CYBERSECURITY CAPACITY REVIEW

Mongolia

February 2025

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

TABLE OF CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers:	Louise Axon and Joe Fulwood
Reviewed by:	Professor William Dutton, Professor Michael Goldsmith, Dr Jamie Saunders, Professor David Wall, Professor Basie Von Solms
Approved by:	Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*08/12/2024*	*First draft by lead researchers submitted to the GCSCC Technical Board*
2	*20/12/2024*	*Second draft submitted to hosts*
3	*20/01/2025*	*Feedback received from hosts*
4	*26/01/2025*	*Third draft submitted to hosts*
5	*04/02/2025*	*Final feedback received from hosts*
6	*05/02/2025*	*Final report submitted to hosts*

LIST OF ABBREVIATIONS

APT	Advanced Persistent Threat
CA	Certification Authority
CII	Critical Information Infrastructure
CSIRT	Computer Security Incident Response Team
CTI	Cyber-threat intelligence
EU	European Union
FIRST	Forum of Incident Response and Security Teams
GCI	Global Cybersecurity Index
GDPR	General Data Protection Regulation
GIA	General Intelligence Agency
ISAC	Information Sharing and Analysis Centre
ISO	International Organization for Standardization
KPI	Key Performance Indicator
ISMS	Information Security Management System
ISP	Internet Service Provider
IXP	Internet Exchange Point
ITU	International Telecommunication Union
JICA	Japan International Cooperation Agency
KPI	Key Performance Indicator
MDDIC	Ministry of Digital Development, Innovation and Communications
MNCERT/CC	Mongolian Cyber Emergency Response Team Coordination Centre
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NCS	National Cybersecurity Strategy
NDCI	National Data Centre
NGO	Non-Governmental Organisation
NIDS	Network Intrusion-Detection System
NRI	Network Readiness Index
OSCE	Organization for Security and Co-operation in Europe
PCI DSS	Payment Card Industry Data Security Standard
PKI	Public-Key Infrastructure
TLS	Transport Layer Security
UN	United Nations
UNDP	United Nations Development Programme

EXECUTIVE SUMMARY

In collaboration with the Japan International Cooperation Agency (JICA), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a review of the maturity of cybersecurity capacity in Mongolia at the invitation of the Ministry of Digital Development, Innovation and Communications (MDDIC). The objective of this review was to enable Mongolia to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities.

Over the period spanning 2nd-7th October 2024, the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, information technology officers from the government and the private sector (including financial institutions), telecommunications companies, and the banking sector as well as international partners.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five *dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cybersecurity Culture and Society*
- *Building Cybersecurity Knowledge and Capabilities*
- *Legal and Regulatory Frameworks*
- *Standards and Technologies*

Each dimension contains a number of *factors* which describe what it means to possess cybersecurity capacity. Each factor presents a number of *aspects* grouping together related *indicators*, which describe steps and actions that, once observed, define the stage of maturity of that aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[1]

Figure 1 below provides an overall representation of the cybersecurity capacity in Mongolia and illustrates the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' is placed at the perimeter.

[1] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition," February 2017, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

