacity exists across the entirety of cyberspace, we will inevitably develop cyber ghettos, places where harm is prevalent and where attacks can be successfully deployed, and also from where they can be easily launched. Ultimately, a lack of progress on cybersecurity capacity could result in harms to the prosperity and the well-being of those economies and nations so dependent on cyberspace – increasingly the vast majority of humanity.

The GCSCC has been a collaborative initiative from its inception. Across Oxford University alone, our work has involved the Department of Computer Science, the Oxford Internet Institute, Saïd Business School, Law and Sociology, and the Blavatnik School of Government. The contributions received from academics around the world mirror and extend this breadth of disciplines. Additionally, our research has been inherently a multi-stakeholder process; contributions have been made by experts from industry, governments, civil society and international capacity-building organisations around the world.

The GCSCC's view of what constitutes cybersecurity capacity for a nation is broad, spanning policy, strategy, societal culture, education and training, law and regulation, and cybersecurity technologies and standards. At the time of its inception, the CMM constituted a working hypothesis that was also the broadest of all models and indices then in existence. During the past five years, substantial progress has been made: at the time of writing the CMM has been deployed nearly 100 times across more than 60 countries around the world; and the foundations of a new and complementary Cyber Harm Framework (CHF) have been laid. We have refined the CMM once, based on our learnings in the field, and will continue to do so in close collaboration with the research and practitioner communities. In recognition of the large number of contributors, we openly publish the CMM for the benefit of all.

The following document provides an opportunity to formally acknowledge the progress and efforts of all those involved in the GCSCC's research, while also demonstrating the GCSCC's broad reach, and the positive impact of its activities. We thank those who have contributed and who will do so in the future.

**Professor Sadie Creese**  
*Founding Director, Global Cyber Security Capacity Centre, University of Oxford*

“The Foreign & Commonwealth Office (FCO) provided the seed funding for the creation of the Global Cyber Security Capacity Centre and the development of the Capacity Maturity Model, which have become globally recognised resources for international cybersecurity capacity development. We are pleased that more than 60 countries, including the UK itself, have used the model to better understand national strengths and areas for improvement in cybersecurity capacity. The increasing use of the CMM around the world has allowed us to make it a central part of our international capacity-building programme. The FCO appreciates the support that many other institutions and individuals have put behind these efforts and we look forward to continuing our partnership with them and with Oxford.”

*Dr Alexander Evans,  
Director, Cyber, Foreign  
& Commonwealth Office*

## WHAT MADE IT ALL POSSIBLE?

“The OAS has been collaborating with the GCSCC over the past few years on strengthening cybersecurity capacities across the Americas, including the use and implementation of the CMM. The model has helped the OAS and its Member States to have a better understanding of the capacities and needs of our region. As a trusted partner and member of the Expert Advisory Panel, we believe that these five years are only the beginning of great work, and we look forward to continue working with Oxford in enhancing safety and security in cyberspace and contributing to the development of tools that will benefit the global cyber community.”

Belisario Contreras, Manager, Cybersecurity Program, Organization of American States, and Member of GCSCC Expert Advisory Panel

The research of the GCSCC is aimed at generating knowledge which can inform governments and the international community to adopt policies and make investments that have the potential to significantly enhance safety and security in cyberspace. Since its foundation in 2013, the Centre has worked towards this goal by collaborating with actors at all levels, from individuals to nation states, across all sectors and all regions. The research followed a multistakeholder process.

### Governance

The Centre's holistic approach to cybersecurity capacity assessment is driven by a diverse team of researchers and practitioners representing regions from all across the world and drawn from a diverse range of technical and policy backgrounds.

The technical direction for the GCSCC is set by its Technical Board, which comprises the Director, professors and senior thought-leaders who together cover the breadth of cybersecurity-related disciplines and practice. The Expert Advisory Panel provides thought-leadership to support the Centre's goals. Panel members represent global and diverse stakeholder groups and provide invaluable guidance and expertise across a range of strategic, technical and governance challenges and opportunities.

### Working Groups

In the early years the GCSCC's working groups provided thought-leadership to support its goals. These groups were strategically constituted to represent the five dimensions of the CMM, so that the GCSCC's research outputs reflected the expertise of the global community. Once we had refined the CMM post-pilot phase, we transitioned away from working groups focused on specific dimensions and formed a single Expert Advisory Panel spanning the spread of the CMM.

### Research Sponsors

The establishment, reach and impact of the GCSCC have been made possible by the support of the Centre's research sponsors. This investment has accelerated the GCSCC's research, both theoretical and applied. It has also empowered its global

engagement through initiatives such as the Cybersecurity Capacity Portal. Investments have included seed and continued core project funding from the UK Foreign & Commonwealth Office, the Foreign Ministry of the Netherlands, the Norwegian Ministry of Foreign Affairs, and the State Government of Victoria, Australia.

### Strategic Partners

Critical to the success and impact of the GCSCC's portfolio of work has been the engagement of a number of capacity-building partners that have directly supported the development and deployment of the CMM across the world. These strategic partnerships have allowed the project to reach over 100 deployments (including reiterations) in the first five years of operations; and, in addition, have helped to inform the prioritisation and development of cybersecurity around the world. The collaboration with the World Bank, Organization of American States (OAS), Oceania Cyber Security Centre (OCSC), the International Telecommunication Union (ITU), and the Commonwealth Telecommunications Organisation (CTO) has assisted the GCSCC to test and ultimately consider the results of the application of the CMM, positively impacting cybersecurity capacity around the world.

### Implementation Partners

In order to ensure that all nations around the world have access to the expertise required to complete a CMM assessment, the GCSCC works with a number of implementation partners that function as force multipliers. They help to expand



the reach of the project and utilise their own extensive expertise to support the cybersecurity capacity building work. To date the GCSCC has worked with NRD Cyber Security, and the Norwegian Institute of International Affairs (NUPI), and continues to create new partnerships as opportunities arise.

