Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Collaborative Approaches to a Wicked Problem:

Global Responses to Cybersecurity Capacity Building

February 2018

Preface and Acknowledgements

This report aims to convey the key themes that arose in the Annual Conference of the Global Cyber Security Capacity Centre that was held at the Lecture Theatre, Oxford Martin School, Old Indian Institute, 34 Broad Street, University of Oxford, Oxford, on 6 February 2018. It was a working meeting, held with the objective of producing an output that would recognise the challenges for capacity building to become more strategic and global and to propose ways to help overcome these challenges. Comments on this report are invited from all the participants and the larger community involved in cybersecurity. We hope this report helps you join this endeavour.

Convened under the Chatham House Rule, no quotes are attributed to any individual. We thank all the speakers and participants who have helped shape this report. Appendix 1 provides a summary of the agenda, which identifies speakers, and Appendix 2 lists all of those who attended and contributed to the content of this paper. Appendix 3 provides a list of acronyms and abbreviations used in this report. Appendix 4 lists the sources referenced in the report.

Introduction

There has never has been a more urgent time to invigorate and embrace the need to secure cyberspace for all – where "cyberspace" is used metaphorically to refer broadly to the network of systems and devices that are linked via the Internet (Clark, Berson, & Lin, 2014: 2). In recognition of the efforts and the progress made by a growing international community in cybersecurity capacity building, the GCSCC dedicated its 2018 Annual Conference to the question: How can the community become more strategic and more collaborative in building cybersecurity capacity?

Work in this area has advanced to the point at which discussion can move beyond efforts to coordinate national investments in cybersecurity capacity building and towards a more meaningful global-oriented approach. Nationally and globally, there is a need to ensure that the combined investments of resources around the world, whether intellectual or monetary, result in the greatest gains for the global community.

This report first provides a brief summary of the sessions, focusing on the key questions driving discussion. It then moves to a set of cross-cutting and overarching themes of the day's discussions. Throughout, the report seeks to clarify terminology and actors in order that individuals not directly immersed in capacity building efforts can follow and learn from in this report.

Key Topics and Questions

The chair of the conference, Professor Michael Goldsmith, opened the day by outlining the objectives of the organising committee. The aim was not to focus on the achievements of the Global Cyber Security Capacity Centre (GCSCC).[1] Instead, the aim of this year's conference was for the international community to look at the big picture in order to identify the major questions arising around capacity building practices, capture key challenges the community has been facing, and propose solutions. This report seeks to identify the challenges identified on the day, and critically discuss the solutions proposed.

The conference's sessions were devoted to four topics: **achievements, challenges, implementation, and the future of capacity building**. The following sections provide a brief review of the sessions before moving into an overview of the major themes and issues raised during the day.

Achievements: Building a Globally Strategic Response to Cybersecurity

The first session was asked to address two questions: What are we achieving in cybersecurity capacity building? How are we investing our resources? Paul Cornish of the Global Cyber Security Capacity Centre (GCSCC) chaired this first session that began with presentations from Deputy Chief Executive Mr NG Hoo Ming, CSA Singapore and Robert Collett of the UK's Foreign & Commonwealth Office (FCO). Each speaker reflected on achievements and investments in this area, which led to

[1] Project overviews are available online at https://www.oxfordmartin.ox.ac.uk/cybersecurity/

discussion of these issues by conference participants, along with a wider range of questions and comments.

There was a general sense that the global cybersecurity capacity building community had made significant strides over the years, with a range of national, regional, and global collaborations driving positive assessments and subsequent investments in cybersecurity capacity projects across the world. Nevertheless, some enduring questions remained, such as the very basic issue of what can be done to enhance capacity building? What has been learned over the years across this global community? Are cybersecurity capacity resources currently invested in a way that is reducing cybersecurity risk? Are they being coordinated within and across nations, but also across multiple sectors and actors from the donor community to cybersecurity organisations? How are short- and long-term investments linked to sustained development?

Challenges

The second session focused on the key challenges, such as the difficulties of coordinating investments more strategically across the global community. General questions of this session were: What are the barriers to a strategic global response? How do we coordinate strategic investment across the community? One speaker characterised this challenge broadly as how can we move a system of sovereign nations anchored in the Westphalian contract of 1648 to the realities of a twenty-first century problem requiring global collaboration? This session was led by Sadie Creese, the Founding Director of the GCSCC, with talks by Heli Tiirmaa-Klaar of the European External Action Service and David Satola of the World Bank.

One of the central themes was around the interaction of local and global responses. While we think of cyberspace as a metaphorical global village with a diverse range of actors, it is clear that investment remains national. This session sought to identify and understand the current barriers to a more coordinated global response to cybersecurity capacity building, with a view to a clear and pragmatic pathway forward. This included discussion of the opportunities there are to improve the return on investment of projects through better coordinated systems and better metrics to access their outcomes.

Collaboration

A working lunch session, chaired by Professor Basie von Solms, was dedicated to identifying innovative ideas for collaboration. The session focused on the case of the African region and the value of regional reviews, and the value of best practice examples to understand the unique needs of this region and to avoid needless duplication. Public awareness campaigns, and the development of cybersecurity norms across society were also discussed; as were possible differences in the roles of public awareness, public education, and literacy in shaping cybersecurity.

Implementation

The third session shifted focus to the concrete issues of implementing national and global strategies. What are the obstacles and limitations to strategy implementation? How can we overcome these? Kerry-Ann Barrett of the Organization of American States chaired this session, which carried on with the discussion of barriers to strategy and implementation across the community. Discussion was initiated through talks from George Michaelides, Commissioner of Electronic Communications and Postal Regulation in Cyprus, and Johanna Vazzana of the MITRE Corporation.

