OCSC

Oceania Cyber Security Centre

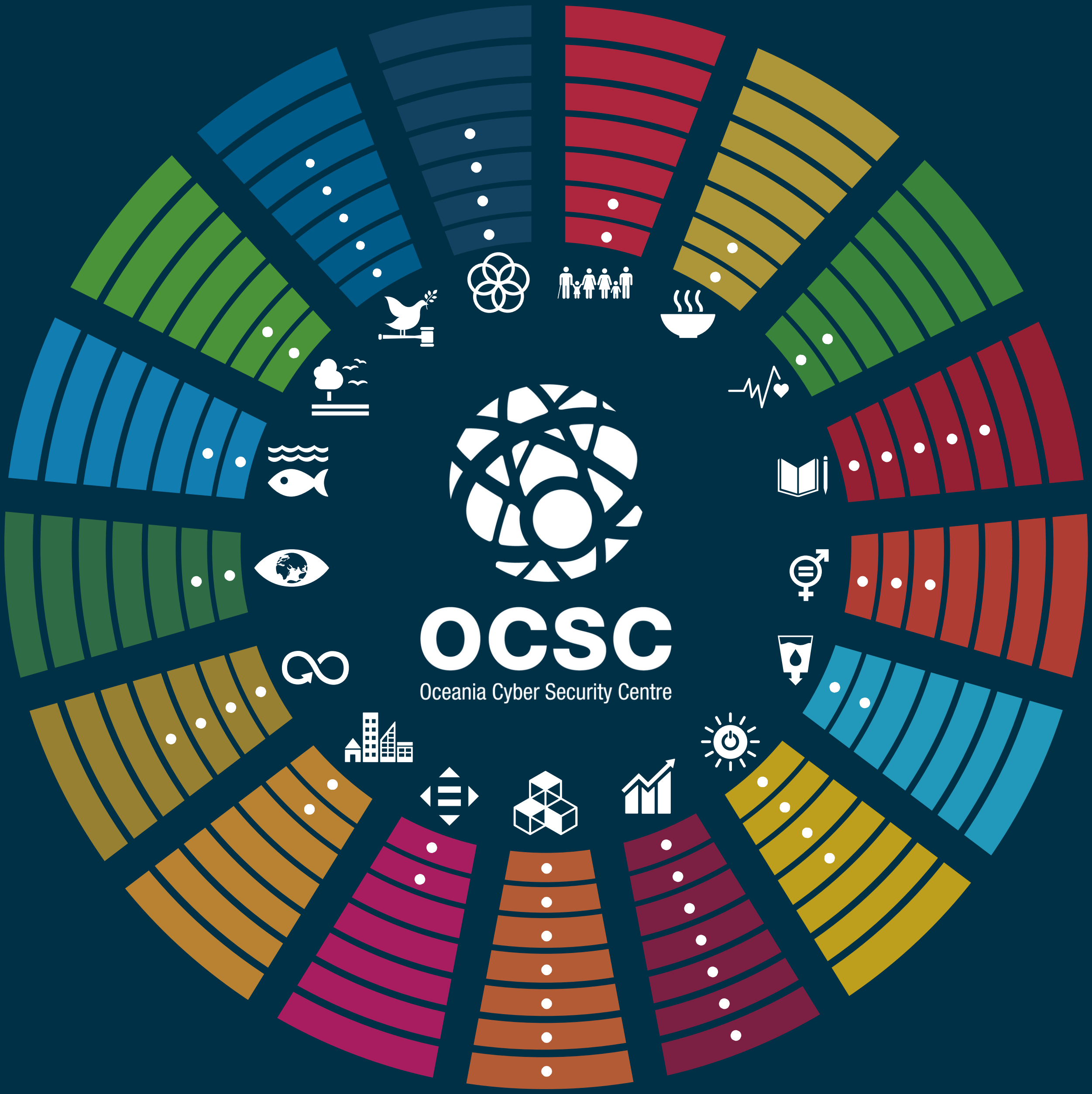
CYBERSECURITY AND SUSTAINABLE DEVELOPMENT

An Intersectional Analysis

2022

TABLE OF CONTENTS

OCSC AND THE 2030 AGENDA



This diagram is based on a combined thematic analysis of the SDG indicator framework and the Cybersecurity Capacity Maturity Model for Nations, which is outlined below. According to this analysis, each dot represents a development theme that OCSC helps to advance under the prescribed SDG. There are five themes altogether: people, prosperity, peace, partnership, and planet. It provides a visual snapshot of the contributions OCSC is making toward the Sustainable Development Agenda.

SUSTAINABLE DEVELOPMENT GOALS

1 NO POVERTY

End Poverty in all its forms everywhere.

2 ZERO HUNGER

End hunger, achieve food security and improved nutrition and promote sustainable agriculture.

3 GOOD HEALTH AND WELL-BEING

Ensure healthy lives and ensure well-being for all at all ages.

4 QUALITY EDUCATION

Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all.

5 GENDER EQUALITY

Achieve gender equality and empower all women and girls.

6 CLEAN WATER AND SANITATION

Ensure availability and sustainable management of water and sanitation for all.

7 AFFORDABLE AND CLEAN ENERGY

Ensure access to affordable, reliable, sustainable and modern energy for all.

8 DECENT WORK AND ECONOMIC GROWTH

Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all.

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

Build resilient infrastructure, promote inclusive and sustainable industrialisation and foster innovation.

10 REDUCED INEQUALITIES

Reduce inequality within and among countries.

11 SUSTAINABLE CITIES AND COMMUNITIES

Make cities and human settlements inclusive, safe, resilient and sustainable.

12 RESPONSIBLE CONSUMPTION AND PRODUCTION

Ensure sustainable consumption and production patterns.

13 CLIMATE ACTION

Take urgent action to combat climate change and its impacts.

14 LIFE BELOW WATER

Conserve and sustainably use the oceans, seas and marine resources for sustainable development.