### Research Across Disciplines At Oxford

The GCSCC is led by academics from across Oxford and since inception members of the Technical Board have been drawn from the Department of Computer Science, the Oxford Internet Institute, Saïd Business School, the Blavatnik School of Government and the Department of Sociology.

The Department of Computer Science is one of the longest-established computer science departments in the UK and offers research activities encompassing core computer science as well as computational biology, quantum computing, computational linguistics, information systems, software verification and software engineering.

The Oxford Internet Institute (OII) is a multidisciplinary research and teaching department dedicated to the social science of the Internet.

Saïd Business School (SBS) is a young, vibrant and entrepreneurial school that delivers cutting-edge education and ground-breaking research known to transform individuals, organisations, business practice and society. In addition to professional leadership from SBS, the GCSCC has worked closely with the school in the development and implementation of the Cybersecurity Capacity Portal.

The Blavatnik School of Government is one of the University of Oxford's newest and most vibrant departments, combining the academic rigour of the top-ranked university in the world with an applied, real-world focus. The school draws on the full range of Oxford University's expertise,

from science, computing and medicine to humanities and social science.

The Department of Sociology was established in 1999 to provide a renewed focus for sociological research and teaching in the University. Sociology at Oxford has a strong analytical, empirical and comparative orientation. Focus is on developing and testing theories that engage with real world problems. Particular strengths include the statistical analysis of social surveys, social demography, collection, management and analysis of complex datasets, the development of rational choice theory, microsocial experiments and simulation studies.

### Regional Constellation Network

In 2017 the GCSCC started to build a Constellation Network of Regional Centres that will accelerate and guide its global coverage and provide contextualised knowledge and application of the CMM within their respective regions. The regional network will seek to provide locally informed approaches to analysing cybersecurity capacity, generating recommendations for next steps in advancing cybersecurity capacity of countries in the region and contributing to a better understanding of the regional cybersecurity capacity. Regional centres will also help to further the development of the CMM and the complementary Cyber Harm Framework (CHF) and to establish cybersecurity capacity as a research discipline in the region.

The first of these partners is the Oceania Cyber Security Centre (OCSC) based in Melbourne, Australia, covering the Australia-Pacific region. In addition to the OCSC, the Centre is also currently building more partnerships to expand the network in the near future.

“The introduction of new undersea cables and mobile networks currently induces fast digitisation for nations in the Pacific region. Thus, maturity of cybersecurity capacity on many levels is becoming essential. The Oceania Cyber Security Centre (OCSC) in Melbourne and the GCSCC have engaged in a three-year collaboration on supporting nations in the Pacific region via CMM reviews. The target is to deploy the CMM in 15 countries in the Pacific region.

In 2018 CMM reviews were successfully completed for Tonga and Samoa. OCSC and GCSCC researchers visited the two countries as part of joint missions with ITU and the Asia-Pacific Network Information Centre. These first activities have created significant interest in the region. The project was presented in 2018 at the United Nations Development Programme conference ‘Together for a Digital Pacific’ in Apia, at the Asia-Pacific Telecommunity (APT) Symposium on Cybersecurity in Seoul and at the Asia Foundation Cybersecurity Expert Exchange in Port Moresby, as well as at the APT Policy and Regulation Forum in Apia. Furthermore, OCSC and GCSCC jointly organised a cybersecurity workshop at the 2018 Asia Pacific Regional Internet Governance Forum in Vanuatu.”

Associate Professor Carsten Rudolph, Director, Oceania Cyber Security Centre, Australia



## THE MODEL

*Six countries formed part of the CMM Review pilot programme: Jamaica, Colombia, Armenia, Bhutan, Kosovo and Montenegro.*

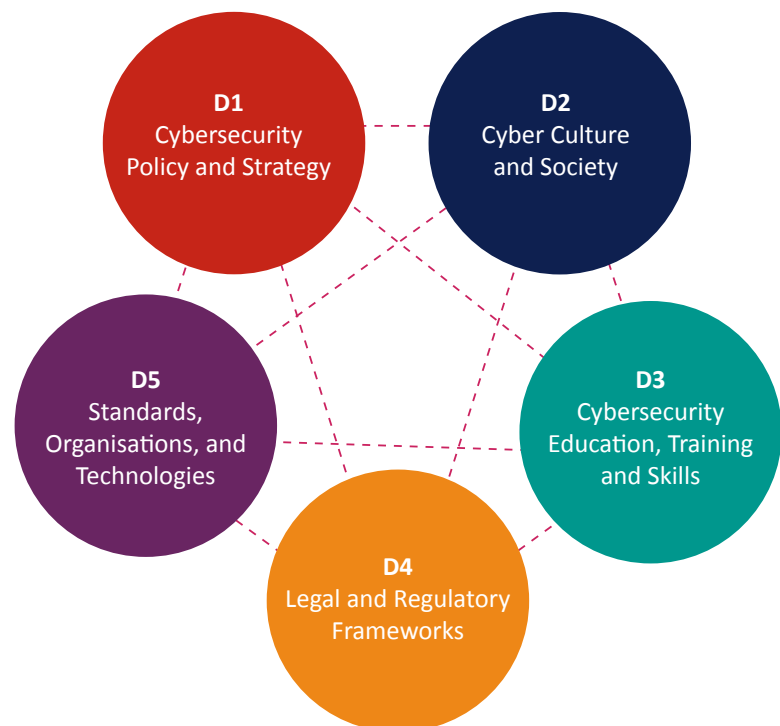
“The World Bank is a long-time strategic partner of the GCSCC, supporting the deployment of the CMM in its pilot phase, and has recently become further engaged through the Centre in the training and engagement of World Bank staff in the deployment of the CMM. The most recent collaborations between the organisations have included a Cyber Security Capacity programme funded by the government of Korea aimed at assessing Albania, Bosnia and Herzegovina, Ghana, Kyrgyz Republic, FYR Macedonia and Myanmar. Such collaborations between the institutions have created greater efficiencies in the global cybersecurity capacity-building community and helped to inform World Bank digital development investments.”