Discussion surfaced issues surrounding the key driving forces behind cybersecurity capacity building, and how these varied across the multiple actors involved at each level of governance and implementation. The session addressed the need for the community to do more to explore each nation's capacity to absorb and find utility in short term capacity building projects and how to ensure that these projects can cumulatively build on one another and result in a broader vision and strategy. This in turn led to discussion of the fit between plans and resources (especially human resources) in implementing coordinated and well-thought out capacity building strategies that have already been adopted.

The Future of Capacity Building

The fourth session provided an opportunity to synthesise and reflect on issues raised throughout the day and consider what implications they might have for the future of cybersecurity capacity building. Questions arose over several challenging issues, such as how to set global priorities based on regional cybersecurity capacity reviews and risk assessments? Sadie Creese, the chair of this session, and founding Director of the GCSCC, launched this discussion by providing her vision of how the GCSCC could evolve in the coming years.

Professor Creese's vision was complemented by Bill Dutton's presentation of an up-date of the GCSCC's analysis of the significance of capacity building, which empirically shows that capacity building does matter in shaping the problems faced by end-users, such as indicated by security products reporting malware, the number of computers infected, and the proportion of pirated software. All of these indicators are correlated, suggesting they each approach aspects of the same underlying problem, but there is a need to develop further indicators that enhance the reliability and validity for measuring levels of end-user problems.

Box 1. The Global Forum on Cyber Expertise (GFCE)

The GFCE Global Agenda for Cyber Capacity Building builds upon themes of cyber capacity building. Each theme constitutes an important foundation for national, regional, and global cyber security developments. They are closely related and constitute key foci for cyber capacity building efforts as identified by the GFCE and are mutually reinforcing.

- Cyber Security Policy & Strategy
- Incident Management & Infrastructure Protection
- Cybercrime
- Cyber Security Culture & Skills
- Cyber Security Standards
- Crosscutting Capacities

See: https://www.thegfce.com/gfce-global-agenda/gaccb-themes

The GCSCC plans to build on this analysis by incorporating the centre's field research more directly into the analysis. Sadie Creese's presentation was further augmented by David van Duren of the Global Forum on Cyber Expertise (GFCE), who described the Forum's approach to building a global platform for countries, international organisations and private companies to exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level'.[2] The GFCE (see Box 10) will be working with partners from academia, including the GCSCC and from NGOs and the technical community to build cyber capacity. In many respects, the GFCE assumes that the future of capacity building will require more collaboration to succeed.

This final session was followed by Professor Michael Goldsmith, who returned to close the conference, making several key points of summary and conclusion. He ended by thanking all the participants for their contributions to a productive day of discussion.

The next section of this report identifies some of the key themes and issues that arose through the day of discussions across all of the sessions.

Major Themes and Issues

The Centrality of Cybersecurity and a Strategy for Capacity Building

The first and all subsequent sessions reflected a strong consensus that cybersecurity is a vital objective at all levels, from individuals and households in local communities to the global community. Many argued that cybersecurity is seldom viewed as a goal in itself – simply for its own sake, rather than to achieve the benefits of security. However, one presenter noted that there are strong arguments for a 'need for safety in cyberspace' as an end in itself – comparable to public safety generally, as well as a means to many other societal goals, such as social and economic success, or our very standard of living (see Box 2). For example, it was noted that key sustainable development goals identified by the High-Level Political Platform for Sustainable Development included building 'resilient infrastructure'[3] (see Box 3).

[2] https://www.thegfce.com/about

[3] See Sustainable Development Goal 9 of the SDG Compass written by GRI, the UN, and the World Business Council for Sustainable Development (WBCSD): https://sdgcompass.org/sdgs/sdg-9/

Box 2. Goals: What are the Long-range Goals of Cyber Security

One speaker focused on identifying the goals that drive cyber security efforts, including:

- Security as an End in Itself that is Valued in Society
- Social and Economic Development
- Prosperity for the Economy and Trade
- Protection of Key Values of a Free and Open Society

Box 3. United Nations Sustainable Development Goals

On 1 January 2016, the 17 Sustainable Development Goals (SDGs) of the 2030 Agenda for Sustainable Development — adopted by world leaders in September 2015 at an historic UN Summit — officially came into force. Over the next fifteen years, with these new Goals that universally apply to all, countries are expected to mobilize efforts to end all forms of poverty, fight inequalities and tackle climate change, while ensuring that no one is left behind.

See: https://sustainabledevelopment.un.org/?menu=1300

However, it was also acknowledged by several speakers that cybersecurity is what has been called a 'wicked problem'. Wicked problems are those that are exceptionally difficult if not impossible to resolve.[4] Given the multiple layers and actors shaping the moving targets of cybersecurity, no one objected to the notion of cybersecurity capacity building being viewed as a wicked problem. It is difficult to resolve given such features as a lack of information, contradictory information, requirements that change over time or across contexts, and uncertainty about the key factors causing the problems.

[4] An early conceptualization of the idea of 'wicked problems' is Rittel, H.W.J. & Webber, M.M. (1973).

Given the difficulties surrounding a wicked problem, it is critical to start taking reasonable steps, even if the resolution of the problem is uncertain. Several steps were identified for nations in moving forward: building a national strategy, creating a cybersecurity incident response team (CSIRT) to manage incidents, addressing cybercrime, building a security culture and associated skills, and identifying the most critical standards.

National Strategies

Several speakers and discussants pressed the point that a desire for cybersecurity capacity building is not enough: there needs to be a strategy and a national agency in place to develop and carry it forward. A strategy can start small, keeping it simple, and be built on overtime, rather than trying to address everything at once. Beginning this strategy also helps build a planning process for cybersecurity, which not only helps develop an understanding of the best approach to cybersecurity planning, but also begins a process of identifying and working with other areas of planning and strategy across government, including law enforcement.