15 LIFE ON LAND

Protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reserve land degradation and halt biodiversity.

16 PEACE, JUSTICE AND STRONG INSTITUTIONS

Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels.

17 PARTNERSHIPS FOR THE GOALS

Strengthen the means of implementation and revitalise the global partnership for sustainable development.

ABOUT THE OCSC

The Oceania Cyber Security Centre (OCSC) is a not-for-profit research and capacity building centre, based in Melbourne, Australia. The Centre is comprised of eight member universities with more than one hundred and twenty experts from a broad spectrum of cybersecurity disciplines including:

- Policy and strategy;
- Human factors and culture;
- Education, training;
- Law, regulation and online safety; and
- Incident response, technical controls and standards.

As a founding member of the Global Constellation of Regional Cyber Capacity Centres, we conduct national cybersecurity reviews and related research using the Cybersecurity Capacity Maturity Model for Nations (CMM). The members of the Global Constellation include:

- OCSC in Melbourne;
- Global Cyber Security Capacity Centre (GCSCC), University of Oxford, UK; and
- Cybersecurity Capacity Centre for Southern Africa (C3SA), based in Cape Town, South Africa.

A CMM review helps countries to benchmark their capacity and identify priorities for strengthening that capacity on the next steps of the cybersecurity maturity journey.

Following a CMM review, the OCSC works with the partner nation to co-develop an evidence-based National Cybersecurity Roadmap informed by the CMM review, key local stakeholders and research. Thus the Roadmap is responsive to the country's own priorities and context and aligned with existing local and regional programs to avoid duplication, guiding the country through the revision or development and implementation of their National Cybersecurity Strategy. A further CMM review in the future can assess the progress and impact of implementation.

As a research and capacity building centre, the OCSC also provides expert independent evaluation for specific programs or problems to understand what works, what doesn't work and why.

METHODOLOGY

The Sustainable Development Goals identify the international community's shared development objectives and benchmark sustainable development progress. How the SDGs are accomplished are set out in the 169 targets of the Global Indicator Framework for the Sustainable Development Goals, which measure advancements towards the goals and track accountability.

To determine the significance of cybersecurity in the 2030 Agenda and to identify OCSC's role in accomplishing the goals, this report has performed a thematic analysis of the SDG Global Indicator Framework and the Cybersecurity Capacity Maturity Model for Nations (CMM). In doing so, it has established how the CMM helps to fulfil the SDGs.

This review began by analysing each of the 169 targets and identified where technology and cybersecurity could contribute to development progress. The selected indicators were then reviewed against the CMM to determine which ones would benefit from Cybersecurity Capacity Building (CCB). In total, sixty targets spread across all the goals were identified.

The CMM was then coded into different areas of impact according to the five themes of the SDGs: peace, prosperity, people, planet and partnerships. For example, factors 1.1, 4.4 and 5.1 were coded as Development Networks under the Partnerships theme, indicating that these factors of the CMM may facilitate development networks that advance the partnerships aspects of the goals. The codes were then applied to the indicators they correlated to. For instance, indicator 16.3 'Promote the rule of law at the national and international level and ensure equal access to justice for all' received a Development Networks code. Meaning that the factors of that code contributed to the advancement of that indicator. This process directly identifies the impact the CMM has on each goal.

By doing this, the research has traced a direct line between the work of the OCSC and the Sustainable Development Goals and identified the contribution cybersecurity capacity building has in achieving the 2030 Agenda.

For brevity, the complete Thematic Analysis code book is available upon request.

Research Team

Joe Fulwood: Lead Researcher.

Jaime Morrison: Researcher.

Dr James Boorman: Research Supervisor.

A/Prof Carsten Rudolph: Research Supervisor.

INTRODUCTION

This report analyses the relationship between Cybersecurity Capacity Building (CCB) and the United Nations Sustainable Development Goals (UNSDGs) and investigates how the activities of OCSC, particularly of the Cybersecurity Capacity Maturity Model for Nations (CMM), contribute to achieving the 2030 Agenda. It begins by outlining the relationship between Information and Communications Technologies (ICTs) and sustainable development and demonstrates the role cybersecurity plays in achieving the goals. It then presents a thematic analysis of the CMM's overlap with the SDGs and gives a detailed outline of how the dimensions specifically address the SDG indicators under the SDGs five core themes identified: peace, prosperity, people, planet and partnerships.

While the exact definition of cybersecurity is contested, for the purpose of this report it should be broadly understood as the effort to combat the multifaceted "threat landscape" associated with cyberspace.[1] It is the practice of preserving the confidentiality, integrity, authenticity and availability of digital information, protecting underlying infrastructure and ensuring confidence in digital services.[2] A broad mix of technical, policy and educational measures are needed to advance cybersecurity to address the full spectrum of modern cyber threats. While cybersecurity is closely linked with ICTs, the traditional techno-centric approach is misguided. A more holistic perspective that equally incorporates technical and human factors is necessary to build sustainable cybersecurity resilience into the future.[3]

The CMM is designed with these holistic principles in mind. The review includes developing a national cybersecurity policy and strategy; encouraging a responsible cybersecurity culture within society; building cybersecurity knowledge and capabilities of the existing and future workforce; creating effective legal and regularity frameworks, and controlling risks through standards and technologies. Together the five dimensions of the CMM represent the breadth of national capacity that is required of a country to deliver cybersecurity effectively.

D1. Cybersecurity Policy and Strategy.

D2. Cybersecurity Culture and Society.

D3. Building Cybersecurity Knowledge and Capabilities.

