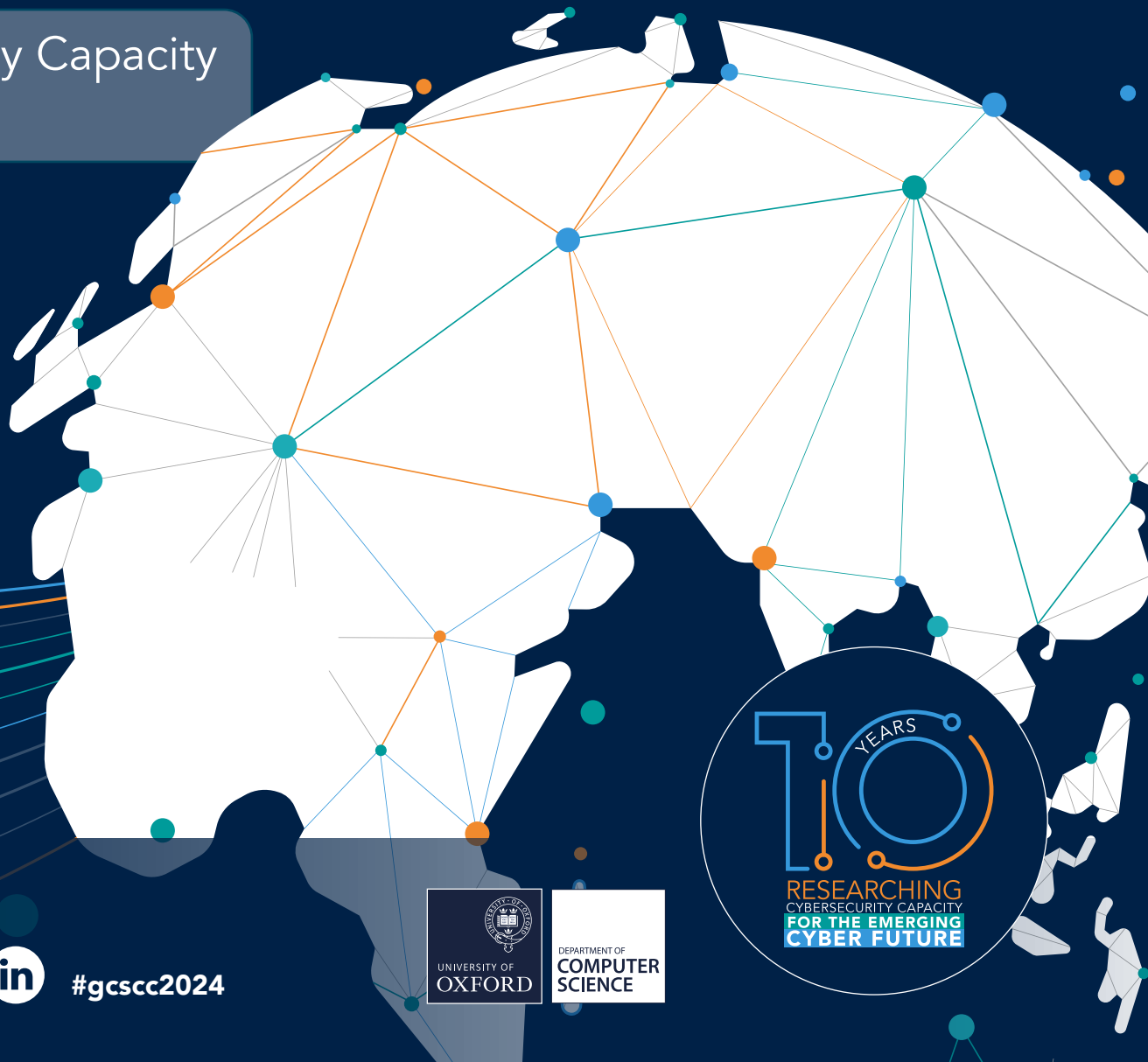
A Decade of Research on Cybersecurity Capacity:

Reflections on Themes and Issues for our Emerging Cyber Future

Notes on the Global Cyber Security Capacity Centre's 2024 Annual Conference



Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

#gcscc2024

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

10 YEARS

RESEARCHING CYBERSECURITY CAPACITY FOR THE EMERGING CYBER FUTURE

Preface and Acknowledgements

This report summarises key themes that arose in the 2024 edition of the Annual Conference of the Global Cyber Security Capacity Centre (GCSCC). It was held at the Oxford Martin School on 30 April 2024. As with previous GCSCC conferences, it was a working meeting, held with the objective of stimulating reflections and insights on the past and future of research on cybersecurity capacity building (CCB), with the aim of recognising the challenges for capacity building to become more strategic and global and to propose ways to address these challenges. In contrast to previous conferences, it marked ten years since the launch of the GCSCC and therefore took on the mission of capturing key aspects of this decade of innovation in capacity building as well as anticipating developments over the coming decade.

The editors take responsibility for any errors or misunderstandings of the discussions which were wide ranging and complex. Nevertheless, we encourage further comments, corrections and amendments on this report from all the participants and the larger community involved in cybersecurity and capacity-building efforts. We hope this report will help the reader to become more engaged with our work.

No quotes are attributed to any individual without their explicit permission, but the notes do seek to paraphrase and summarise the contributions of individuals. The report is anchored in what was said on the day. However, any errors or misunderstandings are the responsibility of the editors and not the speakers. We thank all the speakers, chairs and participants who have helped shape this report. We owe special thanks to Bill Dutton, Lucy Wiseman, Carolin Weisser Harris, Sadie Creese and Jamie Saunders for their reviews of an early draft. Appendix 1 provides a summary of the agenda, which identifies the speakers and chairs. Appendix 2 lists the larger set of those who attended and contributed to the content of this report. Appendix 3 provides a list of the partners, sponsors, and funders of the CMM and its deployment around the globe over the last ten years. A list of acronyms and abbreviations used in this report are provided in Appendix 4, and Appendix 5 lists the sources referenced in the report.

The Application of the CMM over the Past Decade

As cybersecurity threats continue to rise across the world, it is increasingly apparent that the GCSCC's multidisciplinary approach to CCB through the Cybersecurity Capacity Maturity Model for Nations (CMM) was and remains on the right track. The multiple dimensions of the CMM (Box 1) remain critical for helping nations determine where they stand in developing the capacity for withstanding threats to their cybersecurity and where new and greater investments are needed.

Five Dimensions of Cybersecurity Capacity Building

The CMM considers cybersecurity to comprise five Dimensions which, together, constitute the breadth of national capacity that a country requires to be effective in delivering cybersecurity:

- Developing cybersecurity policy and strategy;
- Encouraging responsible cybersecurity culture within society;
- Building cybersecurity knowledge and capabilities;
- Creating effective legal and regulatory frameworks; and
- Controlling risks through standards and technologies.

1

See: **https://gcscc.ox.ac.uk/cmm-dimensions-and-factors**

Progress over the Past Decade

Professor Creese walked through the stages of the CMM's deployments from the first CMM application and review publication in December of 2014, through the evolution to include regional as well as national reports, the reassessments beginning in 2019 and our wider research into the effectiveness of capacity building. To-date, the CMM has been applied in 138 assessments, including 94 countries and 44 reassessments (nations with two CMM deployments).

A key to our progress in reaching countries across the world has been our partnerships with regional and international organisations who are experts in capacity building, as well as our constellation centres in South Africa and Australia. We want to thank those partners.

The experience gained from the conducting CMM reviews has established the value of deploying the CMM both to benchmark current capacity and to identify gaps. This knowledge is helping nations build the evidence-base and business-case justifying investments; understanding what cybersecurity capacity needs to be enhanced and what ought to be prioritised going forward.[1]

The Global Constellation

2

Global Cyber Security Capacity Centre, Oxford University, UK

Oceania Cyber Security Centre (OCSC), Australia

Cybersecurity Capacity Centre for Southern Africa (C3SA), South Africa

See: **https://gcscc.ox.ac.uk/global-constellation**

Forward-Looking Strategies

In moving into the next decade, the GCSCC and its partners have already begun to realise the benefits of the increasing number of reviews in creating a unique database anchored in the reviews for analysis of the factors shaping cyber capabilities and their implications for the countries (Creese et al 2021a, 2021b). Success has also reinforced a growing set of partners and sponsors of CMM assessments around the world. Studies of capacity building at the national level have led the GCSCC team to explore studies of smart city developments and working from home (Box 3). In addition, the CMM has been scaled up and used by major international organisations (IO) for regional analyses, complementing research GCSCC conducts on developments which provide challenges to national capacities, such as artificial intelligence (AI). Nevertheless, investment in CCB and associated research and development has been widely judged to be insufficient to address the growing worldwide risks.