One speaker evoked the metaphor of a wall, arguing that not having a national strategy creates a 'big hole in the cybersecurity wall'. It was noted that by one estimate, from 2016-2018, more countries have developed a cybersecurity strategy, but many others have yet to move ahead. Globally, 77 (40%) of 196 countries have a strategy and 13 (7%) are in the process of drafting one, leaving more than half of the nations without a strategy. In African countries, 11 (20%) of 54 nations have a strategy, and 6 (11%) are in the process of drafting one, leaving nearly two-thirds of African nations without a strategy. Strategically, it was argued that the global cybersecurity community should focus its efforts on working with those nations who most recently drafted, or are currently drafting, a strategy as a means for building a global conversation about this objective. While this hole in the cybersecurity wall might be worrisome, it was noted that progress had been made since 2010, when only a few countries had any cybersecurity strategy.

National Computer Security Incident Response Team (CSIRT)

Creating a Computer Security Incident Response Team (CSIRT) was another concrete step, in addition to drafting a national strategy, that was prioritised by speakers. One speaker raised the rhetorical question: 'How do countries survive without a CSIRT or a strategic plan?' Generally, the lack of a CSIRT is related to a country's stage of digitalisation. During a stage of low digital maturity, there is a potential for national leaders to not see the need for a response team. Once they reach a greater level of digitalisation is when the problems start, and they are shocked and quickly become aware of the need for capacity building. There is a need for building an awareness of the value of a CSIRT before major problems arise.

Cybercrime

As in the area of cybersecurity, some nations were slow in developing cybercrime capacities. However, as fast broadband came to their countries, cybercrime arrived with it, too often to the surprise of public leaders. However, overtime, cybercrime initiatives have become a model of global cooperation, making the police and the justice system excellent partners, which are too often forgotten, in the process of developing cybersecurity processes. For example, in the UK, an excellent guide for working with computer-based evidence was cited, which was developed by the Association of Chief Police Officers (ACPO) – one that should be of value across the cybersecurity community (see Box 4).

Box 4. Digital Forensics and Computer-Based Evidence

The UK's Association of Chief Police Officers (ACPO) has developed a good practice guide for dealing with computer-based evidence was first released in the late 1990s. Since then, there have been five iterations; some of the changes include an update in the document's title. The guide is essential reading for anyone involved in the field of digital forensics. The latest version "ACPO Good Practice Guide for Digital Evidence" has been updated to include more than just evidence from computers.

See: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Cybersecurity Culture and Related Skills

Participants spoke of the 'culture of institutions' and nations being critical to developing the political will and values that are key to capacity building. The working lunch surfaced the importance of cybersecurity norms as a focus of awareness campaigns, such as in the African region, to encourage people to act within the law. In addition, as discussed further below, the recent EU Directive on Network and Information Systems (NIS) focuses on the creation of a 'culture of security' in its Member States (see Box 5).[5]

While the GCSCC has focused on social and cultural aspects of cybersecurity, such as its work on norms and the idea of a cybersecurity mindset (Dutton 2017), the topic was not a prominent theme at the conference. This suggested that there is a need to keep the priority of social and cultural issues of cybersecurity in mind, and explicitly raised.

Box 5. EU's Directive on Security of Network and Information Systems (NIS)

Adopted by the European Parliament on 6 July 2016, this Directive creates a framework for legal measures to support cyber security. The Member States are directed to translate the elements of the Directive into national laws and regulations and also identify the entities that will provide essential services called for in the directive, such as a CSIRT and a national 'NIS authority'. The Member States are also required to set up groups to coordinate cooperation across the Member States. In addition, they are directed to foster a 'culture of security'.

See: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Standards

Finally, the need for standards and best practices in many areas of capacity building was noted, particularly in discussions surrounding the need for information sharing.

Identifying Indicators of Capability in Order to Build on Each

Cybersecurity capacity is built on some as yet to be determined set of capabilities. What are these capabilities? What are the best indicators of each capability? That is, how do we measure each capability? Projects are often built on the objective of addressing some capability, such as awareness

[5] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

raising. Support for such projects requires those supporting them to show that the projects make a difference, which means there is a need to track the impact of projects on particular goals and objectives.

As one participant put it, cybersecurity is a major cost, so it is imperative to put money in the ‘right place’, and not put money into a ‘black hole’. A member of a donor organisation argued that the key problem is not with resources, but in making sure the money gets to the right place. From the donor’s perspective, the right place is often a project that is not duplicating effort and that is complementary to other existing projects.

These issues are a reminder that some indicators of success are relatively simple. Does the money get spent on what it was supposed to be invested in, and is the project doing what it promised? These are primary features of evaluation research, for example, which documents what was actually done. While such evaluations can be politically sensitive, they are based on well-developed approaches to evaluation and policy research (Patton 2015).

The Need to Document and Measure Success: Informing Investment

There was a general sense that the community’s sense of accomplishment needs to be accompanied by independent and convincing indicators – metrics of success. Put bluntly, governments want to know if they are getting a return on investment (ROI) in cybersecurity? A corollary to the need for better indicators is a stronger sense of what to do with them. As one speaker asked: ‘What ambition should we have with metrics of success?’ For example, can they be used more creatively for formative evaluation, and not just validating performance?[6]

Cybersecurity is not as visible and tangible as many other public goods, such as clean water or good roadways. It is more difficult to get the public and its representatives to ‘see’ cybersecurity, making the development of indicators of success all the more important to supporting further investments. In fact, the point was made that success in capacity building can make cybersecurity less visible as nothing bad happens. As one speaker noted, if ‘everything works then nothing happens’. It often

[6] Formative evaluation research is used not simply to assess the value of a project, such as whether it accomplished its aims, but to assess performance at a stage that it is possible to redesign and structure the project from lessons learned in the evaluation process.

only becomes an issue when dramatic breaches or personal problems arise. The immediate and visible wins are over the longer-term and are less visible than immediate failures. For such reasons, as one participant put it: ‘Roofs on schools win over cybersecurity.’