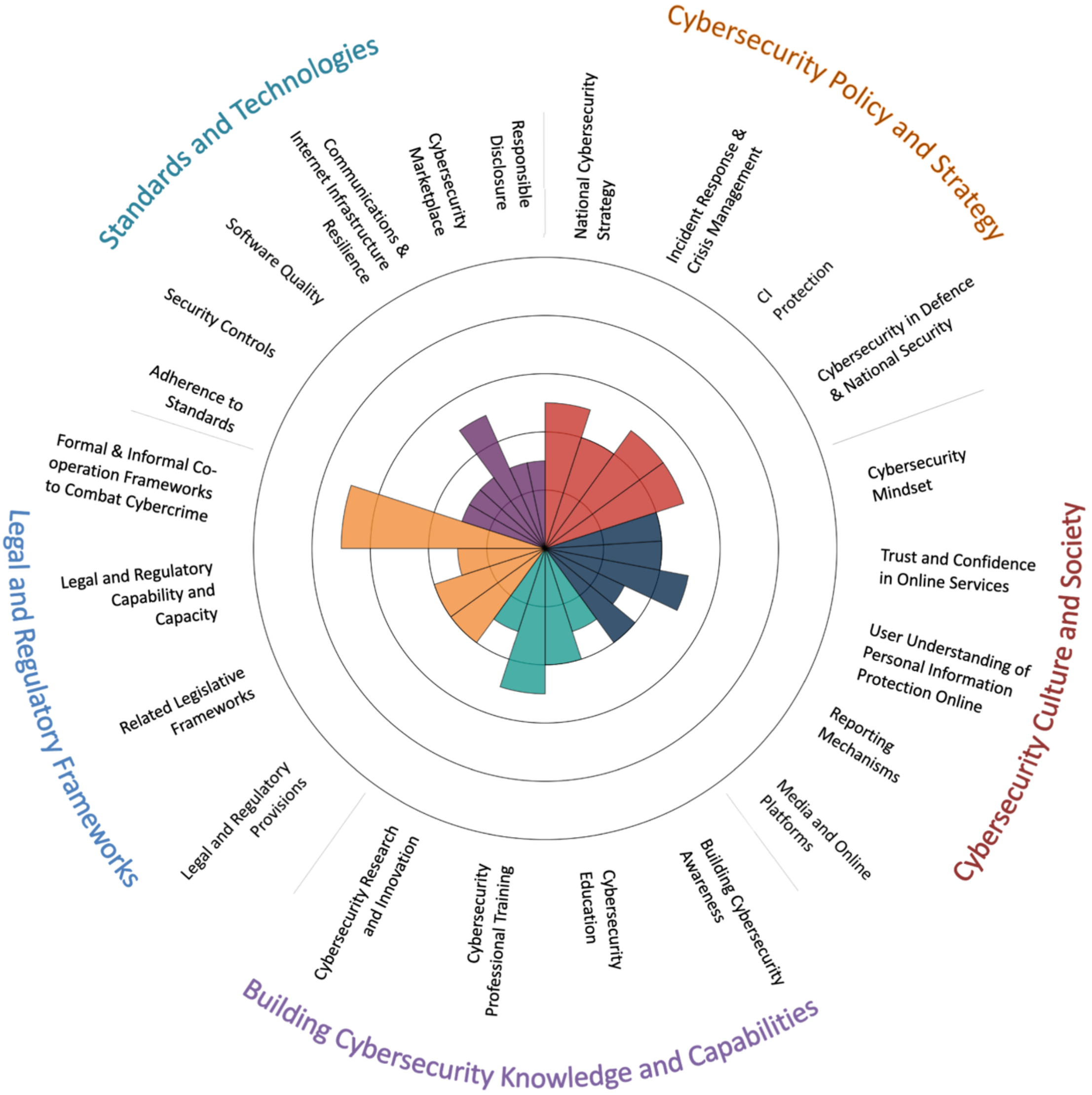
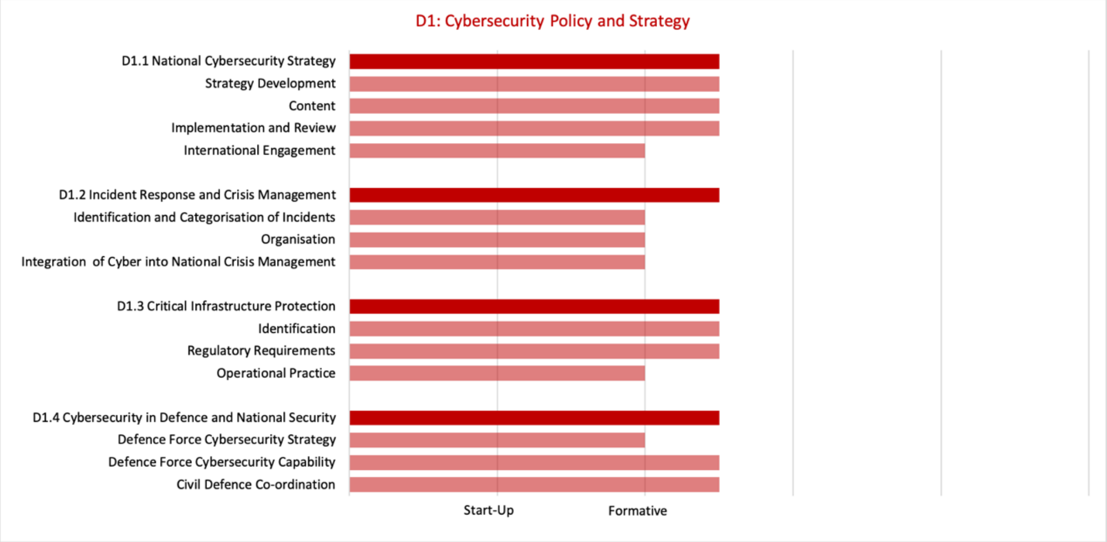