D4. Legal and Regulatory Frameworks; and

D5. Standards and Technologies.[4]

CYBERSECURITY CAPACITY BUILDING AND SUSTAINABLE DEVELOPMENT

Digital development and cybersecurity are two sides of the same coin - a greater understanding of the threats challenging the ICT sector, and building resilience capabilities to them, is necessary for enabling the adoption of digital opportunities and maximising technology as a means of sustainable and inclusive development.[5] As development agencies and donors rush to expand access to ICTs and their development benefits, there must also be a sustained effort to build resilience at a similar pace or risk losing these benefits altogether. OCSC is working to create alignment between resilience and development through its CCB efforts, subsequently helping to fulfil the UNSDGs and achieve the 2030 Agenda. While CCB is not the explicit aim of any of the goals themselves, it is a cross-cutting concern embedded within the SDGs, which OCSC has both a direct and indirect role in developing.[6]

ICTs and the Sustainable Development Goals

ICTs have the capacity to enhance all of the Sustainable Development Goals (SDGs) collectively. Development, technology and achieving the goals are all inextricably linked and interdependent.[7] ICTs facilitate access to essential and high-quality goods and services across various industries and governance systems and can directly reduce poverty, hunger, environmental degradation, and poor health.[8] They help to improve services, increase productivity, decrease costs, enhance ecological monitoring systems, streamline management structures, and facilitate 'intelligent' development.[9] ICTs have subsequently become one of the principal components of economic growth in the twenty-first century. [10]

Cyber Capacity Building and the Sustainable Development Goals

The realisation of these benefits will be limited if not supported by holistic capacity-building efforts to strengthen resilience across all dimensions of cybersecurity. The United Nations Group of Governmental Experts has recognised CCB as an essential element in the sustainable spread of ICTs. [11] A strong ICT sector depends on robust and effective technical controls, appropriate legislation, strategies and regulation, and a skilled technical workforce.[12] Digitised critical infrastructure systems, e-commerce and e-governance, and data analytics are all vital elements of modern sustainable development opportunities, but without resilience, they remain vulnerable to exploitation and unreliable as methods of achieving the SDGs. Furthermore, populations with lower digital literacy skills remain susceptible to online exploitation. This negates the benefits of digital development and constraining progress in the SDGs.

Consequently, CCB is essential in developing communities and economies capable of capturing the benefits of ICT developments, and resilience should be considered at the heart of all future digital development planning. Consequently, the work of the OCSC actively contributes to advancing this development model. Across the Indo-Pacific the centre facilitates progress toward each SDG by deploying the CMM and co-developing National Cybersecurity Roadmaps.

The following table provides a snapshot of the potential impacts ICT developments have on each SDG and the cybersecurity challenges that accompany them. It is not an exhaustive list but seeks to contextualise the role of CCB in achieving the 2030 agenda.

DEVELOPMENT GOAL	ICT DEVELOPMENT IMPACT	CYBERSECURITY CHALLENGE
1. No Poverty	ICTs are critical in supporting market modernisation which advances poverty reduction through rapid economic growth. Economic growth is arguably one of the best forms of poverty reduction and ICTs have a large role to play in modern economic development which could have significant impacts on poverty reduction if they are universalised and distributed in an inclusive manner. ICTs can also increase access to digital financial services. [13]	Poorly designed technological products create space for cybercriminals to exploit market digitisation and undermine the economic benefits of ICT development. ICTs will struggle to have a net-benefit in poverty reduction if they also expose users to criminal activity which could leave them worse off than before.
2. Zero Hunger	Technology helps to increase agricultural resource efficiency & optimises productivity through the digitisation of production and distribution processes. ICTs help to improve supply chain coordination and reduce management costs making more food available to more people. [14]	The technologies and computer systems directly and indirectly involved in digitised food production need adequate protection from malicious actors who could disrupt production and distribution, and consequently destabilise supply chains and generate food insecurity.
3. Good Health and Well-Being	ICTs help to increase medical coverage and enhance care through the improvement of healthcare infrastructure and the digitisation of health services such as telemedicine, remote medical screening, digital health records, etc.[15]	Digital health services are vulnerable to attacks due to a historical lack of cybersecurity investment in the sector. This has left patient data, health infrastructure, and even individual patient devices exposed to cyber-attacks. Such attacks could bring the health system to a standstill, cause untold psychological harm, and even cost lives.
4. Quality Education	ICTs have created a new era of digital learning which has expanded access to education through online teaching and digital skills development. Unrestricted access to educational platforms and content, and enhanced connectivity and collaboration between schools has made education more sustainable. ICTs will continue to be the gateway to sustainable education into the future. [16]	Data breaches are of major concern to educational institutions, but as learning has increasingly moved online or into hybrid arrangements, the instruments of teaching are also at risk. The operation of digital education will cease under a cyber-attack and therefore cybersecurity must be seen as an enabler of sustainable education.
5. Gender Equality	ICTs have helped to empower women by providing greater access to employment opportunities and essential services, such as health and education, which they have historically been excluded from. They have also aided the development of women's support and mentorship networks.[17]	ICTs can open new opportunities to women, but they also present new avenues for cyberviolence and exploitation against women. Holistic cybersecurity is an important element of protecting women's rights and freedoms online and is key to ensuring women maintain access to the positive digital opportunities which ICTs present.