As one speaker noted, it takes ‘moral courage’ to ‘come up with the numbers – to quantify progress’. How can we measure impact? What constitutes success in cybersecurity capacity building and how are we, as a global community, evaluating this? Broadly, what are the best indicators of success?

Work begun by the GCSCC on analysing the impact of capacity building has marshalled preliminary evidence that cybersecurity does indeed matter (Dutton et al 2017; Creese et al forthcoming). This work needs to be progressed further and moved beyond indicators of end-user experiences to show the economic impact of security, work that the UK’s FCO is exploring.

Another effort is focused on indicators of cyber harm and whether capacity building will significantly reduce cyber harms[7] (see Box 6). However, many comments noted the difficulties surrounding the development of metrics in cybersecurity. Metrics can be tricky, such as rankings that can become distractions, focusing countries on moving up in the ranks. Moreover, metrics are likely to change over time, as a country becomes more mature, or as technology changes. The pitfalls of measuring

[7] In 2017, the GCSCC held an expert workshop around research on ‘cyber harm’. See: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/gcscc-workshop-cyber-harm

cybersecurity or failures of cybersecurity are legion. As one article put it: ‘How can cybersecurity improve if the problem can’t be measured?’[8]

Box 6. Cyber Harm

A focus on cyber harm seeks to identify the damaging consequences of deliberate malicious cyber-attacks or attacks on cyber resources as well as of accidental events. What is harmed? What are the different kinds of harm inflected? Who are the relevant stakeholders? How can harm be measured? These questions are guiding exploratory research by GCSCC researchers in developing a better understanding of these issues.

See: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/gcscc-workshop-cyber-harm

A related challenge revolves around investment: How can investment be tracked when it is the sum of inputs from multiple actors across all levels? As one speaker noted: Cybersecurity, like networking and information systems, should be ‘part of the operating budget of every organisation’. Nevertheless, what will inform new and continuing investments when they are so diffused across governmental and other actors?

This question circles back to issues over documenting the success of initiatives in ways that can better inform future investments. Examples were given of how difficult it is to link cybersecurity to such common indicators of well-being as the number of people lifted out of poverty, or increases in economic productivity, but these are the kinds of payoffs that donors and funders of cybersecurity want to see. But as one participant noted, the relationship between prosperity and security can go both ways – saying ‘strong digital economies drive investment into security’.

Cybersecurity is an ‘expensive proposition’, as noted by one speaker. It has been long viewed as a cost, but as these costs have grown overtime, it is important to also convey these investments as an enabler of social and economic development, as well as a means for reducing cyber harms. The need

[8] https://gcn.com/blogs/cybereye/2013/11/measuring-cybersecurity.aspx

for cyber capacity is no longer taken for granted, if there was ever a time it was. Increasingly, governments and other donors and funders want evidence to answer the question: 'Why are we spending so much money on this?'

Of course, all the multiple needs of specific countries do not always match what donors want to support. One speaker remarked rhetorically: 'There is a finite number of donors'. This was one reason why one speaker noted the need to grow the donor community, saying that the community 'needs multiple donors to support relatively specific needs'.

Time Horizons

Capacity building requires strategies and actions across multiple time horizons. On the one hand, there is a need to be able to act immediately to address threats and attacks on security. On the other hand, there is a need for a longer time horizon. In discussion of the ASEAN member states, a speaker noted the need for at least a five-year horizon for planning and investment.

Acting Globally and Regionally to Help Locally

One participant made a strong claim that cybersecurity is 'one of the biggest global problems' we face. Discussions underscored two ways in which this is the case.

First, it is a problem worldwide in that no country has achieved a satisfactory level of cybersecurity. All nations have experienced major problems and also face grave threats.

But secondly, the point arose time and again that solutions to cybersecurity need to be global. If one nation has great capacity, it can be threatened by actors that exploit the weaknesses of nations that lack capacity. In this sense, it is in every nation's self-interest to ensure that capacity building encompasses every nation across the world.

There were a number of local aims and objectives identified throughout the day. They included:

- Putting security measures in place, such as establishing local CSIRTs;
- Implementing confidence building measures;
- Focusing on building and identifying leadership (see Box 7); and
- Simply getting started – starting the process.

There were several interventions around the need to just get started, and that given the iterative and long-term nature of developing strategy and its implementation, it is okay to start small.

Box 7. The Priority of Leadership Issues

Throughout the conference, a number of participants raised questions and issues around the need for leadership on capacity building. They include:

- Picking leaders: Who starts? Who leads?
- The need to identify leadership, select the right leadership.
- Building the capacity of leaders.
- You can't 'do' cyber security, 'you need leadership'.
- Drumming up 'leadership buy in' to gain 'whole government buy in' on security.

The Multi-Stakeholder Nature of the Cybersecurity Ecology of Actors

Much discussion focused on the ecology of actors that build cybersecurity capacity, as well as the multitude of stakeholders in cybersecurity, many arguing that this area is inherently multi-stakeholder. While it is difficult to provide a comprehensive list of actors and stakeholders, there were several key points to these discussions.