It is in this spirit that the following keynote address by Heli Tiirmaa-Klaar is particularly pertinent.

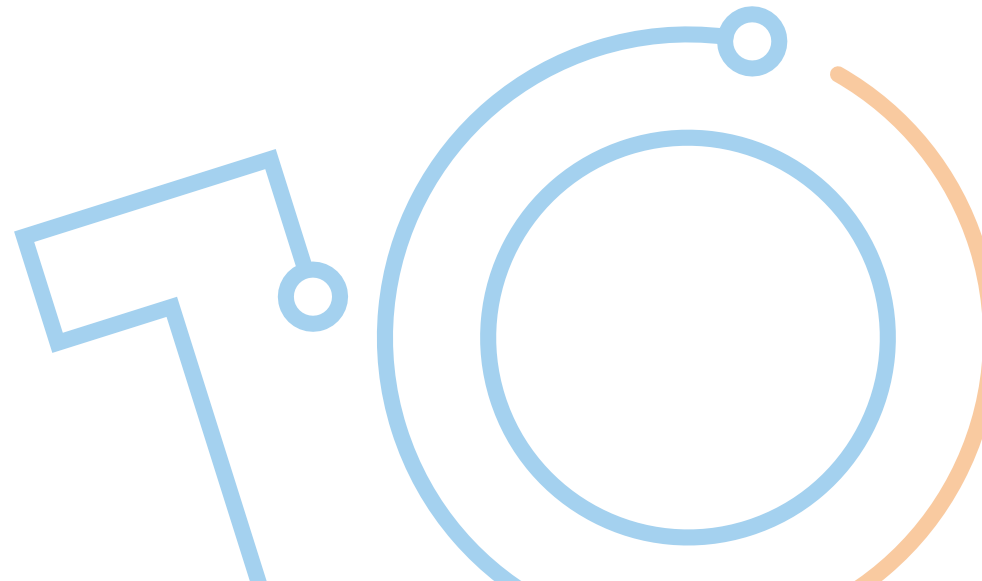

10 YEARS
RESEARCHING FOR THE EMERGING FUTURE
Global Cyber Security Capacity Centre

Keynote: Changing the Capacity Building Narrative

Heli Tiirmaa-Klaar, Director of the Digital Society Institute of the European School of Management and Technology (ESMT) Berlin, kicked off the day by delivering an inspiring keynote, entitled "The Need to Change the Cybersecurity Capacity Building Narrative". She captured a key issue around the difficulties in communicating the social and economic benefits of cybersecurity capacity building while offering a way forward. Her keynote began by comparing the situation at the time of the Centre's conception, with the present. A decade ago, cybersecurity capacity building was an innovation, creating the impetus to set up the GCSCC and work closely with the development community. Presently, while capacity building has been implemented widely, online cyber threats have become more multifaceted, cybercrime has soared, threats have become more severe, and a new frontier in warfare is spreading worldwide. Nevertheless, there has not been a sustained level of investment despite challenges in threats and weaknesses in building the required skills and workforce.

Heli argued that there was a need to redefine our narrative, primarily by moving from a too tech-centric perspective to also communicate the social and economic consequences of cybersecurity capacity building. While it seems apparent that cyber-attacks have led to major economic loses to businesses and nations, there is a dearth of hard data on the impact of capacity building. Also, there has not been a cyber equivalent of Pearl Harbor that galvanised action. Instead, we seem to be experiencing a death by a thousand cuts. And major events, such as the NotPetya ransomware attack, continue to arise. Her own nation, Estonia, was not affected by NotPetya as it had patched vulnerabilities in a timely way, but even in the event of such successes, politicians and pundits are left downplaying its significance – not a serious problem. This calls for changes in the attitudes and frameworks for understanding cyber and CCB efforts. Encouraging organisations and nations to invest now to reduce the problems we will face in the future is challenging, particularly when nations have a growing array of other major economic and social problems on their agendas.

How can we change this narrative to showcase the economic and social rationality of acting now to move CCB to a higher priority in development narratives? Her suggestions ranged from educating leaders to harnessing innovations such as generative AI. Her talk included examples of successful initiatives, such as in how the UK and Estonia have helped Ukraine to withstand major cyber-attacks. Heli ended with a quote from Lewis Carroll, the famous author and lecturer at Christ Church College in Oxford in the 1800s, in Alice's Adventures in Wonderland and Through the Looking Glass, about the need to run faster just to stay in one place. LINK TO KEYNOTE



3

Cybersecurity in Remote Work and Working from Home

Bill Dutton moderated a side event for the conference on remote work, including working from home. The concept of flexible workplaces has been growing for many years as the technology to support remote work became more ubiquitous. The COVID pandemic forced many out of the office to experience working remotely. This sudden shift of workplace norms brought many challenges in keeping networks secure, as the new workplaces brought new threat surfaces. For many organisations, these shifts became part of the new normal as many workers found they preferred working from home or working in a hybrid model. This shift in workplace expectations has profound impacts on how to manage risks and support productivity, but individuals differ in their responses to working from home. Questions included: What types of cybersecurity threats face individuals working outside the office? What types of training and support do workers get from employers when working remotely? How is the sense of distractions and productivity tied towards worker preferences for location of work? How can management best support productivity when work is conducted remotely?

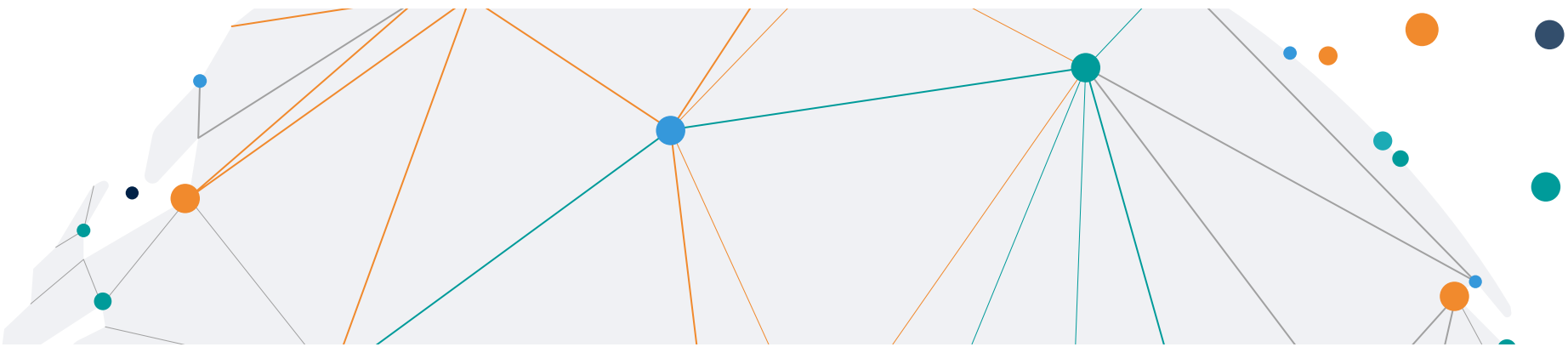
Monica Whitty kicked off the workshop with a presentation on the psychology of cybersecurity in working from home, where individuals might be more isolated from advice and support when faced with cyber issues (Bispham et al 2022al). Patricia Esteve-Gonzalez reported on GCSCC research on whether working from home exacerbated problems with cybersecurity. Her work found that it was a change in workplace, rather than working from home per se that was associated with more problems with cybersecurity. The workshop was concluded by Ruth Shillair, who provided a valuable synthesis of research on models of threat, distractions, and productivity to point out promising directions for future research.