*Sandra Sargent,  
Senior Operations  
Officer, World Bank*

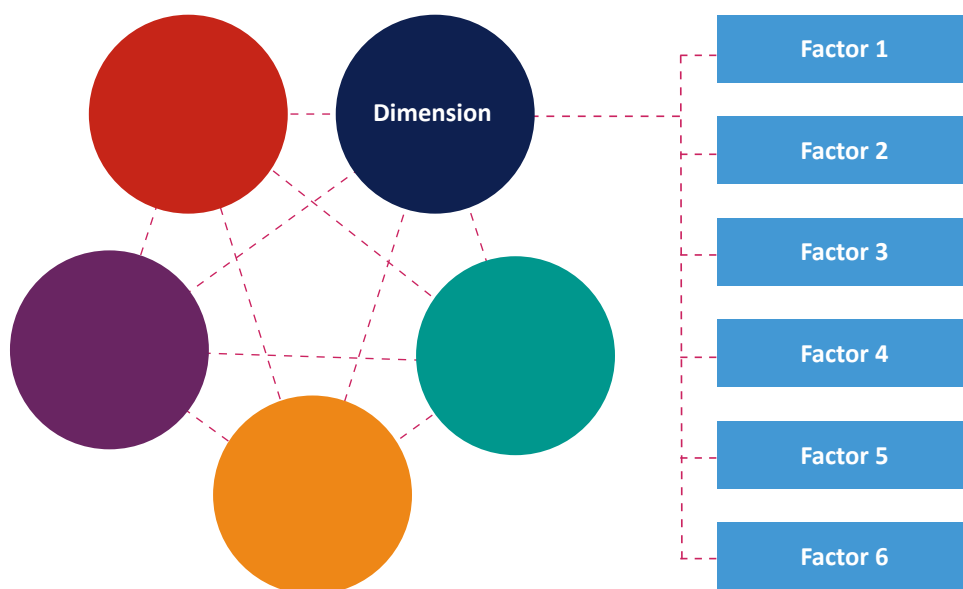
In 2014, the Centre undertook a global collaborative exercise to develop the first iteration of the Cybersecurity Capacity Maturity Model for Nations (CMM), working alongside experts from academia, international and regional organisations and the private sector. The goal was to extract and synthesise the community’s knowledge, identifying the most important factors for a nation’s cybersecurity capacity and the steps necessary for the nation to reach consequent levels of maturity. This process was seeded in an open vision that at least five dimensions should be considered. These dimensions and the factors that constitute them were subsequently refined using thematic-coding analysis, focus groups data and the results of a broad survey of literature.

In 2015 the structure of the CMM was complemented with a deployment methodology and the subsequent piloting of the CMM in six countries across the world. The results gathered from this initial phase of deployment served to revise the first iteration of the model, which also enjoyed support and input from the Capacity Centre’s Technical Board and Expert Advisory Panel. The discussions led to the refinement of existing factors, identified new factors and culminated with the publication of a revision of the CMM in February 2017.

### THE FIVE DIMENSIONS OF THE CMM

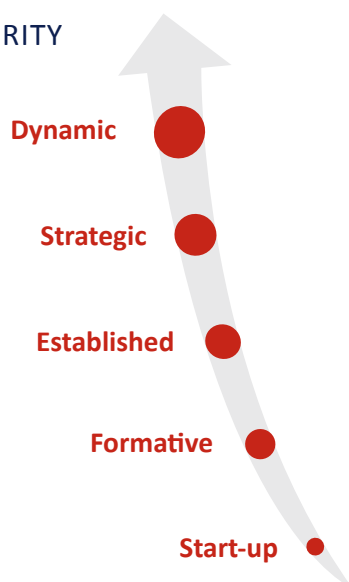


These five dimensions cover the broad expanse of areas that define cybersecurity capacity. Within each dimension there are several factors, each of which presents a number of aspects, each grouping together related indicators of cybersecurity capacity. Those indicators constitute the evidence that the CMM prescribes must be observable for a nation to attain any particular stage of maturity.



The five stages of maturity, illustrated below, range from *start-up* stage to *dynamic* stage. The start-up stage implies an ad-hoc or nonexistent approach to capacity, whereas the dynamic stage represents not only a strategic approach but also the ability of a country to adapt to changing environmental factors. Being in a particular stage means that a country is at a specific level of maturity in cybersecurity capacity. The CMM review ultimately determines which of the five stages of maturity the country has reached and informs the country to allow it to decide potential actions to achieve the next stage (or stages) of maturity. The intention is that the review based on the CMM could be used to build business cases for investment and corresponding expected national cybersecurity performance enhancements. The results of the CMM review are incorporated into a report owned by the country in question.

## STAGES OF MATURITY



“NRD Cyber Security sees a great value in the CMM in assisting nations to assess their cybersecurity capacities in a systematic and research-based way. The model stands out due to the involvement and close interaction of all national cybersecurity stakeholders, which serves as a capacity-building exercise in itself. NRD Cyber Security’s experience of working with many countries around the world shows that the existence of legal and regulatory frameworks for cybersecurity does not necessarily mean that they are implemented, and that cybersecurity capacity exists. We are particularly happy to become a partner of the GCSCC in helping nations to understand their cybersecurity capacities and promote a secure digital environment for the well-being and prosperity of all.”

Akvilė Giniotienė,  
Consultant, NRD Cyber Security

The CMM document can be found online on the Cybersecurity Capacity Portal: [www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0](http://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0)

## MADE BY THE WORLD FOR THE WORLD

The Centre understands that actionable and impactful knowledge contributions are key to the global advancement of cybersecurity capacity and the important work of the Centre's partners. Good cybersecurity capacity may underpin greater adoption, safety, trust and use of cyberspace; the Centre is gathering evidence to confirm this. Consequently, the GCSCC's areas of impact have been focused around three key outputs: stakeholder adoption, influencing policy and research contributions.