6. Clean Water and Sanitation	ICTs increase efficiency in water management through smart sanitation and monitoring technologies. [18]	ICTs are a growing component in modern water facilities which are increasingly vulnerable to cyber threats. Technology which manages data and controls physical operating procedures are essential to modern water treatment and distribution systems, and without the proper protections this technology remains vulnerable to attacks which could disrupt services and produce water shortages.
7. Affordable and Clean Energy	Electricity grids increasingly use ICT technology which helps to reduce costs and consumption through enhanced efficiency, while enabling the uptake of new clean energy production and distribution.[19]	Technology enhanced grids are susceptible to cyber-attacks which can increase electricity prices and paralyse renewable energy sources and smart grids. Therefore, they are a risk to sustainable energy production and development.
8. Decent Work and Economic Growth	ICTs are drivers of economic innovation and growth. They help nurture skilled human capital, reduce volatility, bolster capital markets and shape dynamic economies which create new jobs through digital development. The internet, new technologies and global growth reinforce each other. [20]	While new technologies can boost economic growth, unfortunately they also open new avenues for cybercrime which can negate these benefits. Globally 1% of GDP (US S600 billion) is lost to cybercrime a year. Cybersecurity is necessary in sustaining growth and maintaining the digital economy behind it.
9. Improved Infrastructure	ICTs can be utilised to upgrade the scope, access, and quality of infrastructure networks. The presence of innovative new and flexible infrastructure to meet different climates and demands can assist in creating the environment necessary for economic development to flourish.[21]	Cyber vulnerabilities within improved infrastructure developments must be addressed in order to ensure that new infrastructure networks are resilient and functional. If adequate cybersecurity measures are not developed alongside improved infrastructure development, then the efficiency of this development is inherently threatened as networks will not be able to withstand malicious cyber-attacks.
10. Reduced Inequalities	Increasing access to ICTs can reduce inequalities within societies by enabling vulnerable and marginalised people greater access to support services. ICTs can, for example, facilitate the participation of the elderly, indigenous, people living with disabilities, and and other marginalised groups in new activities. [22]	A digitally underdeveloped country with a high level of cyber inequality may lead to marginalised groups having a heightened vulnerability to cyber insecurity issues which further entrench inequalities. These cyber issues include human trafficking and cyberbullying and can far outweigh the benefits of ICT developments. Adequate cybersecurity is therefore necessary to help reduce inequality and protect marginalised communities.

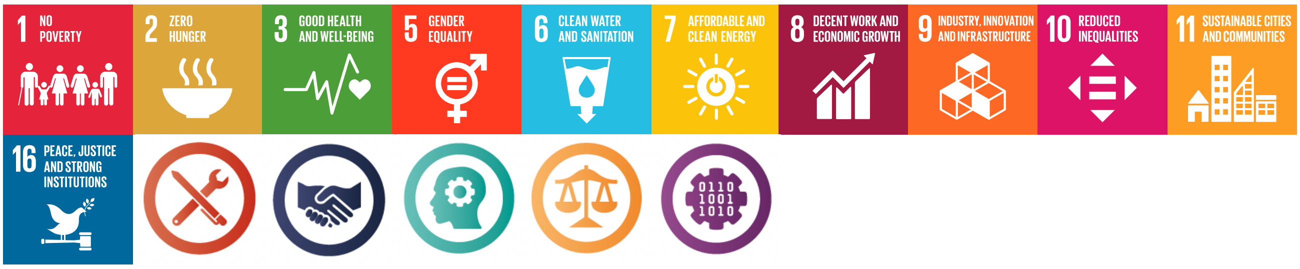
11. Sustainable Cities and Communities	ICTs can contribute to the development of smart cities with efficient and clean services, infrastructure, and lifestyles. Furthermore, ICTs can be used within governance partnerships to link communities and ensure sustainable objectives in the development of cities and communities.[23]	Cities are often the target of cyber criminals and cyber-attacks can potentially disrupt key elements of city life such as police services, water, sanitation, energy and transport. For example, in 2020, New York City faced over USDS2.3b in cyber-related losses largely due to cyber-attacks against city infrastructure.
12. Responsible Consumption and Production	ICTs can be used to achieve lean manufacturing and efficient goods production, as well as enhanced waste management services as evidenced in the European NIS2 directive.[24]	The challenge within this relates to potential cyber-attacks against the systems responsible for consumption and production, such as waste management.[25]
13. Climate Change Action	ICTs are increasingly relevant in advancing environmental sustainability. They help to produce climate modelling and advanced low emissions technologies. ICTs can also be integrated into climate change mitigation, adaptation, and early warning efforts.[26]	Cybersecurity is an important part of our efforts to stop climate change. It maintains vital critical infrastructure, including for example water supply networks and low-emissions energy systems, which help to reduce emissions and advanced resilience.
14. Life Below Water	ICTs may improve marine monitoring abilities, undersea knowledge and contribute to pollution reduction technology and mechanisms. ICTs and cybersecurity can also be used to regulate the illegal wildlife trade, which includes marine animals such as sharks.[27]	Cybersecurity is a key component in combatting Cyberpoachers' who operate in an unregulated online market and is therefore, integral to protecting marine life from the illegal animal trade. It is also necessary for safeguarding marine monitoring abilities and plastic pollution reduction technologies.
15. Life on Land	Digital technologies are utilised to protect wildlife, including from illegal poaching. These technologies include thermal cameras, surveillance technologies and communication equipment. This technology can safeguard biodiversity through enhanced wildlife monitoring and protection capabilities.[28]	These technologies are vulnerable to cyber-attack which undermine their development contributions and endanger native species. Adequate cybersecurity protections are vital to ensuring that wildlife monitoring and protection capabilities are safeguarded.

16. Peace, Justice and Strong Institutions	ICTs can provide greater access to information and data, ensuring transparency and citizen empowerment. ICTs can be utilised for peacebuilding, crisis management and human rights promotion. In the effort to achieve this, multiple stakeholders must collaborate in order to ensure ICT best practice.[29]	Under educated and ill-equipped users are highly exposed to cybercrime. As in the physical world, criminal acts carried out in the digital sphere undermine the core principles of peace and justice and erode the criminal justice institutions responsible for maintaining law and order.
17. The Power of Partnerships	ICTs enable global collaborative networks and capacity building through digital cooperation and communication should be pursued. Collaboration between the public and private sector, as well as civil society and experts is vital to ensuring that ICTs are used for effective partnerships and governance.[30]	Underdeveloped partnerships challenge the effective governance of cybersecurity and are thus invaluable to achieving all the previous goals. Fragmented international cyber regulation and governance fails to facilitate the necessary international consistency needed for a stable cyberspace which is crucial in enabling the positive development opportunities afforded by ICTs.