Figure 1: Overall representation of the cybersecurity capacity in Mongolia

Cybersecurity Policy and Strategy



The first national cybersecurity strategy (NCS) was approved on 28th December 2022 by Decision no. 493 of the Government of Mongolia. Research studies were conducted by MDDIC and GIA to support the NCS development, which created some understanding of the cybersecurity risks faced by the nation. It would be beneficial to identify what is additionally needed to obtain a full picture of the national cybersecurity risk, and how this and other pre-existing research can contribute to this. The NCS contains detailed actions including the establishment of the National Cyber Security Council; the establishment of national Cyber Security Incident Response Teams (CSIRTs) and other actions to protect the CII organisations; actions to mitigate cybercrime; and actions to raise public awareness of cybersecurity.

The NCS was designed to be implemented in two phases, with Phase I spanning 2022-2025, and Phase II 2026-2027. Its defined outcomes are specific and measurable against Key Performance Indicators (KPIs). Alongside the NCS, an Action Plan has been developed, assigning the primary responsible parties for each action and noting any necessary collaborators. According to the NCS, coordination of the programme to implement the NCS is the responsibility of the government and the National Cyber Security Council. The NCS implementation progress has not yet been subject to evaluation; the first evaluation is planned for the end of implementation Phase I (2025) against the metrics and targets defined in the NCS. It will be important to continuously assess the effectiveness of the Council in its current form in coordinating and monitoring the NCS progress, and to ensure that any shortfalls in the budget required implement the actions of the NCS can be identified and escalated. It may also be beneficial to consider a mechanism to engage other stakeholders, such as the private sector and civil society, in the ongoing NCS governance and progress monitoring.

There are four national-level CSIRTs in Mongolia. The Cyber Security Law in 2021 made provisions for the establishment of the National CSIRT, Public CSIRT/CC, and Armed Forces CSIRT.[2] Under the Law, incident response in for critical infrastructure organisations in Mongolia is divided between the National CSIRT, established in 2023 under the General

[2] https://legalinfo.mn/en/edtl/16531350476261

Intelligence Agency (GIA), and the Public CSIRT/CC, established in 2023 under MDDIC. MNCERT/CC, an NGO CSIRT operating since 2014 among private member organisations including banks, mobile operators, and major Internet Service Providers (ISPs), also plays a significant role in supporting the cybersecurity of Mongolian organisations. The National Data Centre (NDC) also plays a role in responding to incidents. Since it hosts the systems of many government agencies, it has previously supported incident detection and response (prior to the Cybersecurity Law) and has continued to do so since the Law.

According to the Cybersecurity Law, it is the responsibility of the National CSIRT to maintain a database of cybersecurity incidents nationwide within a Cybersecurity Incident Database. In practice, both the National CSIRT and Public CSIRT/CC are relatively new establishments, and it was reported that their databases are not yet fully functional. The Database has to-date only registered incidents within the scope of the National CSIRT, and, the effectiveness of the exchange of information from the Public CSIRT/CC to the National CSIRT has not yet been fully tested. This will be critical to ensuring that the information registered in the Cybersecurity Incident Database provides a comprehensive picture of the incidents nationwide, especially given that the responsibility for public and private CII is divided between these two CSIRTs. Obtaining this comprehensive picture will support identification and prioritisation of incidents that risk causing national-level impacts. It will also support a more comprehensive understanding of the threat that the country is facing, and full assessment of the national cybersecurity risk.