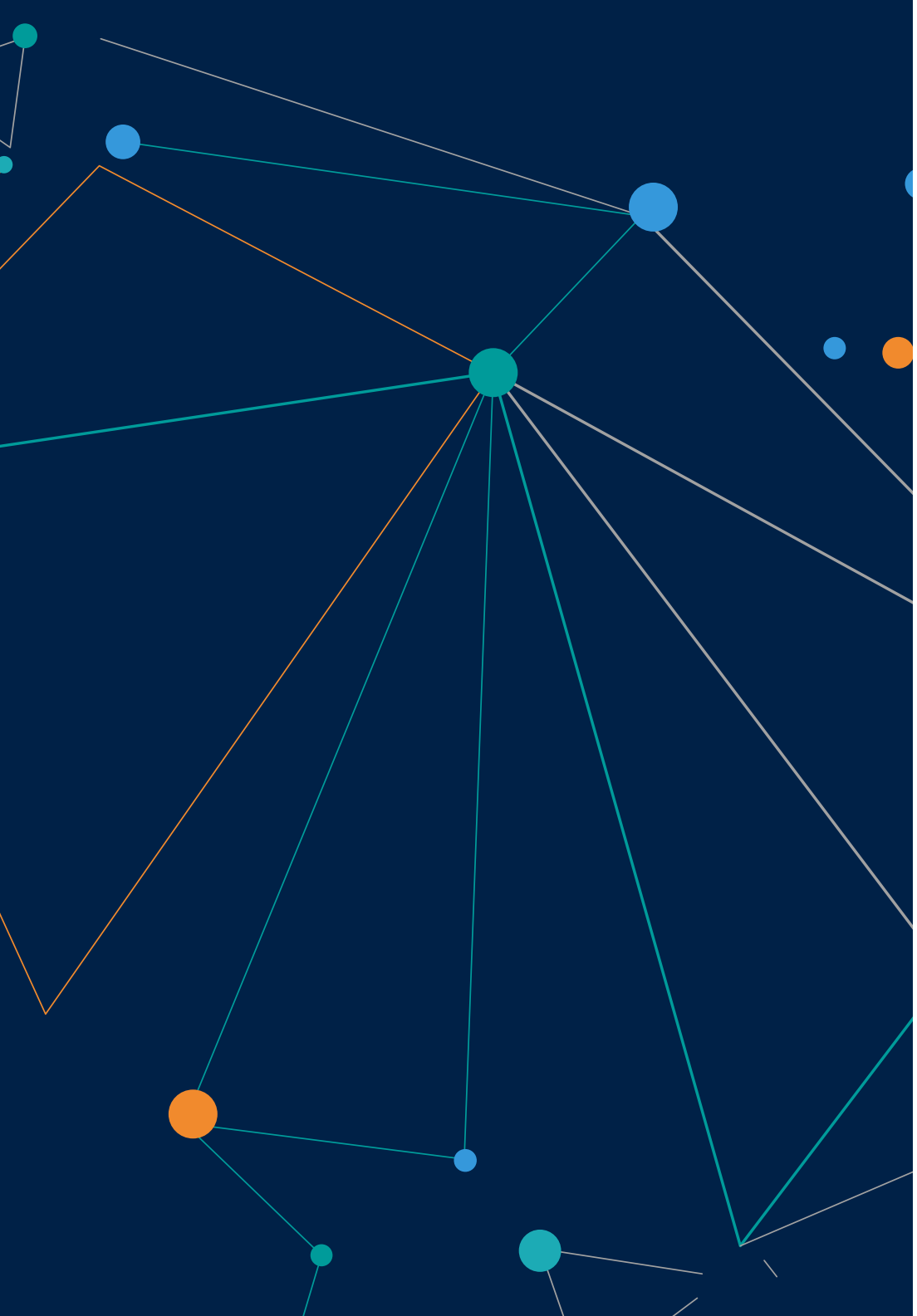
Session 1: Emerging Risks and Challenges for Cybersecurity

The first panel for the day was chaired by Professor Sadie Creese, and featured short talks by John Mallery, Research Scientist, CTO, WFA Group; Stephen Roberts, Professor of Machine Learning, University of Oxford; Heli Tiirmaa-Klaar, Director, Digital Society Institute at ESMT; and Paul Trueman, Executive Vice President, Cyber & Intelligence, Mastercard.

The panel was asked to address an array of questions: How is digital technology evolving and what are the cyber-risk scenarios that must be prioritised for future cyber-resilience? What are the opportunity costs of inaction, and the harm consequences at all scales from global networks to regions, nations, individuals and businesses? Are we responding to the evolving mission to protect people, deliver safety, support human rights and the ability for self-determination and sovereignty? The panel explored the various risks and challenges that exist and are emerging in cyber, from the perspectives of AI, development, policy, private industry and more. The discussion explored the prevalence and challenges of cybercrimes and how they can be combatted, which were complemented by discussions around the potential weaknesses and points of vulnerability in AI models. There were additional presentations on international AI diplomacy and governance, and the shared norms that inform these concepts.

Professor Stephen Roberts focused on lessons learned from over twenty years of his involvement as an engineer in building machine learning models, arguing that tomorrow's challenges for AI are today's problems – tomorrow's problems are here now. In AI cybersecurity, his focus was on identifying three critical attack points: the data you use to train the models; the model itself; and the training or inference algorithms. He pointed out that the pollution of training data has been going on 'forever' in the area of financial training models. However, he argued that different models carry different risks. As a general point, he drew an analogy between an AI model and a "super car", saying that a person driving a 1,000 horsepower car can be dangerous. He argued that we need to move to a NASA-style production process to build in zero faults and redundancy.





Paul Trueman from Mastercard spoke about priorities and protocols to enable security – to make it work. He emphasised that criminals are getting access to smarter technologies, so individuals are now among the usual suspects of nation states and organised crime as bad actors. But all criminals are also obtaining new and better technologies, enabling crime to move into digital spaces, where they can act from anywhere at any time with the benefit of repeatably. This provides the potential for incredible scale to their operations. He noted that ransomware, scams, and other cybercrimes are already at a high level but will only get worse. He used an analogy that was repeated often throughout the remainder of the day, comparing cybersecurity to a roof with an undetected minor leak. It may look safe, and a single drop of water alone will not cause great harm, but eventually a drop of water would leak into the light fixture resulting in catastrophe. In this analogy, it then leads to a lack of trust in the whole system. Paul concluded his remarks with a valuable adage, drawn on a quote from US President Dwight Eisenhower, that: "Plans are nothing; planning is everything." Despite common derision of "plans", what can be learned from a good and continuous review of planning and exercises around cybersecurity is key to an organisation or institution's ability to respond effectively to cyber-attacks.

John C. Mallory, a research scientist, has been at MIT's Computer Science & Artificial Intelligence Laboratory since 1980 and also an Oxford Martin School Associate. His research has focused on national cybersecurity strategies, including technical strategies for cyber defense. He has organised over the years a series of Roundtables on Military Cyber Stability (RMCS), from which he has drawn general points about change in various dimensions of cybersecurity, threat actors, and the phases of international conflict, such as the stages of Reaction, Struggle for Position, and Major Conflict. Given his focus on the rapidly changing contours of international security practices, he expressed some scepticism over the prospects for legislation on AI, which would inevitably be chasing a moving subject and likely to miss the millions of users of AI, as well as the rapid evolution of autonomous weapons systems.

Since 2016, Russia has established two specialised boutique groups focused on designing and executing information operations. These groups are likely

smaller, highly specialised units within larger intelligence or military frameworks, creating strategies and tactics for disinformation campaigns, cyber activities, and psychological operations aimed at influencing public opinion and political environments to destabilise political systems, influence elections, and create social discord in target countries. Such information operations are part of a broader strategy of hybrid warfare, where Russia has employed a mix of military and non-military tactics to achieve its objectives.

The boutique groups use a variety of tools including social media manipulation, fake news, and other forms of propaganda, but hacking and data breaches may also be employed to support these information operations. He argued that we need to understand and describe the technical systems and its vulnerabilities but also the social and economic systems around it for people to be able to understand and trust emerging systems. People need to know where the leak of water from the roof is coming from and why.