OCSC AND THE SUSTAINABLE DEVELOPMENT GOALS

Following the contextualisation of cybersecurity's role in sustainable development, this report will now present the thematic analysis of the SDG Indicator Framework and the CMM to outline the specific alignment between the OCSC's work and the 2030 agenda. Digital sustainable development has been qualitatively coded across five themes: peace, prosperity, people, planet and partnerships. The following analysis investigates the SDGs and the CMM and establishes how the CMM contributes to the SDGs under these themes. The themes are cross-cutting and intersectional, and many of the goals and dimensions of the CMM contribute to sustainable cyber development across multiple different areas.

Peace


1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
0110
1001
1010

Peace and security are foundational elements of the SDGs that are both undermined in an unstable and unregulated digital environment. Failure to protect users from online exploitation or defend the critical infrastructure needed to safeguard citizens' wellbeing threatens these aspects of the SDGs. Consequently, cybersecurity has a decisive role in ensuring that critical digital infrastructure remains safe, reliable and operable. This theme has analysed which goals are inherently tied to the advancement of digital pace and security and identified the contribution the CMM makes toward progressing cyber peace and stabilising critical digital infrastructure.

The 2030 Agenda and the SDGs incorporate a broad understanding of security that goes beyond the traditional state focus by prioritising the rights and dignity of individuals.[31] Within the goals, there is an underlying commitment to prioritising the protection of individuals and advancing development strategies that produce resilient and safe societies where people experience freedom from fear, want and indignity.[32] The development agenda employs a triangular nexus that brings together security, development and human rights to address the root cause of instability and inequality and facilitate inclusive and sustainable development that enables people to prosper.[33] Whether this is individual liberties and human rights, or access to the essential goods and services necessary for a quality life, the dignity and well-being of people are what is prioritised. This security perspective is something the SDGs and the CMM share; they are both committed to helping end practices of violence and exploitation, developing institutions that protect human rights, and building infrastructure resilience in order to protect the public from harmful disruptions.

Individual rights and protections are advanced under Dimensions 2, 3, and 4 of the CMM through a mixture of legal, strategic and cultural capacity building. The CMM helps develop systems that translate fundamental human rights to digital environments, while also equipping users with an improved cybersecurity mindset that allows them to protect themselves better online. Cyberspace is a fertile environment for modern criminal activity, such as labour exploitation, modern slavery and child exploitation, which the CMM helps to prioritise by identifying existing legislative and strategic gaps.[34]

Perpetrators of these crimes are increasingly using modern digital technology to achieve their ends. Subsequently, greater digital resilience and awareness are necessary to combat the problem. In assessing nations' legal and regulatory frameworks against Dimension 4, the CMM assessment provides recommendations on legislating a safe digital operating environment that respects human rights. This may include cross-sector regulatory bodies, child protection measures, and cybercrime cooperation frameworks. In addition to this, Dimension 2 of the CMM assesses the national cyberculture and works to limit individuals' exposure to exploitation through advancing cultural awareness, limiting disinformation, and establishing reporting mechanisms. By identifying these gaps, the CMM helps extend the rule of law to digital platforms and environments and promotes fundamental human freedoms consistent with Goals 8 and 16.

Furthermore, developing individuals' rights is especially important for protecting already vulnerable people and communities, specifically advancing Goal 5 on Gender Equality and Goal 10 on Reduced Inequalities. For instance, gender-based cyber violence is a growing issue worldwide that can take many forms and is a core obstacle to achieving Goal 5 on Gender Equality.[35] According to the Council of Europe, 58% of women have experienced online harassment, with most saying they experienced more online harassment than street harassment.[36] This highlights the pervasive and pressing nature of the issue. Factor 4.1 of the CMM assesses national cybercrime legislation, while 4.3 analyses the capacity of law enforcement to investigate and prosecute cybercrimes. These factors collectively identify gaps in the existing criminal justice framework, which can help foster a holistic and effective legal environment that protects women from cyber violence and advances Goal 5.

In addition to advancing individuals' rights and freedoms, the goals emphasise promoting individuals' access to essential services and protecting the critical infrastructure enabling these services. Under goals 1, 2, 3, 6, 7 and 11, there are indicators committed to ensuring universal access to food, health, clean water and clean energy, while goal 9 seeks to develop reliable and accessible infrastructure that supports individual well-being. The CMM helps to accomplish these goals by identifying and securitisation critical digital infrastructure. Given that cybersecurity is intrinsic in maintaining modern infrastructure built with ICTs,[37] by helping to identify this infrastructure and building strategies to protect it under Dimensions 1 and 5, the CMM assists in stabilising the delivery and development of essential services. By securitising ICT infrastructure, the CMM is helping to advance the goals by ensuring the longevity of ICT development benefits and helping to protect the rights and dignity of users. Collectively, the outputs of the CMM assessment generate practical recommendations which can be adopted to strengthen human security in cyberspace, thereby fostering a safe and peaceful digital environment that grants individuals freedom from fear, want, and indignity.

Prosperity

1 NO POVERTY
2 ZERO HUNGER
4 QUALITY EDUCATION
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
11 SUSTAINABLE CITIES AND COMMUNITIES
0110
1001
1010

Economic development or prosperity is a critical component of the SDGs that is fundamentally linked with cybersecurity. Digital development has become a modern economic powerhouse with vast potential to improve people's quality of life and advance the SDGs.[36] For example, today's global digital economy represents around 20% of the world's total GDP, and in Australia alone, between 2019 and 2020, digital activity added 7.4% (7.5 billion AUD) to the economy.[39] This theme analyses the symbiotic relationship between cybersecurity, ICTs and economic growth, and how the CMM contributes to greater prosperity by facilitating digital infrastructure development and advancing employment opportunities.