The capabilities of the National CSIRT and Public CSIRT/CC have not yet been fully tested, since they are relatively new. It remains to be assessed whether the current structures have the necessary resources, skills and processes required to address the range of cyber-incident scenarios that the country is likely to face. There were some concerns cited that may be resource and skills constraints for the national and public CSIRTs to meet the needs of the full range of constituents assigned to them. It is important to identify how CSIRTs can collaborate more effectively using their joint resources, and how to leverage other elements of the ecosystem, including potentially MNCERT/CC, the NDC, and elements of the private sector. It is also important that governance mechanisms for the ongoing NCS programme are sufficiently well connected, by gathering input from a range of stakeholders, to ensure that the establishments such as the CSIRTs are functioning effectively and identify any gaps.

A national cyber crisis response plan was approved in September 2024. While there have been drills already conducted with various groups, it will be important that exercises are conducted against the newly finalised national crisis-management plan, involving all relevant stakeholders. This will help ensure that the necessary processes and relationships are in place to deal with the range of crisis scenarios that the nation may face, and that the capabilities of the responsible organisations are sufficient.

The list of CII sectors is defined in the Cyber Security Law 2021. Within these sectors, the specific CI organisations have been identified, and the list of operators was published in 2022. CII operators are mandated to meet certain cybersecurity obligations, which include adopting internal procedures for cybersecurity; an action plan for cyber-attacks; having an officer charged with ensuring cybersecurity; having cybersecurity risk assessments conducted every year and information-security audits every two years, and breach reporting.

Formal processes have been defined to evaluate CII operator compliance with the requirements of the Cybersecurity Law. It was reported that enforcement of compliance will begin in 2025. The implementation of good cybersecurity practices is therefore not yet consistent across the CII organisations. In some more mature sectors, there is already compliance with cybersecurity standards, and sharing of threat and vulnerability information and best practices between operators.

It is intended that the provisions of the Cybersecurity Law will raise the level of cybersecurity across CII organisations. It is important to note, however, several potential challenges raised that may need to be managed to ensure effective implementation of the Law. The first area of challenge is the capacity of the identified CII organisations to implement the requirements of the Law. Some organisations consulted expressed concerns about their capacity to meet these requirements. The second area of challenge relates to relevant stakeholders' understanding of the Law, with some confusion reported and disagreement over the required level of detail. The third area of challenge is the capabilities of the relevant stakeholders to enforce compliance with the Law. For the smooth implementation of the Law, it will be critical to identify how to upskill the relevant stakeholders and build trust where necessary.

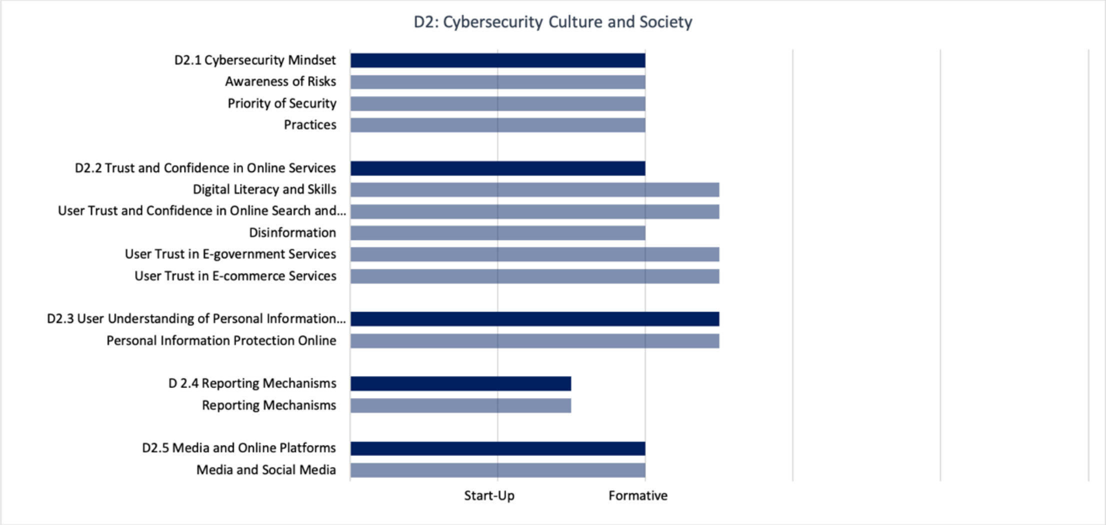
In summary, the Cybersecurity Law and its accompanying procedures create strong progress towards the protection of the CII. It will be critical to ensure continue to monitor CII organisations' capabilities to interpret and implement the requirements of the Law, to ensure that any shortfalls can be addressed, and support is provided where needed. The NCS itself includes metrics for measuring the progress of CII cybersecurity practice, including the "growth rate of CII organisations that have adopted specialised cybersecurity risk-based practices", and the "growth rate of organisations that have established a recovery and continuity management system", which should help with monitoring progress. It will also be important, as compliance with the Law becomes enforced, to test the effectiveness of the planned regulatory approach.