Session 1: Observations

Data: AI models heavily rely on the quality and integrity of the data they are trained on. This data can be an attack vector, where misinformation and false information can pollute the training dataset, leading to inaccurate or harmful model outputs.

Model Class and Functionality: The type and complexity of the model class also determine its susceptibility to attacks. While simpler models with strong inductive biases might face limited risks, more complex, deeper models are increasingly vulnerable due to their greater flexibility and capacity to fit data.

Inference Algorithm Training: The algorithms used for training AI models can be manipulated. This includes poisoning the training process, where attackers inject malicious data or influence the model's learning path, leading to corrupted model functionality.

Challenges of Decentralisation: The proliferation and decentralisation of AI models complicates issues of explainability and the ability to "unlearn" polluted data. This is because models often do not have a clear understanding of the data's integrity, making them susceptible to sustained pollution.

The Need for Robust Safeguards: There is a call for adopting a principles-based, process-driven approach like NASA's model, focusing on building zero-fault safeguards to ensure AI system reliability and security.

Unique Sensitivities and Risks: AI models operate in environments that are both opaque and open, making them uniquely sensitive to data pollution. Attackers can exploit these conditions by subtly altering the data, making it difficult to detect and counteract such attacks. The complexity and depth of modern AI models amplify these risks. While regulatory frameworks and compliance measures can mitigate some threats, the inherent nature of these sophisticated models leaves them vulnerable and difficult to regulate in advance.

Evolving Nature of Cyber Threats: Cybercriminality is evolving, characterised by anonymity, scalability, and repeatability. The primary areas of concern are ransomware, which disrupts and steals data, and scams, both of which are interrelated and mutually reinforcing. The imperative is to enhance capacity and capability to guard against these threats, thereby preventing chaos and maintaining trust.

Strategic Approaches to Cyber Risk Reduction: Effective cyber risk reduction involves understanding threats, vulnerabilities, and potential consequences. Strategies like restraint and deterrence are critical in mitigating these risks. Current international dialogues, especially among the US, Russia, and China, focus on crisis management, strategic abilities, and addressing key issues such as AI's role in controlling nuclear weapons.

Governance and Diplomacy in AI: AI governance involves analysing risks, challenges, and underlying assumptions within AI models. Military AI's key challenges include maintaining stability, speeding up decision-making processes, and ensuring system integrity. The consensus is that AI has fundamentally altered our world, and there is no returning to pre-AI conditions. Effective governance seeks to address these changes through responsible AI practices and comprehensive risk analysis.

In response to audience questions, several other points were made, including:

Security Testing of AI Systems: The level of security testing required varies with the model's complexity. While straightforward models are easier to test, large AI models present vast, accessible volumes for potential attacks. Often, it is challenging to detect ongoing attacks, emphasising the need for vigilant monitoring.

Broken Windows Approach in Cybersecurity: The broken windows approach, focused on addressing minor crimes to prevent larger crimes, faces challenges in cybersecurity due to less visibility and sharing of incidents as well as the erosion of trust following attacks. Trust is crucial for system integrity.

Session 2: Cybersecurity Regulation and Governance through a Regional and International Lens: Will One Size Fit All?

David Wall, from Leeds University, an Oxford Martin Fellow, chaired this session on regulation and governance. He is the Chair in Criminology at Leeds, with a book on cybercrime that came out the day before the conference (Wall 2024). Speakers included: Violanda Botet, Deputy Executive Secretary for the Inter-American Committee against Terrorism (CICTE) at the Organization of American States (OAS); Enrico Calandro, Board Member, Cybersecurity Capacity Centre for Southern Africa (C3SA); Barbara Grewe, Next Horizons Scholar; Szilvia Toth, Cyber Security Officer, Organization for Security and Co-operation in Europe (OSCE); and Monica Whitty, Head of the Department of Software Systems and Cybersecurity and Professor of Human Factors in Cyber Security at Monash University, Melbourne. In addressing cybersecurity regulation, do we risk cyber inequalities and security divides? What are the specific needs for developing economies? Can a multi stakeholder approach facilitate a more globally equal response? What are the barriers that we face and how should we work together to address them more effectively?

Professor Wall noted that current cybersecurity regulation and activity is presented to protect developing countries from becoming crime havens and enabling their citizens to enjoy the benefits of the information society. However, if not handled sensitively, it is in danger of perpetuating the global north-south divide, demanding changes in the budgets of smaller nations to serve the interests of developed

nations, having a 'glocalising' effect on developing countries in shaping their national development, and could ultimately cause 'virtual colonialism'. Professor Wall asked his panel to provide their perspectives on the problem, its solution, and barriers to the solution.

Szilvia Toth noted that many OSCE participating States have benefitted the CMM process. The OSCE was the first regional organization to develop cyber confidence-building measures (CBMs). These are voluntary and non-binding, however states made a political commitment to adhere to them. Implementation of the CBMs – be it on sub-regional or OSCE-wide level – build national capacities and enhance cyber resilience. Good practices and recommendations out of these efforts are publicly shared, for example in the forms of reports or a database of cyber-related terminology compiled from the OSCE region.

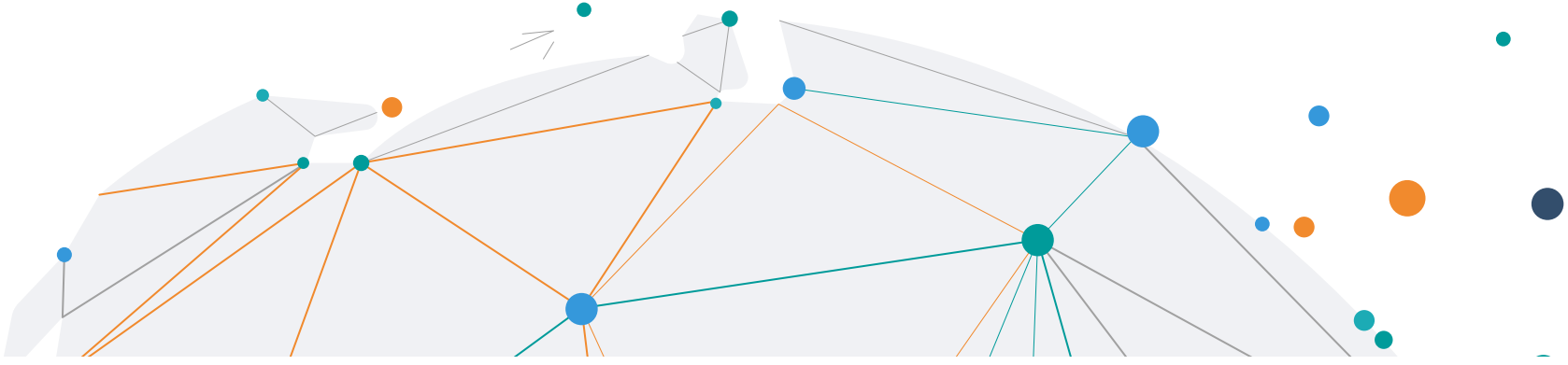
Violanda Botet spoke about how CICTE promotes cooperation and dialogue among OAS Member States to counter terrorism, while respecting the sovereignty of each country consistent with international law. CICTE was established in 1999 and reinvigorated after the 9/11 attack on the United States and currently serves as a useful political forum for discussion and publications on national strategies to prevent and counter terrorism. She stressed the important role that IOs play in cybersecurity capacity building. In 2004 she noted that CICTE was given a mandate by OAS member states to provide technical support to OAS states, including by helping to national develop cybersecurity strategies; cybersecurity emergency response teams (CERTs); CBMs using a multistakeholder and country specific approach. She described CICTE's work as helping to identify threats and serve as a mechanism for promoting and facilitating in the Western Hemisphere cross regional cooperation and for the adoption of more comprehensive international legal frameworks on cyber related matters. In addition, Violanda highlighted three Regional Studies onCybersecurity Maturity in OAS Member States, which utilise the GCSCC's CMM methodology, which provides a unique overview on the levels of cybersecurity maturity in the Americas.