The 2030 agenda emphasises promoting inclusive economic development to raise global living standards and advance human prosperity. Goals 1, 2, 8, 9 and 11 all include advancing economic growth as a means of increasing human well-being and ensuring sustainable prosperity. Resilient and sustainable critical digital infrastructure is foundational to successful digital transformation efforts that can drive both economic growth and development.[40] As is the case for securing a safe and peaceful society, resilient critical infrastructure is also essential for securing the economic benefits of ICT developments.

Establishing cyber resilience can assist in creating an environment that not only facilitates innovation but captures the economic benefits of digital advancements.[41] Service outages and cybercrime cost the global economy billions each year and threaten to undermine the economic benefits that stem from the digitisation of global markets and the spread of technology.[42] Additionally, insufficient cybersecurity strategy, policy, understanding of risk, standardisation, and regulation can inhibit the ability of countries and businesses to participate in the global digital economy.[43] Therefore, resilient critical digital infrastructure is necessary for overall economic digitisation and translating its benefits into human terms. Dimensions 1 and 5 of the CMM help stabilise critical infrastructure and prevent cyber-based economic shocks by helping countries identify digital infrastructure and form strategies to protect it. In doing so, the CMM lays the groundwork for a stable and prosperous digital economy that advances economic development in line with the SDGs.

Goals 4, 8, and 9 also promote economic development's positive employment aspects, which improved cybersecurity capabilities can enhance. These goals each advocate for greater education opportunities that boost employment and innovation to facilitate economic growth. Advanced cybersecurity skills and knowledge are increasingly valuable and sought-after abilities that significantly improve employability in the modern digital economy. In Australia for example there is a need for another 17,000 cyber professionals by 2026.[44] Dimension 3 of the CMM assesses the availability and quality of cybersecurity education and professional development opportunities within countries and helps to establish fit-for-purpose education environments that meet the digital demands of the modern workforce. In addition to this, it reviews the national emphasis on cybersecurity research and innovation and elevates the importance of cybersecurity innovation as a means of sustainable development in the national conscience. Subsequently, the CMM helps to fulfil the objectives of Goals 4, 8 and 9 by laying the foundations for a technically equipped cyber-literate workforce.

People

4 QUALITY EDUCATION
5 GENDER EQUALITY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
0110 1001 1010

Equal access to goods, services and opportunities and the empowerment of marginalised groups are consistent themes within the SDGs. Many digital developments have the ability to promote positive social change by removing access barriers and providing new opportunities.[45] However, the inverse is also true; if users are left unprotected, they will become exposed to the many negative aspects and experiences of ICTs. Enhanced cyber maturity helps to mediate the adverse effects of digital development and subsequently advance the social aspects of the SDGs. The CMM includes regulatory and educational Dimensions which foster a safe and inclusive digital environment that facilitates positive social developments. This theme incorporates the areas of inclusion, empowerment, knowledge and education and demonstrates the positive social outcomes the CMM produces.

Under Goal 4 Quality Education and Goal 9 Industry, Innovation and Infrastructure, there are indicators focusing on universalising access to education and future infrastructure development, which digital solutions can help achieve. New technologies provide innovative new methods of building infrastructure and teaching that remove traditional barriers and advance universal access.[46] Furthermore, by helping to improve accessibility and empowering people to participate in society, ICTs also help fulfil the objectives of Goals 5 Gender Equality and 10 Reduced Inequalities. Advanced digital society can function to connect more vulnerable and marginalised people with essential services, social opportunities, and jobs. However, for these benefits to be realised, there needs to be a stable digital environment and resilient critical infrastructure, which the CMM helps to facilitate under Dimensions 1 and 5.

Another underlying social theme within the SDGs was the availability of education and knowledge. Goals 4 and 8 both include indicators that address quality and accessible education opportunities for people young and old in various formats. Cybersecurity knowledge and education are integral components of all quality modern education systems, given their prevalence and growing importance. Dimension 3 of the CMM focuses on building cybersecurity knowledge and capabilities and reviews the availability and quality of cybersecurity education opportunities across nations. The assessment of this dimension provides recommendations for how high-quality training programs can be implemented to improve students' and professionals' cyber literacy and develop an adequately skilled digital workforce. Furthermore, it reviews the training processes of educators to enhance the quality of digital education, helping to establish a holistic education approach. This dimension directly contributes to Goals 4 and 8 of the SDGs by helping to expand access to education, upskill workforces and advance the capabilities of teachers.

Planet

2 ZERO HUNGER
6 CLEAN WATER AND SANITATION
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
0110
1001
1010

Technology is a central element in the global battle to preserve ecosystems, combat climate change, and limit humanity's negative impact on the environment.[47] Cybersecurity plays a contributing role in facilitating technology-based adaptation and mitigation efforts to sustain our environment. This theme assesses the environmentally-focused SDGs and identifies the additive function the CMM has in promoting these SDGs. It focuses on environmental sustainability and prosperity.

Strengthened digital and cybersecurity infrastructure enables the consistent and efficient management of environmental resources and allows authorities to better prepare for natural disasters.[48] Digitally resilient sustainable infrastructure also ensures the continued operation of essential services for managing and preventing human environmental impacts (i.e. renewable energy).[49] Goal 9 specifically references upgrading infrastructure to ensure that it is sustainable and incorporates environmentally sound technologies. Goals 2, 6, 8 and 11 also include environmental aspects and require resilient digital infrastructure to fulfil their aims. The CMM assesses critical infrastructure protection in Dimensions 1 and 5, which can help build resilience by identifying gaps in existing protection strategies and encouraging reviews that improve regulatory and operating procedures.

Goals 13, 14 and 15 relate directly to preserving the natural environment and mitigating human impacts. Again, ICTs are set to play a significant role in achieving these goals as modern technology enables new forms of monitoring and evaluation and assessment impact. Evidence-informed systems change can reduce waste and environmentally detrimental human outputs, and increase resource efficiency and sustainability.