A defence force cybersecurity strategy has not yet been published, and participants did not report any such strategy being under development. Article 14 of the Cyber Security Law places several requirements on the organisation responsible for the cybersecurity of the armed forces. This might be considered as providing the strategic objectives at a high level. It is unclear whether the potential impact of cybersecurity on national security and defence has been assessed. Making this assessment is important to supporting the development of a strategy for cybersecurity in Defence, and related operational doctrine and rules of engagement.

An Armed Forces Cybersecurity Command has been established. Within this structure, the Armed Forces Centre for Combating Cyber Attacks and Violations was inaugurated in 2021, with support from the North Atlantic Treaty Organization (NATO). There is ongoing training of the cybersecurity command and staff of the Centre through the Mongolian National Defence University and partnerships with other countries. It was reported that there remains a shortage of trained specialists, and no evidence was provided that the sufficiency of the current capabilities has been tested.

The Cybersecurity Law also assigns the responsibility of the armed forces to "*where necessary provide support in the activities of ensuring cybersecurity of the nation*". Collaboration on cybersecurity between civil and defence entities in the event of a national crisis has been formalised through the national cyber crisis response plan, approved in 2024. The plan is new and has not yet been tested, but the intention is to conduct regular exercises against it. As such, there is not yet clear evidence of the effectiveness of collaboration between civil and defence entities. No evidence was provided that the dependencies of the military on civil and CII infrastructures have been assessed. It will be important to establish mechanisms to assess these dependencies, and to assure the ability of civil and CII infrastructure operators to provide these services.

Cybersecurity Culture and Society



Mongolia has an evolving understanding of the risks associated with digital transformation and cybersecurity. Levels and of awareness and prioritisation have increased substantially since 2021 and the introduction of the new national cybersecurity legislative framework. The National Cybersecurity Strategy 2022 and its implementation plan provide further evidence of the government’s awareness and prioritisation of cybersecurity. However, despite a recognised degree of awareness amongst these stakeholders, widespread awareness of cybersecurity risks has not been achieved within the broader government, civil society, or the general public. The improvements to cybersecurity awareness and prioritisation instigated by the introduction of the new laws have not been felt universally, with some key stakeholders still knowing little about the laws. Poor awareness levels amongst senior management and politicians were raised as an ongoing challenge undermining the security of both the public and private sector. This is particularly impactful at a budgetary level. Beyond a leading group of stakeholders, focus groups revealed that most users are not following safe cybersecurity practices. Poor password management, the use of private emails and messaging software for official information sharing at work and not using two factor authentication were commonly discussed poor cybersecurity practices.