### Adoption by Community Stakeholders

The GCSCC has actively socialised the CMM across sectors, to drive conversation around cybersecurity capacity and to help improve global technology. The resulting adoption of the model by various stakeholders demonstrates the positive impact that the research is having by supporting government self-assessments and informing industry resource and tool development.

Contributions include:

- the completion of almost 100 CMM deployments in over 60 countries, working with national governments in all regions of the world
- the increment of expertise and knowledge in the global cybersecurity capacity-building community's portfolio of work, including:
  - development of the *Cybersecurity Capacity Portal* with the Global Forum on Cyber Expertise
  - collaboration with the World Bank and the Korean Internet & Security Agency (KISA) on their *Global Cybersecurity Capacity Program*
  - the *Oceania Computer Emergency Response Team (CERT) and Capacity Assessments* in the Pacific with the ITU and the OCSC
  - Cybersecurity Capacity Building in the Commonwealth with the CTO
- integration of GCSCC research and knowledge into sector resources such as the World Bank's *Combatting Cybercrime Toolkit*, the collaborative development of the *Guide to Developing a National Cybersecurity Strategy* published by the ITU and partners, and the RAND Corporation's *Developing Cybersecurity Capacity Implementation Guide*
- coordination and participation in panels, forums and workshops across the world, including events such as the Global Conference on Cyber Space, the Global and Regional Internet Governance Forum, the World Summit on the Information Society (WSIS) Forum and the Annual Meetings of the GFCE. Additionally, contributions to the OAS CIO Summit, RightsCon, the Commonwealth ICT Ministers Meetings, the Asia-Pacific Telecommunity Cybersecurity Symposium and the George C Marshall Centre's Program on Cyber Security Studies.

### Influencing and Shaping Cybersecurity Capacity Policy

Through the deployment and dissemination of the CMM and its research findings, the GCSCC has influenced and shaped the policy debate and policy-development process in the field of cybersecurity capacity at national, regional and global levels, including:

- UK FCO using the structure of the CMM to underpin its cybersecurity capacity building programme
- contributions to the GFCE Global Agenda for Cyber Capacity Building and the 2017 Delhi Communiqué as well as to the GFCE Working Groups



- the Commonwealth Cyber Declaration at the Commonwealth Heads of Government Meeting in 2018, providing commitments to national cybersecurity maturity assessments
- international commitments to cooperate, to protect economic and social rights, and to share commitments towards a stable cyberspace
- the development or revision of National Cybersecurity Strategies through the adoption of CMM report recommendations in countries such as FYR Macedonia, Lithuania and Sierra Leone.

### Research Contributions and Dissemination of Evidence

The Capacity Centre collects valuable data from stakeholders across various geographical regions, as well as from public and private sectors and civil society. Such data allows the GCSCC to produce diverse outputs and drive the advancement of the cybersecurity capacity research community in a range of disciplines, including Internet science, government policy, sociology, international law and cybersecurity. Contributions take many forms including academic journal articles, conference papers, books and book chapters and the release of discussion and policy papers. For example:

- *Reviewing National Cybersecurity Awareness in Africa: An Empirical Study* (M Bada, et al; CYBER 2018, The Third International Conference on Cyber-Technologies and Cyber-Systems)
- *Cyber Security Capacity: Does It Matter?* (W H Dutton, et al; Quello Center Working Paper)
- *Cyber Harm: Concepts, Taxonomy and Measurement* (I Agrafiotis, et al; Saïd Business School Research Papers)
- *Improving the Effectiveness of CSIRTs* (M Bada, et al; CYBER 2017, The Second International Conference on Cyber-Technologies and Cyber-Systems)

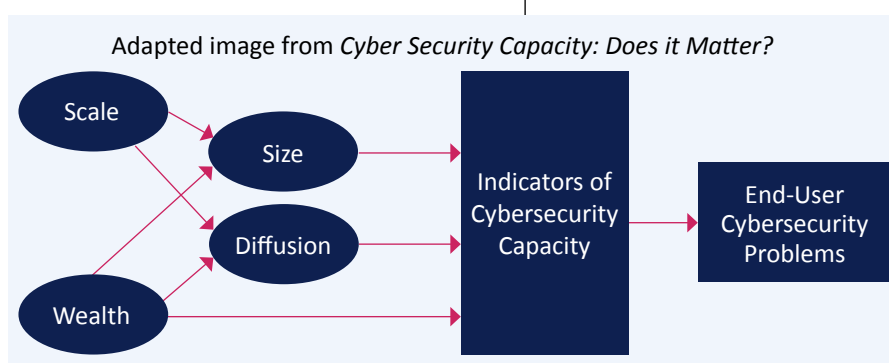
In the GCSCC's early years, the CMM provided the community with new concepts and approaches for thinking about cybersecurity capacity, rethinking awareness campaigns and conceptualising the idea of a cybersecurity mind-set and the harms associated with failures in cybersecurity. More recently the GCSCC's research has expanded to include empirical outputs, such as a study of awareness campaigns in Africa, as well as quantitative empirical research that uses existing datasets available from the ITU, WEF and others. This has allowed the GCSCC to present concrete results on the impact of cybersecurity capacity (see figure below).

The Centre's work has also been acknowledged and referenced in third-party publications, such as:

- *Stay the Course: Why Trump Must Build on Obama's Cybersecurity Policy* (T Howard, et al; Information Security Journal: A Global Perspective)
- *The Cyber-Frontier and Digital Pitfalls in the Global South* (N Schia; Third World Quarterly)
- *Politics of Cybersecurity Capacity Building: Conundrum and Opportunity* (P Pawlak, et al; Journal of Cyber Policy)
- *A Study on the Development for the National Cybersecurity Capability Assessment Criteria* (S Bae, et al; Journal of the Korea Institute of Information Security and Cryptology)

“The CTO has worked with the GCSCC from the launch of their pilot CMM deployment programme, with the research findings relating to the cybersecurity capacity assessment for a number of both Commonwealth and non-Commonwealth countries. Using the CMM has enabled the CTO to better understand and identify cybersecurity gaps and, as a result, develop robust national cybersecurity strategies for various countries. The CTO looks forward to continuing our positive relationship with GCSCC and working with our members to support their own ICT capabilities.”