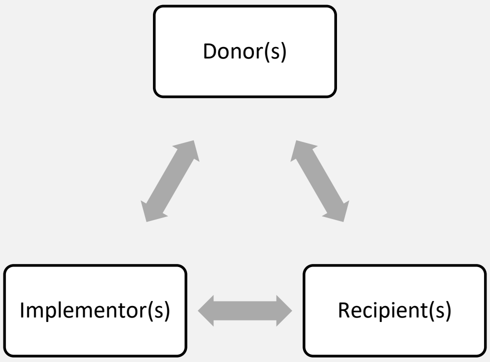
First, cybersecurity is not simply a technical project. It is 'multi-disciplinary' and not just 'multi-stakeholder'. In addition to technical expertise, there is a great need for very different sets of skills and knowledge bases, such as those involved with international diplomacy, strategy building, and national policy and regulation, in addition to actors from industry, and non-governmental organisations (NGOs).

Secondly, beyond its multi-disciplinary aspects, is the need for a multi-layered or multi-level approach, from the ministerial level, to senior appointed officials, to the technical level, such as those directly involved in training cybersecurity officers and operating a Cybersecurity Emergency Response Team (CERT). Major innovations in cybersecurity across sectors of government also require ‘political backup’ by top politicians within the country. While ‘all believe in a multi-stakeholder model’, as one speaker argued, ‘it is simply hard to realise’ across these many layers.

Clearly, no single set of actors is dominant. Success depends on the interactions across multiple sets of actors, which one speaker referred to as the ‘Holy Trinity’ (see Box 8). However, there are many lists of the kinds of multiple stakeholders that need to be considered in capacity building initiatives.[9]

Box 8. The Holy Trinity of Cyber Security Capacity Building

The interactions among donors, implementors, and recipients are critical to the success of this trinity.



The Centrality of National Capacity in a Local Context

One argument was that progress has to be anchored in national capacity. Local, regional and global – supra-national – capacity building processes are all critical, but these efforts depend on national actors who network from the top-down, bottom-up, and side-to-side. Ideas as well as very practical steps, such as training, need to be fostered at the national level, such as in making capacity building a national priority.

[9] For example, see a report from NETmundial: http://content.netmundial.br/contribution/the-importance-of-a-multistakeholder-approach-to-cybersecurity-effectiveness/180

National approaches are critical in order to tailor activities to the local context. As one speaker put it: 'no one size fits all' for capacity building. For example, training needs to be tailored to each country's needs. Likewise, some countries are not yet involved in capacity building, and here there is a need to focus more on developing awareness of the issues. At the same time, local initiatives need to complement regional and global initiatives, avoid duplication, and achieve a collective impact – requiring coordination.

Implementation Gaps and the Routinisation of Innovations

While strategy development was a focus of considerable discussion in the early sessions, the discussion over the day moved increasingly to aspects of implementation. Implementation is a stage in the process of innovation – moving an abstract, new idea, into a concrete set of activities.[10] The implementation stage of an innovation was developed further in discussion of the routinisation of an innovation – how an idea once implemented can become part of routine practices.

An innovative idea can falter at any of these stages. It can fail to be implemented in the ways envisioned by the strategy, for example. This often happens as new ideas are changed as they meet the practical realities of different social and political contexts (Pressman and Wildavsky 1973). But also, even if successfully implemented, an innovation can fail to become a routine aspect of an organisational or institutional repertoire of activities, variously called 'rountinisation' or 'institutionalisation' (Rogers and Agarwala-Rogers 1976: 163-4). So even a successful project can fail in the longer-run if it does not reshape routine practices.

Cybersecurity capacity building is a case in point. Visions are not always realised in their implementation, and valuable innovations often fail to become part of organisational routines. As one speaker noted: 'National strategies are easier to develop than to implement.' This was due, according to the speaker, to such factors as the strength of internal government structures that often conflicts with cyber as a 'cross-cutting' enabler. In addition, each actor needs to see the big picture as well as their specific role in the national mission, including an understanding of their

[10] Work on the concept of implementation as an aspect of the innovation process was a focus of the innovation literature. See Rogers and Shoemaker (1971), and Pressman and Wildavsky (1973).

responsibilities and the structure of accountability for each actor. Aligning strategy and its implementation is therefore a complex and iterative process – or continuing cycle.

In this respect, discussion recognised that implementation of security innovations and the routinisation of successful initiatives need to become part of capacity building. Not only do these efforts arise in different stages of the innovation process, but they involve different actors with different capabilities. The ability to think strategically and understand how to build a strategy requires a different set of skills than implementing the resulting plans. One participant spoke of developing a 'pipeline of staff', but also about the need to identify and protect them, such as by letting them focus on their work, rather than sending them off to lecture around the world.

Building a Community: Developing and Nurturing Human Capital

There is a strategic need for governments to invest in human capital development of cybersecurity. On the one hand, one speaker argued that there is a lack of expertise in cybersecurity at all levels, but also arguing that there is a need for a 'massive' volume of cybersecurity experts and cybersecurity competence across the workforce in Europe and globally. There are simply not enough people to effectively implement capacity building initiatives.

Explanations for this shortcoming are many. One reason is that the cybersecurity profession is quite young, making it difficult to create a large talent pool of experienced individuals. Also, daily cybersecurity operations are major, and take up most of the available expertise and staff, leaving few staff available for capacity building projects. In addition, several cited the degree that the public sector is losing many skilled staff who are 'cherry picked' by the private sector, attracted by higher wages and better working conditions. Public sector organisations need to look for creative ways to attract and retain skilled employees; including the possibility of offering academic scholarships in exchange for set terms of subsequent public service, and early retirement options. Attracting and retaining more people in the capacity building business is a key to greater success.