Enrico Calandro spoke about the activities of the Cybersecurity Capacity Centre for Southern Africa (C3SA), based in the Department of Information Systems at the University of Cape Town, South Africa, part of a consortium with Research ICT Africa (RIA), the GCSCC), and the Norwegian Institute of International Affairs (NUPI). He provided an overview of the work that he and colleagues have been focused on the study of regulatory efforts across Africa since 2020.

They deploy the CMM, conduct research and organise outreach activities. He sees promise in furthering a multistakeholder approach, which he believes countries of Africa have approached through a process that started in 2023, but they faced an overall lack of capacity building and the difficulties of agreement among 55 countries. The key barrier, he argued, was sustainability given that priorities change and timelines are difficult to meet. Capacity building still needs to establish more credibility with national governments across Africa.

Monica Whitty, a Professor at Monash University, shifted the conversation about cybersecurity to focusing on the individual as part of a whole system. A human factors researcher, she has studied how individuals fall victim to scams, with romance scams being one of her areas of concentration, telling a fascinating anecdote about an unhappily married woman meeting a man on social media who needed some money, who then sold her details to another group, who tricked her into going to China to sign off on some papers. Her work exposes the serious vulnerabilities of individuals to deceptions online. She addresses these issues by trying to raise awareness but also changing behaviours that lead to these problems (Whitty and Buchanan 2012). The Serious Organised Crime Agency (SOCA) instituted a project to address mass marketing scams creating international forums that fostered more communication about the issue, but it also demonstrated how important it was to understand the drivers of crime. The poverty and inequality that fosters criminal activity is necessary to approach as a multidisciplinary problem. But the challenge of addressing the psychology of victims is also huge, but you can help people feel they are part of the solution by listening and understanding their perceptions.

Barbara Grewe began her intervention by appreciating being back in Oxford, which she amusingly characterised as the "Disneyland for Academics". She quickly brought us to key questions about the government's role in cybersecurity. Noting that 9/11 exposed a hole in national security, it also served to raise questions about cyberattacks. Did we need new frameworks? One of her major points was that CCB should be seen as a common good. How does the cybersecurity of a foreign country affect you? She explained that malicious actors do not go directly into their target country, but often go through a weak country to get into a safer country. That is one example of why we do cybersecurity capacity building – it is one part of active cyber defence. But clarity of advice is critical and effective cooperation is needed between partners to make sure that the advice is consistent.



Session 2: Observations

Trust Building: Implementing CBMs in Cybersecurity enhances capacities and trust among stakeholders. The CMM is suggested as a methodology to assess the effectiveness of these programs.

Research and Training: Efforts are being made to centralise research activities both regionally and inter-regionally. This includes behavioural analysis, awareness-raising, and training to understand how individuals are affected by fraud.

Intersection of Security Domains: Cybersecurity is at the intersection of national and economic security, affecting both areas significantly. This dual impact raises the need for pursuing CCB and the government's role in it. Cybersecurity is considered a common good, impacting everyone.

Local Context and Multi-Stakeholder Approach: One size does not fit all; local context is crucial when building CCB. Understanding the environment for CCB efforts is challenging, but CMM Dimensions can help. The solution is multi-stakeholder and multi-disciplinary.

Coordination and Collaboration: Coordination and collaboration are vital for building national cybersecurity strategies. Sub-regional coordination, supported by cultural commonalities and understandings, aids states in crafting these strategies. Engagement and tailored approaches are necessary. Providers of CCB need to communicate and collaborate with each other to ensure consistency of guidance and implementation when different providers act within the same country.

Global Cyber Resilience: Countries with weak cyber resilience pose threats to their partners, acting as weak links in global infrastructure. There are ongoing discussions about whether states can mandate and impose cybersecurity standards on other countries.

Defining Success: Questions persist about what success in CCB looks like and the metrics for it. One key aspect is fostering the right mindset and attitude in member states.

Information Sharing and Cultural Impact: CBMs facilitate information sharing on critical areas and vulnerabilities. Cyber issues are intertwined with other development areas such as poverty, with cultural factors playing a significant role.

Planning and Roadmaps: A phased approach with established baselines and risk registers can improve efficiencies and impact. Meeting countries where they are and understanding their national context is essential.

Political and Psychological Barriers: Political engagement is a significant barrier to CCB efforts. Democracies are often in flux, with personnel changes impacting projects. Medium to long-term timelines should be considered, as there is currently an overemphasis on short-term impact work.

Mindset and Recipient-Centric Approach: Mindset can be a barrier, with a need to prioritise listening and understanding recipients over imposing solutions.

Session 3: Improving the Evidence-base for Capacity Investments

The third panel was chaired by Jamie Saunders, Oxford Martin School Fellow and Technical Board Member of the GCSCC. The speakers were: Nick Beecroft, International Cybersecurity Lead, BAE Systems Digital Intelligence; Anat Lewin, Senior Digital Development Specialist, World Bank; Nick Moore, Senior Expert, Integrity; and Caroline Troein, Cross Thematic Programme Officer, International Telecommunication Union (ITU).

The panel was motivated by a concern that countries across the world invest significant sums in CCB but are often left without direct evidence of the strategic impact of these interventions on measures of societal, economic or national security benefit (such as the SDGs). A lot of work has been done to analyse the linkages between cybersecurity and these higher-level national impacts, but many believe that more is required. How can we improve our community's ability to demonstrate the strategic impact of cybersecurity capacity building? What are the challenges in doing so? This panel explored the challenges currently facing the monitoring and evaluation of CCB programs, informed by the application of Theories of Change and disciplinary methodologies from development assistance and other professions. The discussion addressed the impact of monitoring and evaluation on return on investment and other economic valuations of CCB programs, the challenges facing MEL efforts such as data availability, and conceptually analysing CCB efforts as complementary to the SDGs. A side event at the conference focused on building a community and developing solutions for CCB Impact Evaluation (Box 4).

Workshop on Improving Cyber Capacity Building (CCB) Evaluation Practice: Road to GC3B Geneva 2025

This side event for the conference was organised by the GCSCC, Integrity and Royal Holloway University London Information Security Group in support of the GFCE's Strategy and Assessments Working Group. It discussed some of the challenges and potential solutions in evaluating impact of CCB. The team presented the four pillars of the project: theory (understanding of how CCB is expected to work), Data (understanding what data can be used to measure theory and context), methodology (understanding how to use theory and data to make evaluative judgements), and use (case studies on the use of evaluation evidence to systematically improve CCB policy and practice). With respect to theory, the P-I-O framework, which is commonly used in International Development context, was suggested as a useful approach to CCB. With respect to data, there was support for more of an understanding of what data can be drawn on to monitor outcomes, especially data beyond implementer perceptions. In terms of analysis, the group raised several challenges around the use of analysis to identify CCB effects but saw a value to clear examples of analysis applied to CCB contexts. On use, there was broad agreement to support use of evidence to inform CCB, even though the CCB community may not use or refer to evidence in the same way as other sectors.

Several participants suggested that the term evidence may not be a term CCB practitioner use to refer to evaluation, with evidence referring more towards evidence of crime.

Anat Lewin with the World Bank noted that her organization funds $220M of lending for cybersecurity activities each year, amounting to about four percent of the Digital Development's lending budget. This presently supports activities in 56 countries. Their focus is on the development of national cybersecurity strategies, creating cybersecurity agencies and action plans, supporting the development of incident response capacities through CERTs and Computer Security Incident Response Teams (CSIRTs), and industry and public awareness raising. If a country does not have a CMM assessment, they will consider supporting one if the country is interested. Anat spoke about the scarcity of cybersecurity data to support informed decision-making and research/analytics in the field. She called for the cybersecurity for development community to work together to support the standardization of definitions, the creation of consensus-based methodologies and the provision of assistance to developing countries with statistical capacity building so that data on cybersecurity can be collected in a comparable fashion across countries.

Caroline Troein with the ITU followed, reminding us of their mission statement: to connect the unconnected. The ITU focused on supporting global connectivity and, as others in the early days of the internet, were not thinking about how people are safe and secure online. However, they see cybersecurity, like the Internet and AI, to be an enabler across many sectors and activities. ITU cannot support connectivity and cybersecurity alone. They need developed countries to take responsibility for many of these issues. They also produce the Global Cybersecurity Index (GCI). Many use this data, and want to know how it is evolving, leading to many workshops and information campaigns. To explain what we are doing and what we are trying to measure, we need to tell a story.