Dr Martin Koyabe,  
Manager, Technical  
Support & Consultancy  
Division, Acting Head  
of Membership &  
Communications  
Department,  
Commonwealth  
Telecommunications  
Organisation



## CMM REVIEWS AROUND THE WORLD

Almost 100 reviews of over 60 nations since 2015 and counting, providing learning opportunities for understanding what works and does not work in cybersecurity capacity building



### PARTNERS



THE WORLD BANK  
IBRD • IDA



OAS



Oceania Cyber Security Centre



COMMONWEALTH  
TELECOMMUNICATIONS  
ORGANISATION



Norwegian Institute  
of International  
Affairs



NRD Cyber Security

Information on CMM assessments  
around the world is available on the  
Cybersecurity Capacity Portal:  
[www.sbs.ox.ac.uk/cybersecurity-capacity](http://www.sbs.ox.ac.uk/cybersecurity-capacity)

## IDENTIFYING AND MITIGATING CYBER HARM – DEVELOPMENT OF A FRAMEWORK

“ITU is enjoying the partnership with the GCSCC, which complements and enriches the ITU’s mandate on cybersecurity. The CMM assessments, being undertaken together in different regions, proved to be an effective way to deliver assistance to countries, specifically developing ones, as well as demonstrating the ability from organisations with different mandates and scope to join efforts and synergise.

The common approach taken by ITU and the GSCC provides national stakeholders with the mechanisms to identify strengths and weaknesses of their cybersecurity posture and suggests potential corrective measures to be applied. The CMM adds value to the ITU’s work on some thematic areas such as Computer Security Incident Response Teams (CSIRTs) and National Cybersecurity Strategies.



Marco Obiso, Head, ICT Applications and Cybersecurity Division, International Telecommunication Union

The GCSCC is in the process of developing a complementary holistic and robust model for understanding the harm experienced by nations as a result of a lack of capacity. The Cyber Harm Framework (CHF) expands the existing CMM with a methodological underpinning, backed up by a data collection system, for relating cybersecurity capacity indicators to the areas in which harm might be reduced. The results aim to facilitate countries’ understanding of how harm can be reduced and to enable prioritisation of capacity investments towards harm reduction.

Researchers at the GCSCC have been conducting focus groups with cybersecurity experts from diverse disciplines and regions to understand how cyber harm manifests for a nation and its citizens. These interviews provided insights into the definition of cyber harm and the current limitations in detecting and measuring it. They also highlighted the need for enhanced response strategies and controls. In 2017 the GCSCC published a working paper that has led to the development of a taxonomy of cyber harm. This taxonomy has grouped the types of cyber harm into four levels: individual, organisational, infrastructural and national. Within each of these levels, there are six distinct types of possible harm: physical, psychological, economic, cultural, political and reputational. The table below provides examples of how these types of cyber harm might be observed.

<ul style="list-style-type: none"> <li>• Bodily injury</li> <li>• Property damage</li> </ul>	<ul style="list-style-type: none"> <li>• Depression</li> <li>• Panic/stress</li> <li>• Anxiety</li> <li>• Self-harm</li> <li>• Virtual harm</li> </ul>	<ul style="list-style-type: none"> <li>• Financial loss</li> <li>• Loss of shareholder value</li> <li>• Job loss</li> <li>• Market degradation</li> </ul>
Physical	Psychological/emotional	Economic
<ul style="list-style-type: none"> <li>• Disruption of electoral system</li> <li>• Loss of citizen trust in government</li> <li>• Reduction in power projection</li> </ul>	<ul style="list-style-type: none"> <li>• Reduced consumer base</li> <li>• Deteriorated international relations</li> </ul>	<ul style="list-style-type: none"> <li>• Loss of communication means</li> <li>• Loss of cultural property</li> <li>• Harm to social value</li> </ul>
Political/governmental	Reputational	Cultural

We are currently developing qualitative metrics for measuring the full scope of potential harm to identified assets. Interviews and focus groups will continue throughout 2019 and we invite any interested party to participate in this important research.

## COUNTRY INSIGHTS FROM RECENT CMM REVIEWS

The following section provides examples of the deployments and research findings of the CMM around the world. Each review provides an opportunity to gather new information and learn from different situations as the Centre strives to build its understanding of what constitutes national cybersecurity capacity.

### FORMER YUGOSLAV REPUBLIC OF MACEDONIA

**Early in 2018 the GCSCC conducted its review of the Former Yugoslav Republic of Macedonia (FYR Macedonia) at the invitation of the Ministry of Information Society and Administration and in cooperation with the World Bank through the Korea-World Bank Group Partnership Facility.**

