Global
Cyber Security
Capacity Centre

The Global Cyber Security Capacity Centre

"There is no future that does not involve cyberspace, so understanding how to ensure effective cyber security to protect our assets and provide for people's needs is incredibly important. The work of the Global Cyber Security Capacity Centre is not just to understand what good cyber security looks like across all of its dimensions, it's also to establish the frameworks which allow us to measure it over time so we can check that we are investing in the right way and evolving in the right directions. This is essential to safeguard cyberspace as an environment in itself, a critical resource for future generations."

Professor Sadie Creese
Professor of Cyber Security and
Director of the Global Cyber Security Capacity Centre

Global cyber security is a crucial capability to underpin growth and innovation in the online environment and wider digital economy, and support well-being, human rights and prosperity for all.

WORLDWIDE, actors at all levels, from individuals to nation states, need to ensure that cyberspace and the systems dependent on it are resilient to attack, in the face of constant growth in the scale and complexity of our networks, and enormous volumes of data and applications. The international community needs to protect digital devices and information infrastructures from malicious entities seeking to steal secrets, deny access to critical services, and exploit others' identities to commit crimes. It is essential to address cyber-crime and maintain the trust placed in our systems, while ensuring that this trust is justified. Cyber space and our assets within it need to be protected to ensure that critical digital infrastructures and services can operate effectively now and in the future.

The Global Cyber Security Capacity Centre is focused on helping the international community increase the impact, scale and pace of cyber security capacity-building by:

- Investigating the drivers for current capacity-building activities and the conditions required to increase resources
- Providing the scientific framework to enable individuals and institutions to measure and understand effective cyber security, providing an evidence base and model for supporting benchmarking, policy formation, and measuring effectiveness
- Pooling, evaluating and sharing information on best practice and experiences in capacity-building activities
- Creating and keeping up to date a critical guide to global expertise on cyber security
- Setting out what needs to be done in order to analyse priorities, and identify and close gaps in the global response

The work of the Centre is focused on developing a framework for understanding what works, what doesn't work and why – across all areas of cyber security capacity. This is important so that governments and enterprises can adopt policies and make investments that have the potential to significantly enhance safety and security in cyberspace, while also respecting other core values and interests, such as privacy and freedom of expression.

Funded by the UK government, the Centre is working with a wide range of global partners, including governments, international organisations, leading academics, and the private sector. The Centre will ensure that this knowledge becomes a global resource.