Nick Beecroft with BAE Systems Digital Intelligence followed Caroline. He has been involved in cybersecurity capacity business programmes which address many of the questions surrounding evidence-based assessments. He made a distinction between an impact and its outcome, suggesting than

a one-year impact might lead to an outcome over a five-year period. In cybersecurity, it is relatively easy to measure impact (e.g. enhancements to the security of national infrastructure), but much harder to measure the outcome (e.g. what difference does that security improvement make to national resilience), which is the key evidence for capacity-building investments. This lead-lag problem is exacerbated by problems with the data and its measurement. The adoption of capacity-building approaches such as the MREL process and results framework have required Nick and his colleagues to learn new methods to ensure they apply rigour in trying to capture impacts and outcomes. So progress is happening, but there's much more to learn about how to capture and measure the ultimate benefit of cyber capacity building.

Nick Moore, an economist with Integrity, has previous experience as an expert at the International Initiative for Impact Evaluation (3ie), all key to this panel. He noted that development and cybersecurity capacity building are a two-way street – they each support the other. That said, evidence is difficult to marshal for making any causal claims. Natural experiments are nearly impossible to fund and implement in this area. He did implore the community to be question-led. The data gathered should be shaped by the question. He emphasized the value of a broader approach to measuring key outcomes of interest. This includes drawing on more granular measures of threat detection and response commonly used by IT departments and CSIRTs. The sector is fortunate that lots of high frequency data exists, so – he argues – let's start documenting the opportunities and challenges in using this, like our World Bank colleagues have done with a focus on mobile data.

Discussion added to these points in a variety of ways, but a key theme was the difficulties in collecting good data. Data from public records that could be informative, like data on mobility available in 42 countries that could be useful to predict outbreaks, such as around COVID-19, are simply not available. Many other data sources are simply insufficient, fragmented, of questionable integrity, not harmonized across countries or overtime, and so forth. Cross-nationally, there are often differences in the definition of the same terms as well as how they are measured. It is a very difficult problem. Perhaps when the government or other organizations support a country, they should come up with key performance indicators (KPIs) for each, so its impact could be gauged. But governments can only record or collect the funding and project level impacts, not the longer-term outcomes.

Session 3: Observations

Resource Collaboration: Organisations lacking resources or expertise rely on partners to meet their clients' needs within available timelines.

Improvement and Measurement: Establishing the appropriate timing for measuring results after interventions is crucial for achieving meaningful insights. Emphasis is placed on understanding impacts and outcomes over the short and long term, from immediate outcomes to five-year impacts.

Cross-Disciplinary Approaches: Lessons from development assistance programs and other professional disciplines can help understand impacts.

Monitoring, Evaluation and Learning (MEL) should go beyond being a mere tick-box exercise, focusing on prioritisation and rapid problem-solving in critical environments.

Shared Challenges and Bidirectional Relationships: Cybersecurity is recognised as a shared challenge, with a bidirectional relationship between development and capacity building.

Scientific Methods and Data Challenges: Different data methods and the scientific method vary by question and project, with ongoing struggles to produce useful insights. Project evaluations often rely on untestable theories, with debates on appropriate MEL theories that sometimes overlook key questions.

SDGs and Cybersecurity: Connecting SDGs and CCB efforts is appropriate; absent cybersecurity, many harms prevent achieving SDGs. Evaluation and analysis can reinforce these connections.

Data Gaps and Integrity: Identifying data gaps and ensuring data integrity is crucial. Data availability and consistent reporting remain significant challenges.

Rethinking the conceptualization of return on investment (ROI) for cybersecurity programs is necessary. High-level assumptions impact how CCB efforts quantify ROI.

Economic Justifications: The economic rationale for investing in cybersecurity often focuses on GDP loss and performance metrics. Can we develop other indicators?

Data Ownership and Privacy: Measuring and analysis of programs and outputs requires managing the owner of the data, but many programs and portals do not own the data available. Yet, managing data ownership is essential for measuring and analysing program outputs. Many programs and portals do not own the data they utilise, further complicating these efforts. Initiatives must balance security with other values, such as public safety and individual privacy.

Session 4: Evolving Meaningful and Sustainable Partnerships for Cybersecurity

The day's final panel was chaired by Ciaran Martin, Professor of Practice in the Management of Public Organisations, Blavatnik School of Government, University of Oxford. His speakers were: Viv Danks, Director, Solutions Architect, Palo Alto; Gigi Flores Bustamante, Future of Digital Security Analyst, Institute for Security and Technology (IST); Tal Goldstein, Head of Strategy, Centre for Cybersecurity, World Economic Forum; Tereza Horejsova, Senior Outreach Manager, Global Forum on Cyber Expertise (GFCE); and Carsten Rudolph, Deputy Dean at the Faculty of Information Technology, Monash University/Melbourne, and Director for Research, Oceania Cyber Security Centre (OCSC). The panel was asked for examples of effective partnerships they have we observed, what works well and when are there critical capability gaps? Which public and public-private partnerships are needed and is new policy required to ensure they succeed?

Tereza Horejsova with the GFCE led off saying that the need for cooperation seems too simple, too common sensical. However, if everyone acted for themselves there would be clear duplication and inefficiency, when resources are already inadequate. People have to understand that more cybersecurity capacity building will mean more cyber resilience and therefore have major economic payoffs.

Carsten Rudolph from Monash University, Melbourne, and the OCSC began with an example of partnering on the provision of undersea cables to support connectivity for Pacific island nations with one another and with Australia, Latin America and the US. The capacity of cable systems and their costs Impressed on the Pacific island nations the importance and effectiveness of a regional approach. Nevertheless, there are major challenges in sharing facilities and expertise. Moreover, while Pacific Island nations are aware of cybersecurity and the geopolitics of the region, these issues are not considered to be as immediate as such critical issues such as climate change and its existential threats to the Pacific as a region, which is one of the most vulnerable in the world to its effects. In his talk, Carsten shared his experience working on the conduct of CMM reviews with the OCSC in the Pacific context, and on the development of the OCSC Roadmap, which provides a phased approach to implementing the recommendations of a CMM within the contexts of these island nations limited resources and competing priorities.

The WEF's Tal Goldstein then focused on the divide between nations in maturity levels. He also spoke to the increasing divides between companies. [A side event at the conference focused on the difficulties of small and middle-sized enterprises (SMEs) acquiring the time and expertise to deal with cybersecurity, see the David & Goliath Workshop] Cisco is a US company with many global partners. National sovereignty concerns can lead to isolated ways of solving problems, but they are simply not as effective as strong partnerships. Different industrial sectors have unique issues, such as finance and food chains, which are completely different from cybersecurity. A relevant initiative is the Cyber Threat Alliance – 'by industry for industry', sharing cyber threat information among companies and organisations. At the centre of this alliance is the ethos: You can't just be a collector, you need to share. 'You can't take if you don't give'.

Gigi Flores Bustamante of the IST spoke on research focused on public-private partnerships to address ransomware attacks. IST organised the Ransomware Task Force (RTF) as a multistakeholder initiative involving government, industry, and civil society partners, which has provided numerous recommendations for combatting ransomware, many of which have been implemented by partners. The research on public-private partnerships to combat ransomware was an outcome of the 2022 Counter Ransomware Initiative. Its purpose is to serve as a cyber capacity building tool for governments looking to either improve existing partnerships or initiate new ones. There are questions about what partners get out of these partnerships but there is an eagerness to participate, particularly from the private sector, creating an opportunity for collaboration for government-led public-private partnerships.

Viv Danks, Director, Solutions Architect, PaloAlto Networks, focused on data sharing, suggesting that there have been moves away from supply-driven capacity building to more demand-driven capacity building, such as created by ransomware attacks. His organisation recommends five actions to increase cyber resilience to ransomware attacks, which include: maintaining an incident response plan, ensuring complete visibility of attack surfaces, leveraging the power of AI and automation to modernise security operations and reducing the burden on overworked analysts, and implementing enterprise-wide Zero Trust network architecture, and protecting cloud infrastructure and applications.