**Key observations from the review:**

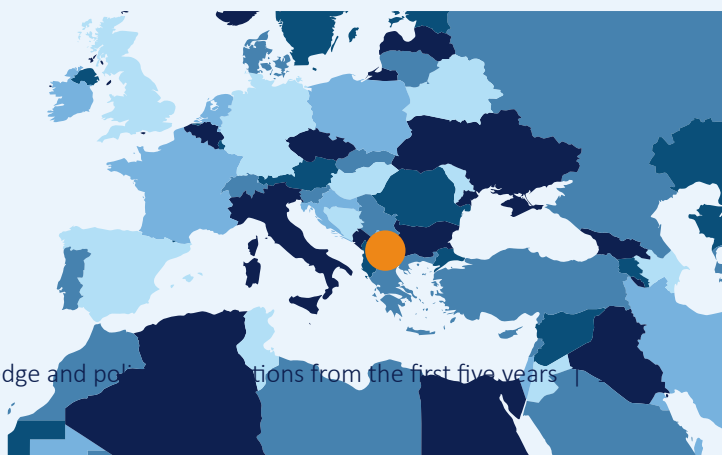
- At the time of the review, the country had no official national cybersecurity document. As a result of the assessment a working group was created, followed by a National Cybersecurity Strategy finally adopted by the government in July 2018. This development demonstrated the country's willingness and efforts to act upon key priorities and recommendations. In addition a multi-stakeholder, inter-agency coalition was formed, bringing together the Ministries of Information Society and Administration, Defence and Interior.
- The cyber ecosystem in FYR Macedonia was still in its early stages, primarily because internet users are not aware of the associated risks. Ultimately, however, participants explained that, in some government agencies and leading companies, a cybersecurity mind-set has started to develop.
- FYR Macedonia has been active in promoting a safer Internet and has had a regular engagement with the EU's Safer Internet Day initiative since 2010. Such initiatives exemplify the increase in cybersecurity awareness-raising efforts, although these are mostly completed on a voluntary basis with limited resources by nongovernmental organisations and with ad-hoc support from the government.
- Training on electronic evidence provided by the Academy for Judges and Public Prosecutors of Macedonia was shown to be in place, though the capacity of prosecutors and judges to handle cybercrime cases and cases involving digital evidence was considered by review participants to be limited and ad-hoc.

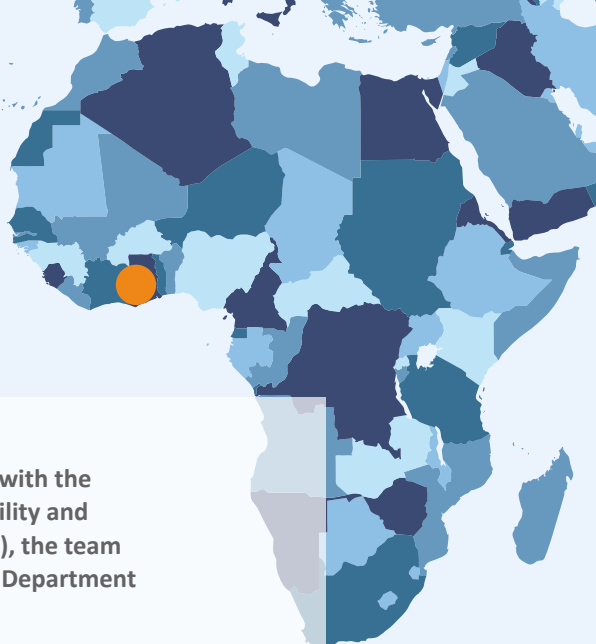
FYR Macedonia was keen to use the momentum resulting from the CMM review and launched an awareness-raising campaign in October 2018 to conduct promotional activities related to cybersecurity and create educational resources to be distributed via different media channels.

The direct translation of the CMM recommendations into the National Cybersecurity Strategy and the action plan which ensued in December 2018 for this implementation showed that the CMM can both provide a bench mark for decision-making and practical support when countries are drafting their national strategy.

You can read the full FYROM CMM review report on the Cybersecurity Capacity Portal: [www.sbs.ox.ac.uk/cybersecurity-capacity/content/fyr-macedonia-cybersecurity-capacity-review-2018](http://www.sbs.ox.ac.uk/cybersecurity-capacity/content/fyr-macedonia-cybersecurity-capacity-review-2018)

Around 70% of the CMM recommendations were incorporated into their National Cybersecurity Strategy (adopted July 2018); the remaining recommendations are planned to become part of the follow-up Action Plan for 2018–22





## GHANA

The GCSCC conducted the CMM review in Ghana in partnership with the World Bank, KISA under the Korean-World Bank Partnership Facility and NUPI. At the invitation of the Ministry of Communications (MoC), the team travelled to Accra in January 2018. Representatives from the US Department of State and MITRE joined the review as observers.

### Key observations from the review:

- At the time of the assessment, Ghana had a National Cybersecurity Policy and Strategy, which had been drafted in 2016 and led by the MoC. However, the implementation was still at a very early stage and, before commencing new initiatives, the government's plan was to align and coordinate the programmes and initiatives outlined in the five-year strategic plan for 2016–20, with already ongoing projects.
- Particular attention was paid to the launch of the National Cyber Security Centre, the implementation of coordinated awareness campaigns across the country, the equipment of the national Computer Emergency Response Team with the required budget and human resources, and the establishment of systematic processes and mechanisms to enhance information sharing between Critical National Infrastructure owners.
- The CMM concluded that Ghana does not yet have a cyber-conscious culture. Participants described Ghana's culture as generally very trusting, with users not well aware of the risks associated with the use of the Internet. Cyber awareness in the government and in the private sector, with the exception of large international companies, was described as minimal. In response to these findings, the government took several steps to develop a cybersecurity culture, including events such as National Cybersecurity Month in October 2018 and the implementation of a nationwide programme to address cybercrime-awareness gaps in cooperation with UNICEF.
- In December 2018 Ghana acceded to the Budapest Convention after the CMM report had identified ad-hoc informal and formal cooperation mechanisms and limited capacity of prosecutors and judges to handle cybercrime cases and cases involving digital evidence. This gap was further addressed by the continuation of training for judges and prosecutors as part of the Council of Europe's GLACY+ Project.

These initiatives provide evidence for the increasing maturity of Ghana's cybersecurity capacity and the steps taken by the government show that the issue has become a priority. The CMM review helped to identify areas for prioritisation and continues to provide a benchmark for further areas for action.

Since 2015 the GCSCC has completed 11 CMM reviews in North, West, East and Southern Africa in partnership with the World Bank, the ITU, and the FCO. Further CMM reviews on the African continent are planned.

## SAMOA

In collaboration with the ITU, the GCSCC and its regional partner the Oceania Cyber Security Centre (OCSC) undertook a review of the maturity of cybersecurity capacity in the Independent State of Samoa at the invitation of the Ministry of Communications and Information Technology (MCIT) in April 2018. This mission to Samoa was the first CMM review conducted in partnership with the OCSC, marking the beginning of strengthening cybersecurity capacity in the Oceania region.