Additionally, Goal 14 and Goal 15 outline the aims of protecting marine ecosystems and animals and ending illegal wildlife poaching sales online. Under Dimension 4, The CMM helps identify gaps in national legal frameworks that enable online criminal behaviour and deficiencies in the justice system to hold such criminals accountable. Therefore, it assists in establishing the criminal justice frameworks necessary for sustainable development to occur and prevents ICT development from exacerbating environmental issues.

Partnerships

1 NO POVERTY
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
0110
1001
1010

Given the interconnected nature of the SDGs, they cannot be achieved by a single actor alone. Instead, they require a series of local and global partnerships and cooperative stakeholders who engage in collaborative sustainable governance. Effective CCB is the same, it requires a multistakeholder response involving a variety of key actors, including supranational organisations, national governments, the private sector, civil society and cybersecurity experts. This need for advanced partnerships and governance is acknowledged within both the CMM and the SDGs, and this theme investigates the overlap between them. It addresses collaboration, legislation, policy, governance issues and international cooperation and demonstrates how the CMM facilitates meaningful governance partnerships.

Goal 17 on Partnerships for the Goals specifically aims to strengthen the global partnerships advancing the 2030 agenda, including enhancing international resources and knowledge sharing. The goal strives to fully operationalise technological developments in every country and emphasises targeted and effective capacity-building efforts. As a development practitioner operating within a global constellation in coordination with international governments, OCSC actively advances this goal through its multistakeholder approach, which shares knowledge, expertise, and financial resources with low and middle-income countries. Within the CMM specifically, Dimensions 1, 4 and 5 all examine international collaboration on cybersecurity concerning strategy, legislative frameworks, and standards. The reviews strongly emphasise a transnational and multistakeholder approach to CBB and position cyber-development in a collaborative governance space. In addition to goal 17, Goals 1, 9, 12 and 16 all strive for closer international capacity building cooperation in their various areas which OCSC and the CMM help facilitate.

REFERENCES

1. Russell Buchan. 2018. 'Cyber-security'. https://www.oxfordreference.com/view/10.1093/acref/9780199670840.001.0001/acref-9780199670840-e-1636
2. ITU. 2018. 'ITU Explainer: Cybersecurity.' https://www.gp-digital.org/wp-content/uploads/2018/08/ITU_Explainers_cybersecurity.pdf
3. Pollini et al. 2021. 'Leveraging human factors in cybersecurity: an integrated methodological approach.' Leveraging human factors in cybersecurity: an integrated methodological approach | SpringerLink
4. Global Cyber Security Capacity Centre. 'The CMM'. https://gcscc.ox.ac.uk/the-cmm
5. Hathaway and Spidalieri. 2021. Integrating Cyber Capacity into the Digital Development Agenda. GFCE. Integrating-Cybersecurity-into-Digital-Development_compressed.pdf (thegfce.org)
6. Schia and Willers. 2020. 'Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries'. https://doi.org/10.1007/978-3-319-71059-4_115-2
7. ITU. 2021. Digital technologies to achieve the UN SDGs. Digital technologies to achieve the UN SDGs (itu.int)
8. Higon, D., Gholami, R and Shirazi, F. 2017. 'ICT and environmental sustainability: A global perspective.' Telematics and Informatics, vol. 34(4). PP. 85-95. https://doi.org/10.1016/j.tele.2017.01.001
9. ITU. 2021. Digital Technologies to achieve the UN SDGs.
10. Hathaway and Spidalieri. 2021.
11. The United Nations. 2021. 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement
12. The United Nations. 2021.
13. Barry, J. 2019. 'Information Communication Technology and Poverty Alleviation'. https://www.routledge.com/Information-Communication-Technology-and-Poverty-Alleviation-Promoting/Barry/p/book/9780367665968
14. Dirk van der Linden; Ola Aleksandra Michalec; Anna Zamansky. 2020. Cybersecurity for Smart Farming: Socio-Cultural Context Matters. 10.1109/MTS.2020.3031844; Kam-Fung Cheung Michael G.H. Bell Jyotirmoyee Bhattacharjya. 2020. 'Cybersecurity in logistics and supply chain management: An overview and future research directions'. https://doi.org/10.1016/j.tre.2020.102217; Natalia Serbulova Sergey Kanurny Anastasia Gorodnyanskaya and Anna Persiyanova. 2019. 'Sustainable food systems and agriculture: the role of information and communication technologies'. https://iopscience.iop.org/article/10.1088/1755-1315/403/1/012127/pdf
15. Jessica L. Kamerer, EdD, MSN, RNC-NIC Donna McDermott, PhD, RN, CHSE. Cybersecurity: Nurses on the Front Line of Prevention and Education. https://doi.org/10.1016/S2155-8256(20)30014-4; Lynne Coventry, Dawn Branley. 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. https://doi.org/10.1016/j.maturitas.2018.04
16. Jeremy Wu. 2021. 'The Role of Information and Communication Technology in realising Sustainable Education by 2030'. https://gdc.unicef.org/resource/role-information-and-communication-technology-realizing-sustainable-education-2030
17. UN Women. 2017. 'Reshaping the future: Women, girls, ICTs and the SDGs'. Reshaping the future: Women, girls, ICTs and the SDGs | UN Women – Headquarters
18. Clark, M., Panguluri, S., Nelson, T., and Wyman, R. 2017. 'Protecting drinking water utilities from cyberthreats'. https://doi.org/10.5942/jawwa.2017.109.0021
19. Evgeni Sabev, Roumen Trifonov, Galya Pavlova & Kamelia Rainova. 2021. 'Cybersecurity Analysis of Wind Farm SCADA Systems'. Cybersecurity Analysis of Wind Farm SCADA Systems | IEEE Conference Publication | IEEE Xplore
20. Barry, J. 2019. 'Information Communication Technology and Poverty Alleviation'. https://www.routledge.com/Information-Communication-Technology-and-Poverty-Alleviation-Promoting/Barry/p/book/9780367665968; Oxford Economics. 2016. 'Cybersecurity as a growth advantage'. https://www.oxfordeconomics.com/resource/cybersecurity-as-a-growth-advantage/