The Global Cyber Security Capacity Centre

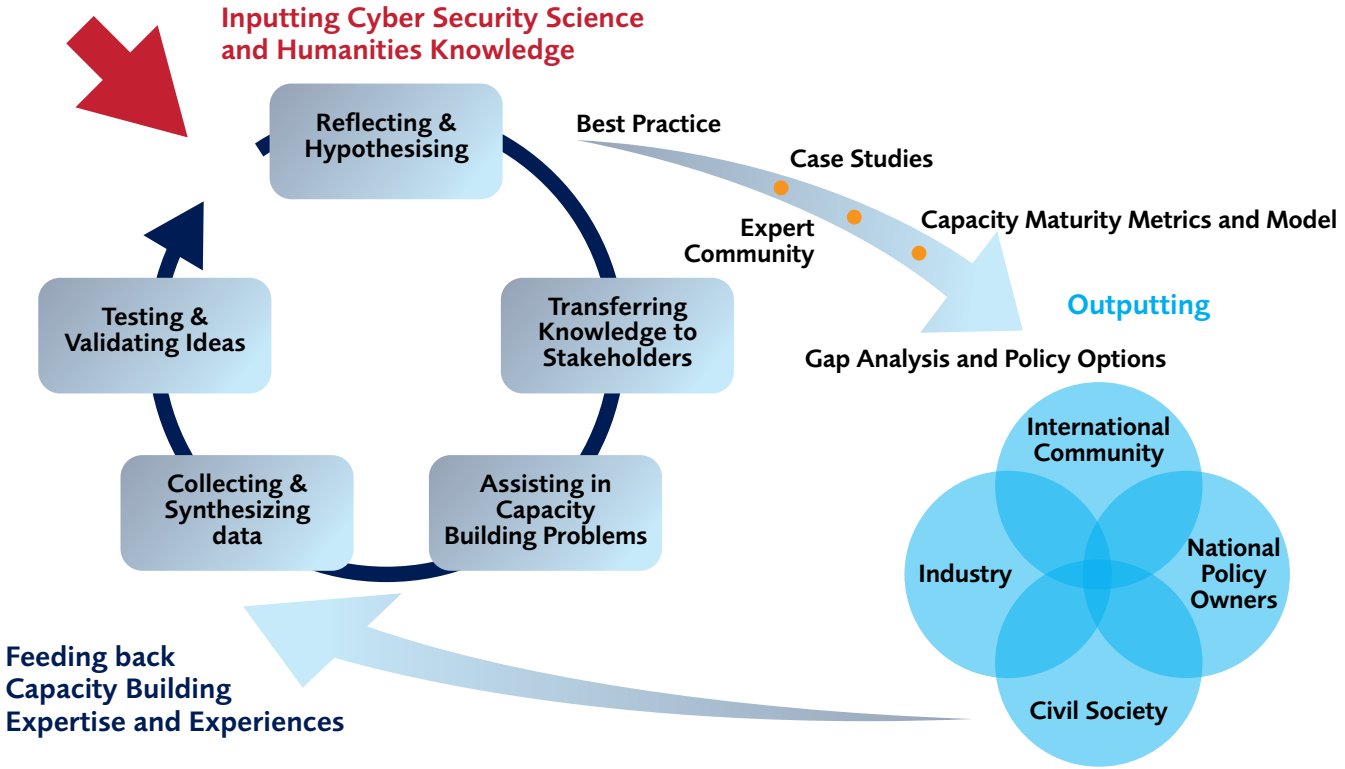
A MULTI-DIMENSIONAL CONCEPT

Cyber security is a multi-dimensional concept that spans:

1. devising cyber policy and cyber defence
2. encouraging responsible cyber culture within society
3. building cyber skills into the workforce and leadership
4. creating effective legal and regulatory frameworks
5. controlling risks through technology and processes

The Centre has established working groups to focus on the nuances of capacity across and within these multiple dimensions, the types of activities which can deliver and increase capacity, where best practice exists, the conditions under which increases in capacity should be sought, and the ways in which the dimensions relate to and depend upon each other for success.

Research within and across the working groups will adopt the following principles:
Avoid reinvention: seek to identify best practice wherever it arises
Inclusivity: to consider relevant global and multi-cultural issues
Objectivity: to maintain an objective approach, with members of working-groups representing their individual and community knowledge, not commercial or partisan interests
Rigour: seek evidence to support and challenge their hypotheses, and avoid confirmation-bias
Mutually Supportive: to identify and investigate relationships which may exist with other dimensions



MEASURING THE CURRENT STATE OF CYBER SECURITY

At the core of delivering increased cyber-security capacity is the ability to understand and measure what exists, and how to enhance it.

The centre is gathering and analyzing ideas and best practices in each dimension in order to map the current state of cyber security, and identifying how these different dimensions interact with and depend upon each other. This will enable us to develop the metrics appropriate for measuring the quality and effectiveness of cyber security capacity in each dimension, and reflect on the levels of maturity that can be achieved and under what conditions. Over time the maturity model will provide a benchmark opportunity for capacity in these areas and a mechanism for documenting and testing evolving practices for relevance and usefulness.

Key to this work is effective collaboration with organisations already engaged in capacity-building activities worldwide, and the centre seeks and welcomes the involvement of a global community of experts, from our working groups and beyond.