In addition, public and private sector organisations are looking into automation as a way to ease the human capital bottleneck. For example, ForAllSecure, a team at Carnegie Mellon University, won a

DARPA Cyber Grand Challenge with Mayhem, one of the first systems to play a Capture the Flag game against humans and win.[11]

The Challenges of Coordination – Developing the Clarity for a Global Response

A corollary of these observations is the need to better coordinate efforts across nations and across actors within nations in order to achieve cybersecurity cooperation to achieve a 'better collective impact' – a 'safe and secure cyberspace' where national borders are more porous if not less relevant than in other public domains. One speaker noted that coordination was not the biggest problem – it was clarity. However, as can been seen across a variety of initiatives, clarity is being approached through information and toolkit developments as one means to support coordination and collaboration. As one speaker said: 'Do we really need another portal?' Likewise, another participant cited a 'proliferation' of tool kits, as nations often believe that an existing toolkit 'doesn't quite fit' their own particular needs. Of course, this is a tendency across the technology community generally, which some refer to the 'not-invented-here' syndrome, which can undermine efforts to avoid duplication of effort.

However, coordination is difficult when many cybersecurity actors are so focused on day-to-day operations and to 'putting out fires'. In this spirit, a number of strategies for achieving better coordination were identified. These included:

- Identifying, documenting, clarifying, and sharing best practices, such as through the development of detailed case studies and success stories;
- Creating and diffusing toolkits that can enable nations to follow good practices and not reinvent the wheel, such as noted with the cybercrime toolkit funded by Korea but involving seven international organisations (see Box 9);
- Developing a consensus at multiple levels (local to global) by convincing all parties and nations of the benefits of cooperation;

[11] https://techcrunch.com/2016/08/05/carnegie-mellons-mayhem-ai-takes-home-2-million-from-darpas-cyber-grand-challenge/

- Working bi-laterally to engage key nations, a model the World Bank has found successful in serving as a fiduciary with governments – helping to broker investments one nation at a time, such as in producing its cybercrime toolkit (see Box 9);
- Donors can help force or incentivise the cyber community to work more closely together;
- Closing the gap that can exist between donors and implementers (see Box 10);
- Identifying, supporting, and networking regional hubs for a global network;
- Solving the cybersecurity leadership problem around who in the end takes the lead on national and international initiatives; and
- Developing information resources that can be shared globally to avoid duplication and insure greater quality assurance in sources, such as the Cybersecurity Capacity Portal (see Box 11).

Box 10. The Donor Gap

A number of speakers referred to a gap between donors and those paid to 'deliver' on a project. A number of reasons were cited for this gap developing:

- A donor doesn't always get what they think they paid for, creating a need to clarity and transparency between donors and recipients;
- Not getting anything, such as in the case of a failed project, suggesting that more evaluation of the feasibility of proposals should be conducted, or that there should be a greater tolerance for failure, given the difficulties facing innovative projects with complex requirements for collaboration;
- A recipient cannot demonstrate success or have convincing evidence of the impact of a project, suggesting the need to build in an evaluation component.

Box 11. Cybersecurity Capacity Portal

The cybersecurity capacity portal, is a global resource for cyber security capacity building and how best to achieve it, and an online space for sharing experiences, best practice, and new developments. It has been developed with the Said Business School, University of Oxford, and in partnership with The Global Forum on Cyber Expertise (GFCE), a new global platform promoting cyber capacity building.

See: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front

An example of coordination efforts was provided in the ASEAN region, through an ASEAN Cyber Capacity Programme (Box 12). For example, it developed a workshop to develop a consensus around a set of cyber norms for responsible state behaviour for cyberspace, leading to a set of initiatives to support these norms, such as starting with awareness raising.

Box 12. ASEAN Cyber Capacity Programme (ACCP)

The ACCP aims to build cyber capacity in ASEAN Member States. It will enhance regional ability to respond to the evolving cyber threat landscape and to build a secure and resilient ASEAN cyberspace.

https://www.csa.gov.sg/~/media/csa/documents/amcc/factsheet_accp.ashx?la=en

The ASEAN region includes ten countries. Building a road map to address the region involved tailoring initiatives for each country's needs, but also beginning with the biggest members, anticipating that their progress would spur smaller members to follow.

Another example arose around the commonwealth nations with 52 countries. Despite major variations in the size of the nations, common law nevertheless provides for some level of consistency across these nations, and the institution provides mechanisms for drawing together the experts as well as the ministers in relevant sectors to deal with particular problems, creating an opportunity for greater international collaboration and sharing, such as through a planned meeting of the heads of commonwealth governments (see Box 13). Similarly, the commonwealth nations have been successful in developing a cybercrime initiative (see Box 14).

Box 13. The Commonwealth Heads of Government Meeting, London, April 2018

The Commonwealth is a diverse community of 52 nations that work together to promote prosperity, democracy and peace. In April 2018, the UK will host the Commonwealth Heads of Government Meeting (CHOGM) when leaders from all the member countries are expected to gather in London and Windsor. They will come together to reaffirm our common values, address the shared global challenges we face and agree how to work to create a better future for all our citizens, particularly young people.

https://www.chogm2018.org.uk/

An example – perhaps an exemplar – of global cooperation was the area of cybercrime. A model that arose in regional collaborations, such as Europe around such institutions as the Council of Europe, has become a global and sustainable model, according to one speaker. This example suggests that it is possible to have a global response to cybersecurity capacity building and might well present a useful model on how to proceed.