21. Maglaras, L., Ferrag, M., Derhab, A., Mukherjee, M., Janicke, H. and Rallis S. 2019. 'Threats, Protection and Attribution of Cyber Attacks of Critical Infrastructures'. https://arxiv.org/abs/1901.03899; Clark, M and Hakim S. 2017. 'Cyber-Physical Security'. https://link.springer.com/book/10.1007/978-3-319-32824-9?noAccess=true
22. Huey, L and Ferguson, L. 2022. 'Another Digital Divide: Cybersecurity in Indigenous Communities'. https://www.crimrxiv.com/pub/jdn1dmbt/release/1
23. European Commission. 2011. 'Report of the Meeting of Advisory group ICT Infrastructure for energy-efficient buildings and neighbourhoods for carbon-neutral cities'. https://ec.europa.eu/information_society/activities/sustainable_growth/docs/smart-cities/smart-cities-adv-group_report.pdf
24. O'Donoghue, C. 2022. 'Cybersecurity 2.0: European Parliament adopts new draft directive'. Cybersecurity 2.0: European Parliament adopts new draft directive | Technology Law Dispatch
25. Sataloff, R.T., Johns, M.M., and Kost, K.M. (2019) "Industry 4.0 and cybersecurity Managing risk in an age of connected production. https://www2.deloitte.com/us/en/insights/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html
26. Popp, D. 2011. 'International Technology Transfer, Climate Change, and the Clean Development Mechanism.' https://www.journals.uchicago.edu/doi/epdf/10.1093/reep/req018; UNFCC. 2016. 'ICT Sector Helping To Tackle Climate Change.' https://unfccc.int/news/ict-sector-helping-to-tackle-climate-change#:~:text=According%20to%20the%20Global%20e,intelligently%20use%20and%20save%20energy
27. ITU. 'Goal 14. Oceans.' https://www.itu.int/en/sustainable-world/Pages/goal14.aspx
28. Norton, K. 2020. 'The 21st Century Threat to Wildlife is Cyberpoaching'. The 21st Century Threat to Wildlife is "Cyberpoaching" | NOVA | PBS; WWF. 'Wildlife Crime Technology Project'. Wildlife Crime Technology Project | Projects | WWF (worldwildlife.org); Peng-Yong Kong. 'A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles'. A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles | IEEE Journals & Magazine | IEEE Xplore
29. Asian Development Bank. 2016. 'Information and Communication Technology for Peace and Partnership'. https://www.adb.org/publications/ict-peace-and-partnership; Bertot, J., Jaeger, P. and Grimes, J. 2010. Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. GOVERNMENT INFORMATION QUARTERLY, [s. l.], v. 27, n. 3, p. 264–271. https://discovery.ebsco.com/linkprocessor/plink?id=d83589c2-6377-30f0-944c-80cf8ea7b9f2
30. Asian Development Bank. 2016.
31. The United Nations Trust Fund for Human Security. 2017. 'Human Security and Agenda 2030'. Human-Security-and-the-SDGs.pdf (un.org)
32. The United Nations Trust Fund for Human Security. 2017.
33. The United Nations Trust Fund for Human Security. 2017.
34. Wilson, T. 2020. 'Collaborative Jutsice and Harm Reduction in Cyberspace: Policing Indecent Child Images'. https://journals.sagepub.com/doi/full/10.1177/0022018320952560
35. UNDP Europe and Central Asia. 2021. 'Cyber Violence disempowers women and girls and threatens their fundamental rights'. https://www.eurasia.undp.org/content/rbec/en/home/blog/2021/Cyberviolence.html.
36. Council of Europe. 2022. 'Cyberviolence against women'. https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women
37. Maglaras, L., Ferrag, M., Derhab, A., Mukherjee, M., Janicke, H. and Rallis S. 2019. 'Threats, Protection and Attribution of Cyber Attacks of Critical Infrastructures'. https://arxiv.org/abs/1901.03899
38. Oxford Economics. 2016. 'Cybersecurity as a growth advantage'. https://www.oxfordeconomics.com/resource/cybersecurity-as-a-growth-advantage/.

39. Global Forum on Cyber Expertise. 2021. Integrating Cyber Capacity into the Digital Development Agenda. https://thegfce.org/wp-content/uploads/2021/11/Integrating-Cybersecurity-into-Digital-Development_compressed.pdf; Australian Bureau of Statistics. 2021. 'Digital activity in the Australian economy, 2019-2020'. https://www.abs.gov.au/articles/digital-activity-australian-economy-2019-20#:~:text=Digital%20activity%20value%20added%20increased,for%20the%20total%20Australian%20economy.
40. Oxford Economics. 2016.
41. Oxford Economics. 2016.
42. Smith, Z and Lostri, E. 2021. 'The Hidden Costs of Cybercrime'. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
43. Smith, Z and Lostri, E. 2021.
44. AustCyber. 2019. 'Sector Competitiveness Plan'. https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter3
45. Trucano, M. 2005. 'Knowledge Maps: ICT in Education'. https://www.infodev.org/articles/ict-education-gender-special-needs-and-disadvantaged-groups; Simuja, C., Krauss, K and Conger, Su. 2016. 'Achieving inclusive and transformative ICT education practices in rural schools in marginalised communities.' https://aisel.aisnet.org/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1008&context=confirm2016
46. Simuja, C., Krauss, K and Conger, Su. 2016. 'Achieving inclusive and transformative ICT education practices in rural schools in marginalised communities.'
47. House of Commons Library. 2020. 'Climate Change solutions; The role of technology'. https://commonslibrary.parliament.uk/climate-change-solutions-the-role-of-technology/
48. Cybersecurity Guide. 2021. 'Cybersecurity in the environmental protection field'. https://cybersecurityguide.org/industries/environmental-protection/
49. Cybersecurity Guide. 2021.