### Key observations from the review:

- Samoa has published a national cybersecurity strategy in cooperation with the MCIT and the ITU, to include a series of consultations across all levels of government, the private sector, academia and community representatives. The MCIT has been given a mandate to consult across public and private sectors, as well as with civil society.
- Samoa is currently in the process of developing a national incident-response capability. Most focus-group participants could think of ways in which incidents within their organisations could constitute national-level issues but, as yet, it appears that there is no register or catalogue of incidents that is centrally maintained.
- Focus groups suggested that Samoa, consistent with findings from other Pacific Island countries, has a very low level of awareness of cybersecurity. It was noted that people are less interested because cybersecurity is fairly new to the country and not widely used, and there is a general lack of knowledge about any national cyber-attacks or personal bad experiences with cyber-incidents.
- Cybersecurity awareness among the general public is low. Under the leadership of the MCIT and in partnership with the Ministry of Police, new provisions have been made for the government to re-introduce the Cyber Safety Pasifika awareness campaign.
- Samoa currently lacks any cybersecurity-specific legislation, although several legal instruments touch upon cybersecurity-related activities. The government is aware of this issue and is currently working towards ratifying the Budapest Convention on Cybercrime, as well as thoroughly examining and re-evaluating domestic legislation.
- As part of the implementation of the national strategy, the MCIT and the Office of the Regulator are leading the assessment and development of suitable cybersecurity standards.

The GCSCC first visited the Pacific in 2015 to complete a CMM review of Fiji in partnership with the CTO. The recent review of Samoa in April 2018 was soon followed by a review of Tonga in June 2018. The collaboration between the GCSCC and OCSC aims to assess all nations in the Oceania region over the next few years.





## GEORGIA


For the CMM review in Georgia, the GCSCC collaborated with its latest implementation partner, the Lithuanian technology consulting firm NRD Cyber Security (NRD-CS). The deployment of the CMM marks another step towards closer collaboration between the GCSCC and NRD-CS following the company's contribution to CMM reviews in Lithuania and Bangladesh in 2017 and 2018. At the invitation of the Data Exchange Agency of Georgia (DEA), researchers of the GCSCC and NRD-CS travelled to Georgia in November 2018.

### Key observations from the review:

- Georgia began implementing its first national cybersecurity strategy in 2012. This strategy was reviewed in 2016 and a third iteration is currently underway.
- Georgia approaches cybersecurity as a whole-of-nation challenge that cannot be outsourced to any single independent agency. However, not all relevant stakeholders have been involved in efforts to improve the country's cybersecurity posture to the same extent: while the national cybersecurity strategy recognises the education sector as one of its pillars, resource constraints limit progress in translating this strategic priority into practice.
- Organisations throughout Georgia have achieved considerable advances in operational capacity, with technical coordination on cybersecurity matters surpassing cooperation on many other security issues, largely thanks to strong personal networks.
- Georgia faces challenges replicating these efforts at scale due to a lack of affordable training programmes and educational opportunities. A first master's degree programme dedicated to cybersecurity will open in 2019. In the meantime, Georgia has launched the pilot phase for establishing a cyber reserve, which looks to harness the expertise of cybersecurity professionals working in the private sector for national security purposes without engaging in a competition for scarce cybersecurity talent.
- Early on, Georgia identified threats emanating from foreign influence operations, and exercises simulating the effects of informational warfare and testing responses have been organised. National scenario-based crisis management exercises, held annually, have also featured cyber-related injects.
- Georgia's government CERT and the Ministry of Defence's Cybersecurity Bureau act as coordinating authorities for the two respective groups. The law requires all critical information system subjects (CISS) to designate information security managers and cybersecurity specialists that are eligible to receive free certificate training from DEA, which also offers free penetration testing services to public organisations.

### Important for Georgia's CERT

Under the Law on Information Security, promulgated in 2012, two first sets of civilian and military organisations entities have been identified as CISS.



## REGIONAL CYBERSECURITY ASSESSMENTS OF LATIN AMERICA AND THE CARIBBEAN

Further to the individual country CMM reviews, the GCSCC worked with the OAS and supported two regional studies of the Latin America and Caribbean region (LAC). This resulted in the publication of a first report ‘Cybersecurity: Are We Ready in Latin America and the Caribbean?’ with the the Inter-American Development Bank (IDB) in 2016 that provided a comprehensive and up-to-date depiction of cybersecurity in the region.

The data for this report was collected from country stakeholder focus groups conducted by the OAS and the GCSCC. The stakeholders involved included: government agencies, critical infrastructure operators, the military, law enforcement, the private sector and academia. The evidence from the reviews and focus groups was then collated using an online tool designed and developed by the OAS in partnership with the GCSCC. Additionally, staff from both institutions collaborated in the CMM reviews in Jamaica and Colombia.

The report was made up of two main sections. The first section, ‘Expert Contributions’, presented essays on cybersecurity trends in the region written by international cybersecurity experts covering topics specific to Latin America and the Caribbean, such as

- capacity building and diplomacy
- privacy and trust
- cybercrime legislation
- sustainable and secure societies

The second section, ‘Country Reports’, provided an overview of the current state of cybersecurity in the countries in the LAC region. Each country profile provides a short overview of recent cybersecurity developments in the country, statistics on the country’s population, number of people with Internet access, mobile phone subscriptions, and percentage of Internet penetration. In addition, each profile shows the country’s maturity level for each indicator allowing nations to be better informed and identify areas for prioritisation and investment to support the advancement of national cybersecurity capacity.

A follow-up regional study was completed by the OAS in 2018, with the findings and report expected to be published later in 2019.