Box 14. Commonwealth Cybercrime Initiative

The Commonwealth Cybercrime Initiative (CCI) unites 35 international organisations, including Interpol, OAS, Council of Europe (CoE), Commonwealth Telecommunications Organisation (CTO) and ITU, contributing to multidisciplinary programmes in Commonwealth countries. These organisations form the CCI Consortium.

http://thecommonwealth.org/commonwealth-cybercrime-initiative

Despite many speakers and participants who stressed the need for better coordination, at least one speaker argued against a fixation on coordination. As he put it: 'You need to accept a certain messiness' in national and international cybersecurity collaborations. At times, so much attention is focused on coordination that problems arise, creating a need to 'coordinate the coordinators'. Another speaker emphasised that collaboration and coordination is far more difficult than many not involved in capacity building might think. He referred to a set of problems that made collaboration over cybersecurity a virtual 'minefield' (see Box 15).

Box 15. The Capacity Building Minefield

It is important to recognise the challenges to collaboration on cybersecurity capacity building, which create a virtual minefield to traverse. The problems include:

- In many countries, the area is uncharted ground with no tried and proven pathways;
- Many key actors do not buy in to the need for capacity building;
- Some fear the risks such as the waste of resources, given competing demands;
- Many instinctually want to guard and protect their existing fiefdom, which they could see compromise by collaboration on cybersecurity and the sharing of information that this might involve;
- Collaborations involve new actors, which means key stakeholders do not know who is important;
- Accountability is difficult when there is often a lack of clarity over responsibilities; and
- Trust among those collaborating is difficult to achieve – it does not come automatically.

Institutionalising Capacity Building as a Routine Collaborative Activity

The organisation of capacity building needs to be developed within each nation in conformity and in collaboration with many other areas, such as trade, agriculture, and defence, but also in relevant regional and global organisations. It is important to institutionalise these efforts in order to ensure their routine use and sustainability over time. An example came up in discussion over training. A speaker cited what she referred to as 'fly by training' as opposed to 'sustainable training'. Instead of, or in addition to, flying a team in to offer a one-shot training session, local and national organisations need to focus on 'training the trainers' to ensure that training services such as this can be offered in a sustainable way.

The EU provides another and recent example of an effort to institutionalise cybersecurity and develop international coordination through its Directive on Security of Network and Information

Systems – the NIS Directive (see Box 5, above). As one speaker called the Directive a good move. As he put it: ‘This is the best way. It does not give any choice. We have to do this!’

Summary and Conclusion

Throughout the conference, it was clear that cybersecurity capacity building has a global mission that is anchored at the national level, which recognises that no one size fits all and that local contexts are critical. For example, national strategies and response teams are critical national building blocks. Nevertheless, local-national success depends on global up-take of capacity building which is progressing. Advances are being made in awareness, investment, metrics, information sharing about best practices, and the coordination of projects.

However, capacity building is facing major challenges in the allocation of scare resources when it is difficult to document success, but blindingly obvious when failures occur. Moreover, the metrics are difficult to develop and trust, given the disincentives for many to report problems. And there is a major shortage of the personnel needed on the capacity building front.

Recognising these challenges is key to the next phases, which seek to build on success to-date. Plans are in place to build and promote a global network of expertise and continue to tap the wisdom of this international set of experts in cybersecurity capacity building.

Appendix 1. The Agenda for the Conference

10:00 Welcome and Session 1, Lecture Theatre, Oxford Martin School.

The conference began with a welcome by Professor Michael Goldsmith, Director of the Global Cybersecurity Capacity Centre (GCSCC), which led into the first session focusing on what the project is achieving in cybersecurity capacity building, and how are the resources of the centre being invested in achieving these outcomes.

Chair: Prof Paul Cornish, GCSCC

Speakers: Deputy Chief Executive Mr NG Hoo Ming, CSA Singapore

Robert Collett, Foreign & Commonwealth Office, United Kingdom

11:15 Coffee and tea

11:30 Session 2

What are the barriers to a strategic global response? How do we coordinate strategic investment across the community?

Chair: Prof Sadie Creese, Founding Director of the GCSCC

Speakers: Heli Tiirmaa-Klaar, European External Action Service

David Satola, World Bank

12:45 Working Lunch Chancellor’s Court at the Bodleian Library

New collaboration ideas in cybersecurity capacity building

Lead: Prof Basie von Solms, Global Cyber Security Capacity Centre

14:15 Session 3

What are the obstacles to strategy implementation? How can we overcome these?

Chair: Kerry-Ann Barrett, Organization of American States

Speakers: George Michaelides, Commissioner of Electronic Communications and Postal Regulation, Cyprus

Johanna Vazzana, MITRE Corporation

15:30 Coffee and tea

15:45 Session 4

How do we set global priorities based on regional cybersecurity capacity reviews and risk assessment?

Chair: Sadie Creese, Founding Director of the Global Cyber Security Capacity Centre

Speakers: Bill Dutton, GCSCC

David van Duren, Global Forum on Cyber Expertise

16:50 Closing Session

Prof Michael Goldsmith, Director of the Global Cyber Security Capacity Centre 17:00

Drinks Reception

18:00 End of Conference

Appendix 2. Attendees at the Conference

First	Last	Organisation
Ioannis	Agrafiotis	Global Cyber Security Capacity Centre
Matt	Allison	Access Partnership
Ivan	Arreguín-Toft	Harvard University
Louise	Axon	University of Oxford
Maria	Bada	Global Cyber Security Capacity Centre
Kerry-Ann	Barrett	Organisation of American States
John	Bassett OBE	RUSI
James	Boorman	Oceania Cyber Security Centre
Peter	Burnett	Quarter House Ltd
Enrico	Calandro	ResearchICTAfrica
Andrea	Calderaro	Cardiff University
Kaja	Ciglic	Microsoft
Robert	Collett	Foreign & Commonwealth Office
Simone	Conrad	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
Paul	Cornish	Global Cyber Security Capacity Centre
Sadie	Creese	Global Cyber Security Capacity Centre
William H.	Dutton	Global Cyber Security Capacity Centre
Simen	Ekblom	Ministry of Foreign Affairs Norway