To find out more about our work and how you can benefit and get involved please visit our website at:
www.oxfordmartin.ox.ac.uk/cybersecurity

Dimension 1 - devising cyber policy and cyber defence

In an era of globalization, technological innovation and rapid expansion of cyberspace, effective national and international cyber security is of critical importance. This working group is examining the best ways of resisting and recovering from cyber intrusions in order to help inform a more effective and comprehensive national and international cyber security policy.

DELIVERING CYBER SECURITY must include capability in early warning, deterrence, resistance and recovery. The scope of this research is to consider the effectiveness of security policy in delivering national defence and resilience capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general.

We would expect a mature cyber security policy to provide the necessary security capacity at all levels of society – government, national infrastructure, businesses, the third sector and individuals. Security capacity must be unobtrusive, yet effective, and must also have the flexibility to deal with new challenges as they arise in order to cope with the ever-changing nature of cyberspace. Consideration must be given to how cyber security fits with more traditional security policy, and the working relationships between the various public bodies involved in keeping cyberspace secure. Government needs a way of coordinating effectively with the custodians of cyberspace in industry. It is also important to consider how to recover from a major cyber intrusion in the event that one succeeds.

At the international level, our work looks at the strategies that peer nation-states and developing countries use to enhance their cyber security capacity, to identify targets for increased collaboration, as well as challenges to effective cooperation. We need to consider international development activities: how these might contribute to national policy in the form of securing states from cyber threats, and how to proceed diplomatically if an intrusion comes from within another jurisdiction. We will also consider whether states using cyberspace to police criminality could or should cooperate internationally to achieve an acceptable level of oversight, while still respecting users' privacy and retaining the benefits of cyber communication. Finally, it is important to examine how governments and communities can effectively inform their adversaries, allies and the public about the shift to a more defensive posture.

Throughout our work we will also consider how cyber security capacity can be built under constraints. Assuming resources are limited, what should be the relative importance of warning, deterrence, defence and recovery? Measures to deter attacks may seem ideal in that they offer to preserve the benefits of cyberspace without distorting the policy environment and society itself. But sustaining a credible deterrent posture in cyberspace presents a number of difficulties and consideration must also therefore be given to defence and recovery. A key aim of the working group is therefore to establish which of these objectives are likely to prove most cost-efficient and effective in terms of policy.

WORKING GROUP

This working group comprises policy makers, national and international defence organisations, together with experts in cyber warfare, and national and international security strategy development. The working group is led jointly by Paul Cornish, Professor of Strategic Studies, Strategy and Security Institute, University of Exeter, and Professor Ivan Toft, Departmental Lecturer, Blavatnik School of Government, University of Oxford

Dimension 2 - encouraging responsible cyber culture within society

Business and industry, governments and civil society are increasingly encouraging consumers and citizens to conduct transactions and participate in civic, social and public affairs online. Networked individuals are also organising activities from the grass roots using social media. For these institutional and citizen-originated initiatives to be successful, networked individuals need to be confident that they are adequately protected in cyberspace. They must be aware of risks, know how to use the Internet safely and securely, and have the time and inclination to take the necessary steps to do so.

THIS WORKING GROUP is conducting research to find out more about individual users' attitudes and beliefs with respect to security and privacy, and what they understand as their cyber responsibilities. This will help determine whether users in general need more support with cyber security, and identify demographic groups who may require particular assistance in accessing services or reassurance that cyberspace is safe to use.

We suspect that individual users are often insufficiently aware of the risks and of best security practices when conducting transactions online. Many citizens see the Internet as a utility and hope to be able to use it safely without having to spend much time and effort on updates. Most other utilities do not require such user input, as safe practices are built into the infrastructure and taught from an early age. As cyber service providers are far from a point at which computing will be provided in such a utility state, users can be left vulnerable to cyber attacks unless adequate measures are taken to protect them, by themselves or others.

It is likely that the answer lies only partly in making people more aware of security threats. Over-stating risks could be counterproductive as it could create a culture of fear around cyber space. This could turn certain groups of people away from the Internet, particularly those who have little experience online, cutting them off from benefits such as better access to education and services. Understanding what consumers and citizens think of cyberspace is the first step in helping them make best use of it.