You can access the results and the full report on the Cybersecurity Capacity Portal: [www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf](http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf) and on the OAS Observatory of Cybersecurity in Latin America and the Caribbean: <http://observatoriociberseguridad.org/graph/countries//selected//0/dimensions/1-2-3-4-5>

## LOOKING FORWARD

In the next couple of years, the GCSCC is looking forward to further developing its regional partnerships. 2019–20 will see the continuation of the OCSC CMM reviews in the Pacific region, as well as the start of similar partnerships in Southern Africa and South East Asia. In total, by 2021 the estimation is that a further 50 countries will have completed a CMM review providing an unparalleled research opportunity for understanding national cybersecurity capacity.

The regional partnerships will be pivotal to the uptake and sustainable use of the CMM and CHF around the world, to the expansion of global cybersecurity networks that support this activity, and to the multiplication of opportunities for increased collaboration of capacity-building activity internationally.

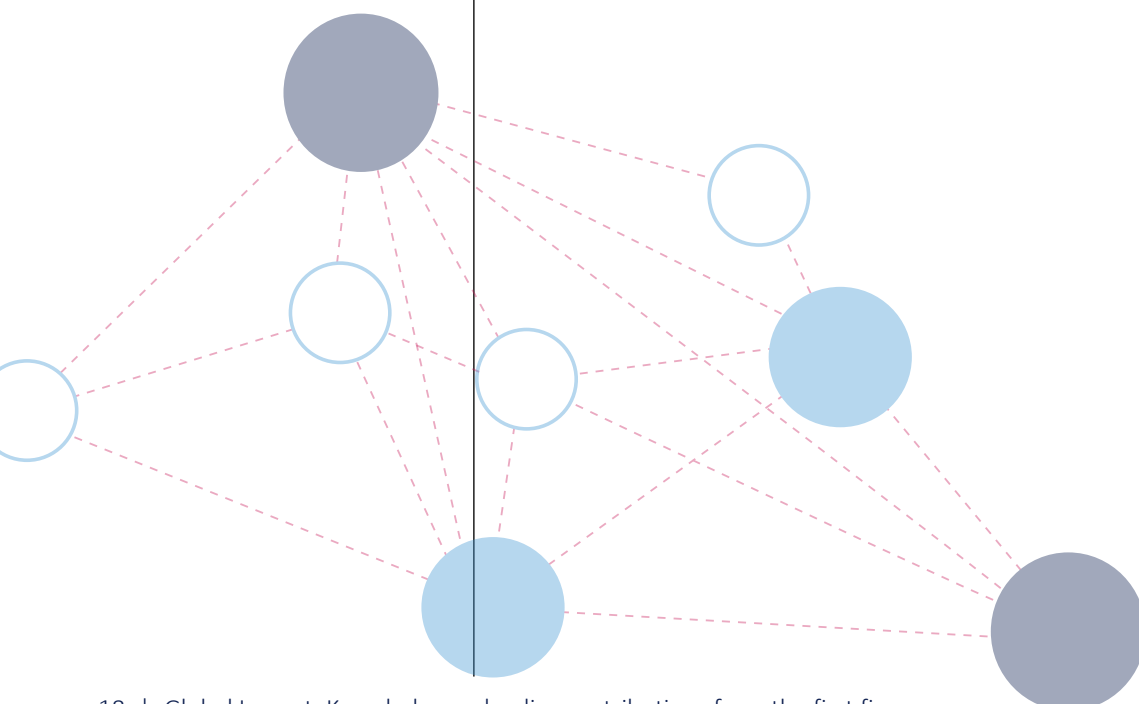
2019–21 will also see increased research outputs, including the publication of a new iteration of the CMM based on the lessons learnt since the second revision in 2016, as

well as the publication and integration of the CHF into the CMM. This enhancement will ensure the delivery of a robust capacity maturity assessment package, thus amplifying the calibre of the research, its outputs and the opportunities for capacity building around the globe.

Specifically, three major research strands will be prioritised:

Firstly, having collected field data from more than 100 reviews, the dataset will become a fundamental resource for original research due to its increase in scale and complexity. This will enable the project to conduct analysis of the factors driving capacity building as well as determine the implications of capacity building for societies around the world.

Secondly, the GCSCC will move from the collection of data primarily by its field research team to the creation of a 'structured field coding' instrument that will enable researchers to collaborate with teams across the world who can collect data



in a way which is replicable and comparable to their own data. This will make for a dramatic advance in the scale of the data collection as well as its empirical reliability and validity for cross-national comparative research.

Thirdly, qualitative interviews and focus groups with experts are yielding a very comprehensive systematic categorisation of the harms associated with failures in cybersecurity. The GCSCC expects to further develop its taxonomy of harms, which will help anchor more systematic quantitative and case-study research to more concretely see the costs of failing to protect the security of individuals, organisations and nations.

The continued adoption of these research-driven models by the international community will be an important contribution to the GCSCC's impact; it will also contribute to research as it produces data to analyse, by working with capacity-building organisations such as the World

Bank, the OAS, the CTO and the ITU, and countries which are donating funds and investing in capacity building in third-party countries. This collaboration is underpinned by an education and training strategy which the GCSCC has started to develop in 2018 and will deploy over the next two years. This includes the systematisation of training available to partners of the GCSCC through remote and face-to-face training.

The GCSCC therefore looks forward to advancing its research and engagement programme to promote and embed the use of the models as opportunities arise, strengthening synergies and fostering further collaboration and knowledge-exchange with more countries around the world.

*If anything in this publication caught your interest and you would like to get involved as a research sponsor, implementer or collaborator, get in touch at:*  
[cybercapacity@cs.ox.ac.uk](mailto:cybercapacity@cs.ox.ac.uk)



**Global  
Cyber Security  
Capacity Centre**



[cybercapacity@cs.ox.ac.uk](mailto:cybercapacity@cs.ox.ac.uk) | [twitter.com/CapacityCentre](https://twitter.com/CapacityCentre) | [www.oxfordmartin.ox.ac.uk/cybersecurity](http://www.oxfordmartin.ox.ac.uk/cybersecurity)

Global Cyber Security Capacity Centre, University of Oxford  
Department of Computer Science, 15 Parks Road, Oxford OX1 3QD, UK