Cybersecurity in Ukraine, particularly in the context of lessons learned about public-private partnerships, became a focus of discussion. For example, it was argued that informal contacts came to matter more than formal contacts, such as in public-private partnerships, as they built a strong level of trust in moving forward. As much as many tech companies want to make the crisis in Ukraine 'not happen', partnering needs to focus on engaging the relevant actors. You need to be able to answer questions about why you are gathering people together. But in Ukraine and elsewhere there is a basis for optimism as it is bringing partners together. SPAM used to be a major problem, but now we have systems to block SPAM. The SPAMHAUS Project protects billions of user mailboxes. Live Virtual Classes (LVCs) can be provided internationally. CyberGirls provides opportunities for girls and women across Africa to acquire skills in cybersecurity and safety. Recent history provides many grounds for optimism in countering new forms of cyber-attacks

Session 4: Observations

Enhancing CCB is essential for improving global cyber resilience, such as the continuity of business processes.

Coordination can support CCB by leading to more efficient, effective, and improved outcomes. Pooling limited resources can create a greater impact, particularly for developing countries. Discussion of the case study in the Pacific suggests that a regional approach is crucial for managing diverse development levels and resource availability.

Data Ownership: Who owns data is complex, often involving multiple claims. Data is managed by custodians, not the owners, complicating permissions management for individual data owners. Shared experiences and priorities within and across organisations can bridge concerns over issues such as trust and privacy.

Managing Priorities:
Building partnerships is valuable but time-consuming, requiring careful management of competing priorities. Cybersecurity competes with other major regional priorities, like climate change and geopolitical issues. But there are inequalities. While large companies show improvement in cyber maturity, smaller companies are less likely to have the expertise and resources to keep up. Maintaining cybersecurity awareness and literacy is challenging in all companies, due to the rapidly evolving threat landscape, but particularly difficult is smaller enterprises. Despite the shared nature of cyber threats, an isolationist approach persists. There can be serious conflicts between national sovereignty and the need to share knowledge to combat threats. Specialised interest and sectoral groups can effectively share data if they build a trusting environment.

It's crucial to understand the appropriate contexts for partnerships to succeed, such as the success of partnerships for Ukraine. Determining the optimal point to involve private capabilities and managing the relationship between public, private, and non-profit actors is challenging.

Public-Private Dynamics: Informal contacts can be as effective as formal ones in forging public-private partnerships.

Summary and Conclusions

The concluding session for the day began with a brief personal perspective from Joanna LaHaie, Director for International Engagement & Capacity Building in the Bureau of Cyberspace and Digital Policy in the US Department of State.

She began by recounting her early experience as a Peace Corps Volunteer in the education sector. She recalled commenting on the deficiencies in the local schools she had been working in as a volunteer when a more experienced local colleague responded by noting that less than a decade before there were no schools in this area. There had been great progress, but still work remains to be done.

She used this poignant example to congratulate the cybersecurity community on its progress over the past ten years, but also reminding all that much work still needs to be done. GCSCC has done much in developing the categories of cybersecurity capacity building and its CMM and identifying gaps in capacity-building initiatives, some of which have been filled, such as by the creation of the GFCE, focused on fostering international collaboration for strengthening cyber capacity and expertise worldwide. From her perspective, there had been a number of major wake up calls around cybersecurity, such as the NotPetya ransomware attack, successful initiatives from the Open-Ended Working Group (OEWG), the COVID-19 pandemic, and the war on Ukraine, which has literally changed what cybersecurity means. These dramatic events have raised the priority for CCB and built a lot of momentum behind collective defence.

She closed her brief talk with an analogy, comparing a bully picking on a small kid in the playground versus a bully facing a bunch of kids who come together to protect the small kid from the bully. In many ways, she saw the Russian War on Ukraine to have created more solidarity across the world for many nations, particularly the NATO members, to work together in supporting Ukraine. Paraphrasing Benjamin Franklin's famous quote, she suggested nations are realising that we need

to stand together, or we stand alone. Collective defence has been more effective in response to malicious actors. This seems to be the need going forward: to have a more collective and integrated approach to assistance on big issues, such as cyber, space, and digital policy, recognising these issues are closely connected and require an internationally integrated approach for security.

What we want and need to do to support capacity building is expensive. Increasingly, we need shared investment – a pooling of resources, more partnerships, as we have done in Ukraine. We need a shared purpose to win the war, and to tackle cybersecurity capacity building. But having done this with Ukraine, we should have more confidence that we can do it elsewhere. In the US, it feels like there is a new definition of "we" as we move forward.

Professor Sadie Creese thanked Joanna LaHaie for providing such an inspirational vision for the cybersecurity community. She thanked all the speakers and participants of the conference for their ideas and contributions to the day urging all of us to build a collaborative vision for policy and practice. The GCSCC will continue to pursue key questions, so Professor Creese asks: What are the options we should be exploring? How can they be made more effective, and what is the cooperation and collaboration agenda we should be following?

She ended by returning to the Lewis Carroll's quote of the Red Queen that our keynoter, Heli Tiirmaa-Klaar reminded us of: "My dear, here we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that." - Lewis Carroll,"Through the Looking Glass"

Appendices

1 The Conference Agenda

2 The Conference Participants

3 Partners and Sponsors, and Funders of the GCSCC's CMM

4 List of Acronyms and Abbreviations

5 Sources Referenced in the Report

Appendix 1: Conference Agenda

GCSCC 10th Anniversary Conference - Agenda

Our Annual Conference returns to the Oxford Martin School, University of Oxford, on Tuesday, 30 April, 2024, marking the GCSCC's 10th anniversary!

Cyber-threats continue to rapidly evolve, particularly amid geopolitical instability, enhanced digital attack capabilities, and growing inter-dependencies and vulnerability throughout supply-chains and our critical infrastructures. Pre-positioning of malware and insider threats must be assumed. At the same time, we are witnessing massive progress towards AI-futures. Associated digital technologies and the Internet of Things (IoT) is becoming pervasive, with quantum and space innovations expected to follow in quick succession. The cyber capacity community needs to deliver responses to enhance cyber-resilience in the face of continued capacity deficits in the global workforce. What should be the community's priorities in cybersecurity capacity building? What are the principle risks moving forward?

9:30 Registration, coffee and tea

10:00 Welcome and Introduction
Sadie Creese, Professor of Cybersecurity and Director of the Global Cyber Security Capacity Centre (GCSCC), University of Oxford

10:15 Keynote: "The need to change the Cybersecurity Capacity Building narrative".
Heli Tiirmaa-Klaar, Director, Digital Society Institute at European School of Management and Technology (ESMT)

10:45 Panel Opening, Discussion I: Emerging risks and challenges for cybersecurity.
How is digital technology evolving and what are the cyber-risk scenarios that must be prioritised for future cyber-resilience? What are the opportunity costs of inaction, and the harm consequences at all scales from global networks to regions, nations, individuals and businesses? Are we responding to the evolving mission to protect people, deliver safety, support human rights and the ability for self-determination and sovereignty?

Chair: Sadie Creese, Professor of Cybersecurity and Director of the GCSCC

Speakers:

- John Mallery, Research Scientist, CTO, WFA Group
- Stephen Roberts, Professor of Machine Learning, University of Oxford
- Heli Tiirmaa-Klaar, Director, Digital Society Institute at European School of Management and Technology (ESMT)
- Paul Trueman, Executive Vice President, Cyber & Intelligence, Mastercard

11:45 Coffee and tea

12:00 Panel Discussion II: Cybersecurity regulation and governance through a regional and international lens: Will one size fit all?
Do we risk cyber inequities and security divides? What are the specific needs for developing economies? Can a multi-stakeholder approach facilitate a more globally equal response? What are the barriers that we face and how should we work together to address them more effectively?