Our research will compare knowledge and attitudes to responsibility, risks, security and privacy and best practice across different countries and over time. Understanding users is critical to developing cyber security technologies and policies, making it critical for this working group to connect with other dimensions.

WORKING GROUP

This working group is composed of experts who have backgrounds in: social research on the Internet; human behaviour related to security; household security technologies; national policies on security in the areas of privacy and data protection and freedom of expression; survey research; data analytics; and policy analysis. It is co-chaired by Professor Angela Sasse, Director of the Science of Cyber Security Research Institute, UCL, and Professor William Dutton, Professor of Internet Studies, University of Oxford.

Dimension 3 - building cyber skills into the workforce and leadership

Business use of cyberspace has grown rapidly in recent years, and leadership and workforce skills in security risks have struggled to keep up, potentially leaving organisations exposed to threats. This working group is examining the current state of cyber security training and education and identifying what needs to be done to better protect organisations now and in the future.

WE WILL CONSIDER education and training in cyber security for pupils, undergraduates, postgraduates, apprentices, vocational students, general staff, IT specialists, executives and policy makers. We will examine what currently works, what has been tried and failed, and the reasons for this.

Executive training is a key area for our research, as business schools' curricula have traditionally included very little about managing information risks, let alone cyber security ones. Dealing with cyber security has conventionally been a technical issue but there is now an increasing awareness that these risks need to be understood and addressed at executive level.

It is vitally important for business people to understand technical issues, and for security experts to be more aware of corporate needs. Education and training can help spread the message that cyber security cannot solely be the remit of the IT department, but has to be everybody's responsibility. Businesses also need to consider both external and internal risks, such as criminals blackmailing an employee to pass on passwords. Managers need to be made aware of the importance of applying best practice.

There is almost certainly a role for IT specialists within organisations to communicate to junior or senior managers the need for better security. While many will be highly qualified, people enter into the IT industry by diverse routes, and some may also require additional training in certain aspects of cyber security.