Arnau	Erola	University of Oxford
Andrew	Fitzmaurice	Templar Executives Ltd.
Esther	George	International Association of Prosecutors
Akvilė	Giniotienė	NRD CS
Michael	Goldsmith	Global Cyber Security Capacity Centre
Matthew	Griffin	Global Cyber Security Capacity Centre
Faisal	Hameed	University of Oxford
Gael	Hernandez	Interconnection Policy and Regulatory Affairs
Nigel	Hickson	ICANN
Qendresea	Hoxha	Swiss Federal Department of Foreign Affairs FDFA
Eva	Ignatuschtschenko	UK Cabinet Office
Nigel	Jones	IAAC
Olly	Jones	PROTECTION GROUP INTERNATIONAL
Thomas	Jordan	Foreign and Commonwealth Office
Ines	Kaljee	Dutch Ministry of Foreign Affairs
Lea	Kaspar	Global Partners Digital
Philip	Lark	George C. Marshall European Center for Security Studies
Steven	Malby	Commonwealth Secretariat
George	Michaelides	Commissioner of Electronic Communications and Postal Regulation Cyprus
Julia	Mills	Australian State Government of Victoria

NG Hoo	Ming	CSA
You Jin	Moon	CSA
Patrick	Mulcahy	Foreign & Commonwealth Office
Niels	Nagelhus Schia	NUPI
Eva	Nagyfejeo	Global Cyber Security Capacity Centre
Jason	Nurse	University of Oxford
Puay Son	Ong	CSA
Lara	Pace	Global Cyber Security Capacity Centre
Sithuraj	Ponraj	CSA
Sarah	Puello Alfonso	Global Cyber Security Capacity Centre
Carsten	Rudolf	Oceania Cyber Security Centre
David	Satola	World Bank
Anita	Sohan	CTO
David	Souter	ICT Development Associates
Heli	Tiirmaa-Klaar	EEAS
Anri	Van der Spuy	ResearchICTAfrica
David	Van Duren	Dutch Ministry of Foreign Affairs
Manon	Van Tienhoven	Global Forum Cyber Expertise
Johanna	Vazzana	MITRE
Basie	Von Solms	Global Cyber Security Capacity Centre

Carolin	Weisser	Global Cyber Security Capacity Centre
Jeb	Webb	Oceania Cyber Security Centre
Louise	Williams	Global Cyber Security Capacity Centre

Appendix 3. Appendix Acronyms and Abbreviations

ACCP	ASEAN Cyber Capacity Programme
ACPO	Association of Chief Police Officers
ASEAN	Association of Southeast Asian Nations
CCI	Commonwealth Cybercrime Initiative
CHOGM	Commonwealth Heads of Government Meeting
CoE	Council of Europe
CSIRT	Computer Security Incident Response Team
CTO	Commonwealth Telecommunications Organisation
DARPA	Defense Advanced Projects Agency
EAC	East African Community
ECOWAS	Economic Community of West African States
EU	European Union
FCO	Foreign & Commonwealth Office, United Kingdom
GACCB	Global Agenda for Cyber Capacity Building
GCSCC	Global Cyber Security Capacity Centre, Oxford Martin Centre
GDP	Gross Domestic Product
GFCE	Global Forum on Cyber Expertise
GRI	Global Report Initiative
ICBO	International Capacity Building Organisations

ITU	International Telecommunications Union
LAC	Latin America and Caribbean
NIS	Network and Information Systems (EU-wide Directive)
OAS	Organization of American States
OCSC	Oceania Cyber Security Centre
ROI	Return on Investment
SADC	Southern African Development Community
SDGs	United Nations Sustainable Development Goals
WBCSD	World Business Council for Sustainable Development

Appendix 4. References

Clark, D., Berson, T., & Lin, H. S. (eds). (2014). *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington, D.C.: National Academies Press. http://doi.org/10.17226/18749

Creese, S., Shillair, R., Roberts, T., Bada, M. and Dutton, W. H. (forthcoming), 'Building the Cybersecurity Capacity of Nations', pp. forthcoming in Graham, M. and Dutton, W. H. (eds), Society and the Internet, 2nd Edition. Oxford: Oxford University Press.

Dutton, W. (2017), 'Fostering a Cyber Security Mindset', *Internet Policy Review*, 6(1): DOI: 10.14763/2017.1.443 Available at: https://policyreview.info/node/443/pdf

Dutton, W. H., Creese, S., Shillair, R., Bada, M., Roberts, T. (2017), Cyber Security Capacity: Does it Matter? Paper presented at the Annual Meeting of the Telecommunication Policy Research Conference (TPRC), held at George Mason University, September 8 & 9.

Patton, M. Q. (2015), *Qualitative Research & Evaluation Methods, 4th Edition* (Thousand Oaks, CA: Sage Publications).

Pressman, J. L. and Wildavsky, A. B. (1973), *Implementation: How Great Expectations in Washington Are Dashed in Oakland*. Berkeley, CA: University of California Press.

Rittel, H.W.J. & Webber, M.M. (1973), *Policy Sciences*, 4: 155. https://doi.org/10.1007/BF01405730

Rogers, E. M. and Agarwala-Rogers, R. (1976), *Communication in Organizations*. New York: The Free Press.

Rogers, E. M. and Shoemaker, F. F. (1971), *Communication of Innovations*, 2nd Edition. London: Collier Macmillan Publishers; New York: The Free Press.