Chair: David Wall, Chair in Criminology, University of Leeds, Oxford Martin School Fellow and Technical Board Member of the GCSCC

Speakers:

- Violanda Botet, Deputy Executive Secretary for the Inter-American Committee against Terrorism (CICTE) at the Organization of American States (OAS)
- Enrico Calandro, Board Member, Cybersecurity Capacity Centre for Southern Africa (C3SA)
- Barbara Grewe, Senior Principal International Policy and Strategy at The MITRE Corporation
- Szilvia Toth, Cyber Security Officer, Organization for Security and Co-operation in Europe (OSCE)
- Monica Whitty, Head of Department of Software Systems and Cybersecurity and Professor of Human Factors in Cyber Security, Monash University/Melbourne

13:00 Lunch

14.15 Panel Discussion III: Improving the evidence-base for capacity investments.

Countries across the world invest significant sums in cybersecurity capacity building (CCB) but it remains a challenge to directly evidence the strategic impact of these interventions on measures of societal, economic or national security benefit (such as the Sustainable Development Goals). A lot of work has been done to analyse the linkages between cybersecurity and these higher-level national impacts, but more is required. How can we improve our ability to demonstrate the strategic impact of cybersecurity capacity building? What are the challenges in doing so?

Chair: Jamie Saunders, Oxford Martin School Fellow and Technical Board Member of the GCSCC

Speakers:

- Nick Beecroft, International Cybersecurity Lead, BAE Systems Digital Intelligence
- Anat Lewin, Senior Digital Development Specialist, World Bank
- Nick Moore, Senior Expert, Integrity
- Caroline Troein, Cross Thematic Programme Officer, International Telecommunication Union (ITU)

15:15 Coffee and tea

15:30 Panel Discussion IV: Evolving meaningful and sustainable partnerships for cybersecurity.

What examples of effective partnerships have we observed, what works well and when are there critical capability gaps? Which public and public-private partnerships are needed and is new policy required to ensure they succeed?

Chair: Ciaran Martin, Professor of Practice in the Management of Public Organisations Blavatnik School of Government, University of Oxford

Speakers:

- Viv Danks, Director, Solutions Architect, Palo Alto
- Gigi Flores Bustamante, Future of Digital Security Analyst, Institute for Security and Technology (IST)

- Tal Goldstein, Head of Strategy, Centre for Cybersecurity, World Economic Forum
- Tereza Horejsova, Outreach Manager, Global Forum on Cyber Expertise (GFCE)
- Carsten Rudolph, Deputy Dean at the Faculty of Information Technology, Monash University/Melbourne, and Director for Research, Oceania Cyber Security Centre (OCSC)

16:30 A vision for policy: What are the options we should be exploring? How can they be made more effective, and what is the cooperation and collaboration agenda we should be following?

Chair: Sadie Creese, Professor of Cybersecurity and \ Director of the GCSCC

17:00 Informal Drinks

Appendix 2: The Conference Participants

AFRICOM

Aspen Institute

BAE Systems

Brunskill Security Consulting (BSC)

Cente Tech

Chiba Institute of Technology - Henkaku Center

Cisco

Commonwealth Telecommunications Organisation (CTO)

Cranfield University (Chevening Cyber Security Programme)

CREST

Cyber4Dev

CyberEye

European School of Management and Technology (ESMT)

FIRST

Genesis Analytics

Global Forum on Cyber Expertise (GFCE)

India Future Foundation

Institute for Security and Technology (IST)

Integrity

International Association of Prosecutors

International Telecommunication Union (ITU)

KH Consulting

KPMG UK

Massachusetts Institute of Technology (MIT)

Mastercard

Michigan State University

Microsoft

Ministry of Posts, Telecommunications & Technology Somalia

Monash University

National Policy Agency

National Cyber Security Centre, Switzerland

NetHope

Nihon Cyber Defence

NIKKEI, Inc.

NRD Cyber Security

Oceania Cyber Security Centre (OCSC)

Organisation for Security and Co-operation in Europe (OSCE)

Organization of American States (OAS)/CICTE

Palo Alto Networks

Protection Group International (PGI)

Royal Holloway University London

Royal United Services Institute for Defence and Security Studies (RUSI)

Templar Executives

Tony Blair Institute for Global Change

Toshiba Corporation

U.S. Department of State

UK Foreign, Commonwealth and Development Office (FCDO)

United Nations Office for Disarmament Affairs (UNODA)

University of Cambridge

University of Johannesburg

University of Kent

University of Leeds

University of Oxford, Blavatnik School of Government

Appendix 3: Partners and Sponsors, and Funders of the GCSCC's CMM (in alphabetical order)

Commonwealth Telecommunications Organisation (CTO)

Gesellschaft für Internationale Zusammenarbeit (GIZ)

Global Forum on Cyber Expertise (GFCE)

Inter-American Development Bank (IDB)

International Telecommunication Union (ITU)

Japan International Cooperation Agency (JICA)

Microsoft

Norway

Norwegian Institute of International Affairs (NUPI)

NRD Cyber Security

Organization of American States (OAS)

State Government of Victoria (Australia)

The Netherlands

UK Cabinet Office

UK Foreign, Commonwealth & Development Office

World Bank

Appendix 4: List of Acronyms and Abbreviations

AI	Artificial Intelligence
C3SA	Cybersecurity Capacity Centre for Southern Africa
CCB	cybersecurity capacity building
CERTs	Cybersecurity Emergency Response Teams
CICTE	Inter-American Committee against Terrorism
CMM	Cybersecurity Capacity Maturity Model for Nations
CBM	Confidence-Building Measures
CSIRTs	Computer Security Incident Response Teams
CTO	Chief Technology Officer
ESTM	European School of Management and Technology
EU	European Union
GCSCC	Global Cyber Security Capacity Centre, University of Oxford
GCI	Global Cybersecurity Index
GDP	Gross Domestic Product
GFCE	Global Forum on Cyber Expertise
IO	International Organisation
IST	Institute for Security and Technology
ITU	International Telecommunication Union
LVC	Live Virtual Classes
MEL	Monitoring, Evaluation and Learning
NASA	National Aeronautics and Space Administration
NUPI	Norwegian Institute of International Affairs
OAS	Organization of American States
OCSC	Oceania Cyber Security Centre
OEWG	Open-Ended Working Group
OMS	Oxford Martin School, University of Oxford
OSCE	Organization for Security and Co-operation in Europe
RIA	Research ICT Africa
RMCS	Roundtables on Military Cyber Stability
ROI	Return on Investment
RTF	Ransomware Task Force
SOCA	Serious Organised Crime Agency
SDGs	Sustainable Development Goals
WFA	Wayne Frederick and Associates (WFA) Group

Appendix 5: Sources Referenced in this Report

Bispham, M., Creese, S., Dutton, W. H., Esteve-Gonzalez, P., and Goldsmith, M. (2022), 'An Exploratory Study of Cybersecurity in Working from Home: Problem or Enabler?', *Journal of Information Policy*, 12 (May), https://doi.org/10.5325/jinfopoli.12.2022.0010

Creese, S., Dutton, W. H., and Esteve-González, P. (2021), 'The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions, *Personal and Ubiquitous Computing*, 25, May, 941-955: DOI: https://doi.org/10.1007/s00779-021-01569-6.

Creese, S., Dutton, W. H., Esteve-González, P., and Shillair, R. (2021), 'Cybersecurity Capacity Building: Cross-National Benefits and International Divides', *Journal of Cyber Policy*, 6(2), 214-235. Available at: https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1979617

IDA & OAS (2020), Cybersecurity: Risks, Progress, and the Way Forward in Latin America and the Caribbean. The Inter-American Development Bank (IDB) and Organization of American States (OAS). Available at: https://cybilportal.org/publications/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean/

Wall, D. S. (2024), *Cybercrime: The Transformation of Crime in the Information Age*, 2nd Edition. Cambridge: Polity Press.

Whitty, M. T., and Buchanan, T. (2012), 'The Online Romance Scam: A Serious Cybercrime', *Cyberpsychology, Behavior, and Social Networking*, 15(3): https://www.liebertpub.com/doi/10.1089/cyber.2011.0352

Thank you for reading to find out more visit: **gcscc.ox.ac.uk**

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

#gcscc2024

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

10 YEARS

RESEARCHING CYBERSECURITY CAPACITY FOR THE EMERGING CYBER FUTURE