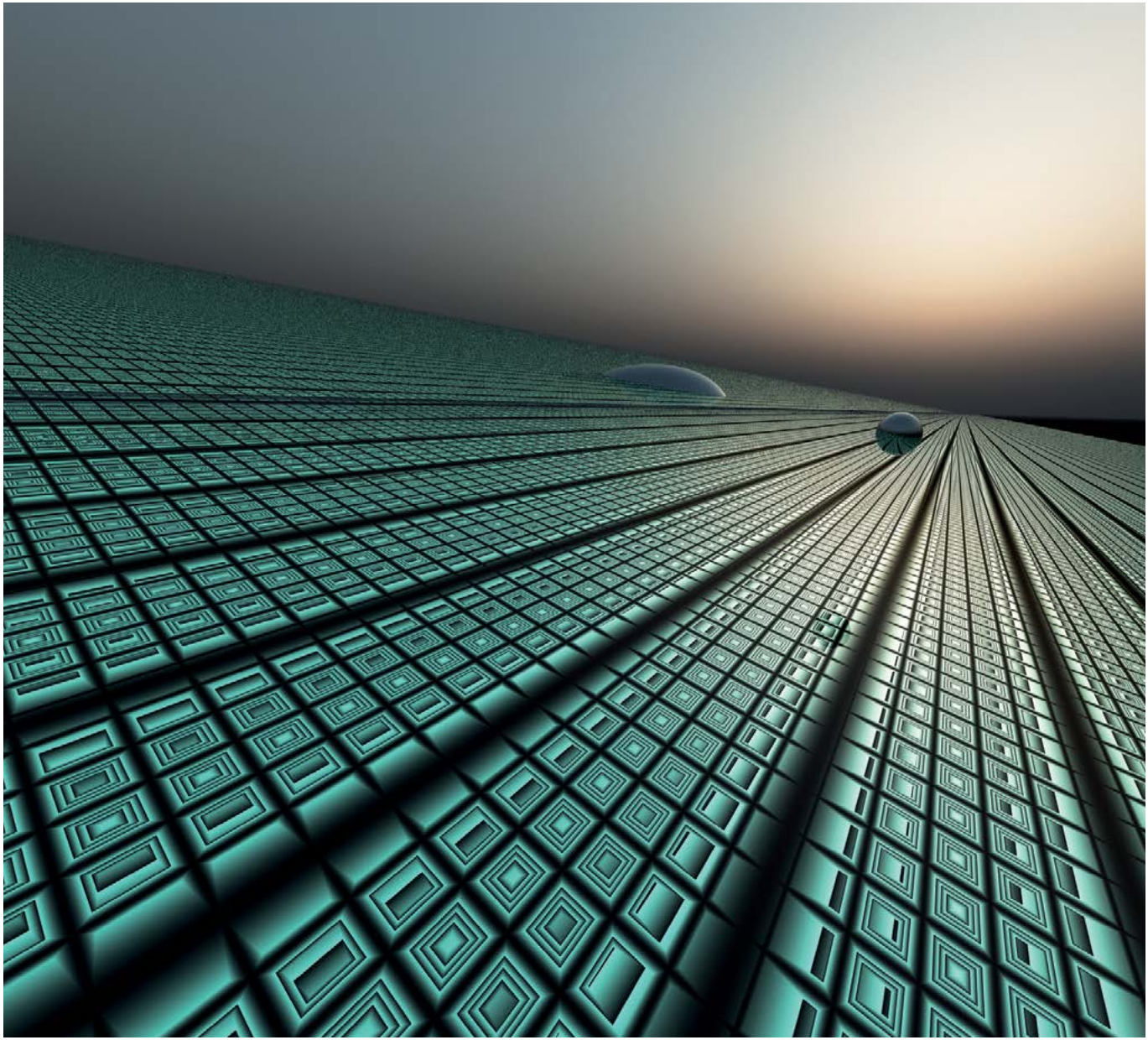
Education in cyber security in schools should both equip pupils to use the internet safely while young and prepare them for their working life. We will be examining how best to add the subject to the curriculum. We need to find out what pupils already know and how the curriculum can help their awareness of cyber security to inform their behaviour as citizens and in the workforce. This is not a straightforward question, because by the time current school pupils enter into employment, the nature of work and the workforce is likely to have changed considerably.

By the end of the research, for each level of education and training, our work will show cases of success and failure, and develop general principals and guidelines to allow organisations to better protect themselves against future cyber attacks.

WORKING GROUP

This working group is composed of representatives from schools and teacher education, university academics, UK and international professional bodies, government Information Assurance skills specialists, and Sector Skills Councils. The group is co-chaired by Andrew Martin, Director of the Centre for Doctoral Training in Cyber Security, University of Oxford, and Professor David Upton, American Standard Companies Professor of Operations Management, University of Oxford.

Dimension 4 - creating effective legal and regulatory frameworks



Organisations, individuals, and governments need to be confident that their data, computer systems and processes are effectively protected in order to reap the full benefits of cyberspace. To achieve this, government intervention is sometimes required, for example to oblige private critical infrastructure providers to develop security risk-management plans. We are investigating how governments can encourage the development of a secure Internet and online environment using law and regulation.

THIS WORKING GROUP will create a set of resources highlighting best practice in all areas of cyber security legislation. Governments across the world will be able to use this to improve their legislative framework, identifying areas where they can do more to protect cyberspace and seeing what steps are required to do so.

To create these resources, we will be examining at a national, regional and international level all the areas of online security that require government action, such as critical national infrastructure, criminal activity, data protection, computer emergency response teams, and education. Criminal activity is one area that receives much attention, but we will be making sure that we also cover legislation that provides incentives for better protection of data and systems: building more resilient systems, deterring an attack, responding after an incident, and from non-malicious actions, such as losing a laptop.

A key issue is how governments can ensure that private critical infrastructure providers meet essential security standards. This is vital because so much of the economy relies on this infrastructure, and breaches can have far-reaching effects. Some countries have asked critical infrastructure providers to voluntarily participate in security standards but there has been limited uptake to date. For the most essential security measures, some governments are considering stronger interventions, and our research will examine the best ways to go about this.

In the area of cybercrime, as well as considering well documented threats, we will be looking at the use of digital equipment in traditional crimes, for example in theft, and consider how the police can make use of new digital technologies without compromising privacy.

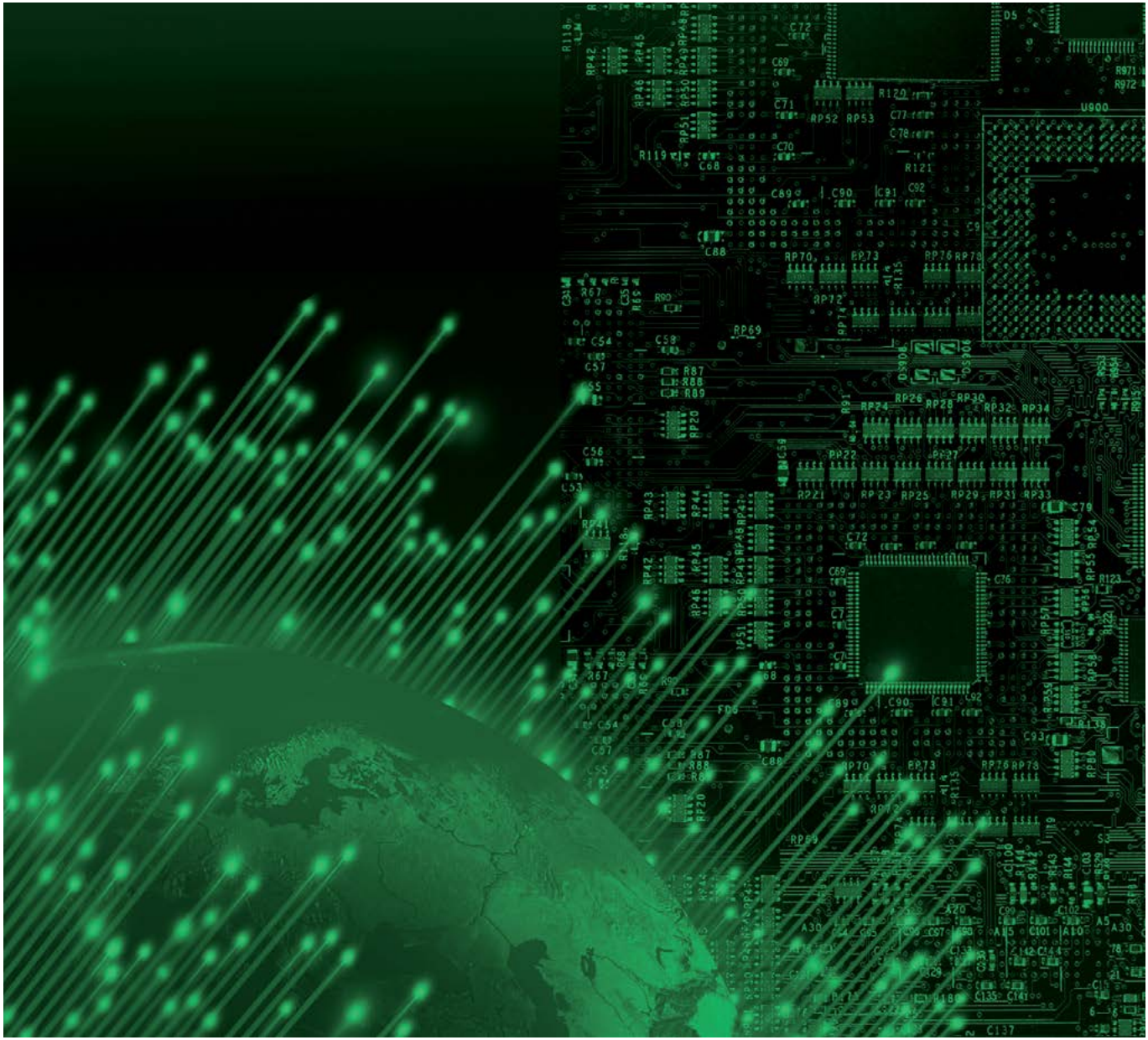
As the effectiveness of laws partially depends on how they are enforced, we will also be looking at the impact of regulatory bodies covering communication and the utilities, and the effectiveness of reporting practices and penalties for data leaks in various countries and regions.

Our research will cover laws and regulations at the global, regional and national level. We will also examine whether national, regional or international approaches are most appropriate for a particular aspect. By the end of the programme, we will have created documents highlighting best practices that will enable policymakers across the world to access knowledge to make decisions on developing effective laws and regulations in their own jurisdictions.

WORKING GROUP

Our working group comprises of international participants from bodies such as the Organisation for Economic Co-operation and Development and the United Nations. Through our members we aim to engage with the experiences of countries of varying size which will help us understand different needs and practices across the globe. The group is co-chaired by Dr Ian Brown, Associate Director of Oxford University's Cyber Security Centre, and Professor Marco Gercke, Director of the Cybercrime Research Institute.

Dimension 5 - controlling risks through technology and processes



Effective and widespread use of cyber security technology, such as firewalls and anti-virus software, is essential to protect individuals, organisations and national infrastructure. We are therefore examining and measuring best practice in the use of technology and associated business processes, and looking at how to ensure good uptake of products.

VIEWS VARY as to what best practice is in the use of security products. This working group will therefore take an independent look at best practice to determine what results in the most effective cyber security.

As well as being used appropriately, security products need to be widely adopted. We will be examining the impact on uptake of the user-friendliness of design, and the optimal configurations of security features to deploy on devices at the time of purchase.

An important consideration regarding uptake is that one cost of security is inconvenience, and this must not outweigh the advantages of the information economy. It is not necessary for everyone to have top-level security –governments' needs are very different from those of the general public. In considering how to encourage greater use of products, we must consider the appropriate security posture for a particular situation.

Business processes around security are also vital, but it is not enough for organisations to simply have a tick-box culture of compliance and training. It is important to think about particular threats to their business and how to react to them. We will try to measure whether organisations have moved to a culture where they are genuinely conscious of, and keen to reduce, the risks from cyber attack.

As well as looking at protection from cyber attacks, we will also examine the tools, structures and processes to help clear up after a security breach and minimise damage. We will be considering which sorts of organisational structure are most effective, and how to protect nations without such a facility, for instance by sharing in regional provision.

Throughout the different strands to this dimension, we will be seeking out projects that are being conducted across the world to help our research, and comparing their success. We will consider whether national initiatives are more or less effective than transnational ones, or whether regional activities would produce better results. We will also examine whether it is better to have various international forums to work on these areas, or if it would be more effective to combine them. The results should allow countries to see what really works in this area, and where there are gaps in their knowledge and approach.

WORKING GROUP

This working group is composed of experts in cyber risk control technologies, operational practices, security usability, trustworthy technology, risk assessment and the security markets, communications and public relations and cyber insurance products. It is co-chaired by Professor Michael Goldsmith, Senior Research Fellow at the Department of Computer Science, University of Oxford, and Professor Fred Piper, Emeritus Professor at Royal Holloway, University of London.

The Global Cyber Security Capacity Centre is funded by the United Kingdom Foreign and Commonwealth Office and hosted by the Oxford Martin School

Global
Cyber Security
Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Oxford Martin School, University of Oxford, Old Indian Institute, 34 Broad Street, Oxford OX1 3BD, United Kingdom
Email: cybercapacity@oxfordmartin.ox.ac.uk • Tel: +44 (0)1865 287430 • Fax: +44 (0)1865 287435 • www.oxfordmartin.ox.ac.uk/cybersecurity