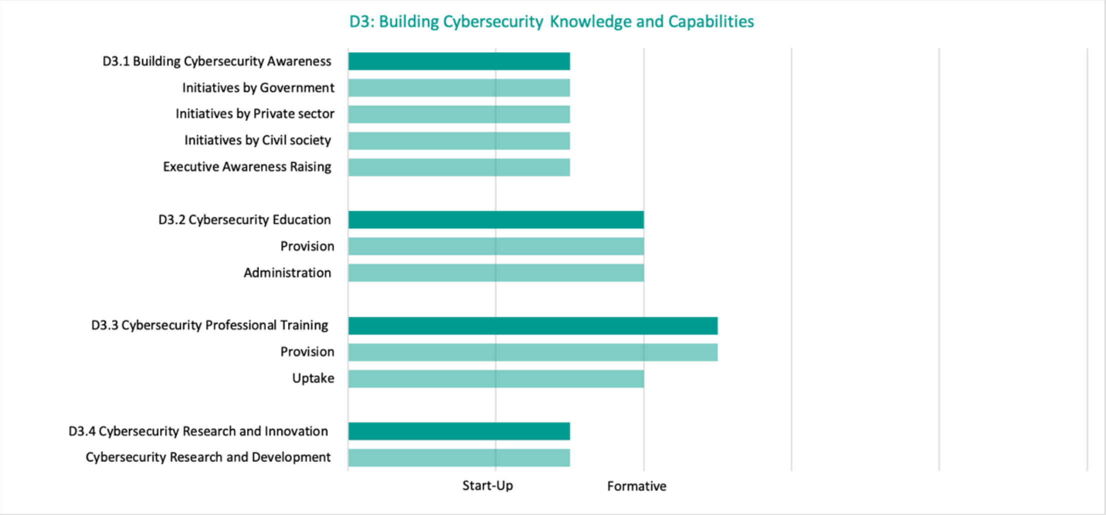
Mongolia has a growing rate of digitally literate internet users who regularly use online social media platforms and e-services as part of their daily routines. This activity is enabled by a robust network of ICT-infrastructure that facilitates user connectivity. Leading stakeholders from the private and public sectors managing key digital services recognize the need to protect them with strong security measures, and in the case of CII, are required to do so under law. Despite this, it was acknowledged that the security of each system is depended on the management of those systems and some organizations have implemented higher security controls than others. At a user level, high rates of digital literacy and uptake of digital services in Mongolia are not accompanied by the routine use of safe cybersecurity practices, or widespread awareness of how to stay safe online. Most Mongolian internet users are reportedly unable to identify legitimate and illegitimate websites and digital services from each other and were described as "gullible" and even "digitally silly" by some focus group participants.

Privacy is a fundamental human right of the Mongolia people under the Constitution of Mongolia. Mongolia has a robust data privacy framework that was established through the *Law on Personal Data Protection 2021.* It includes provisions for the collecting, processing, using and security of personal data that all 'Data Controllers' must follow. Through its security and oversight provisions, the law has established clear measures to try and balance privacy and security needs. At a user level, people do not know what measures they can or should take to protect their personal information online. Culturally, it was suggested that the Mongolian population is not generally aware of how their digital data is used online, and most of the ordinary people in Mongolia are not well aware of the data privacy rights.

Reporting mechanisms for cybersecurity incidents, cybercrimes and other cyber harms are established in Mongolia and operating with some degree of coordination. The National Police Authority, National CSIRT and Public CSIRT/CC are all provided with a mandate under the *Law on Cybersecurity 2021* to receive information pertaining to cybercrimes, cyber-attacks and other violations from their various constituents. Focus group discussions with various stakeholders confirmed that while there is a desire for these established reporting mechanisms to work closely together, they currently do not operate in a coordinated manner. Instead, for the most part, the different reporting mechanisms are siloed from each other.

Traditional and digital media outlets publish coverage of cybersecurity matters sporadically. This includes coverage of international cybersecurity awareness month, cybersecurity events, cybersecurity policy developments, cybercrime cases and more. In some instances, media coverage has incorporated information on how readers and viewers can implement proactive and actionable cybersecurity measures to protect themselves online.

Building Cybersecurity Knowledge and Capabilities



A lack of cybersecurity human resources within the Mongolian labour market is a cross-cutting issues that is having severely detrimental effects on the nation’s ability to improve its cybersecurity capability and maturity. There was unilateral agreement amongst every stakeholder who participating in the CMM focus groups that hiring and retaining skilled cybersecurity professionals was a major challenge to doing anything from implementing the *Cybersecurity Law 2021* through to developing a cybersecurity training course for children. Without substantial consideration and investment this has the potentially to completely undermine Mongolia’s efforts to improve its national cybersecurity resilience.

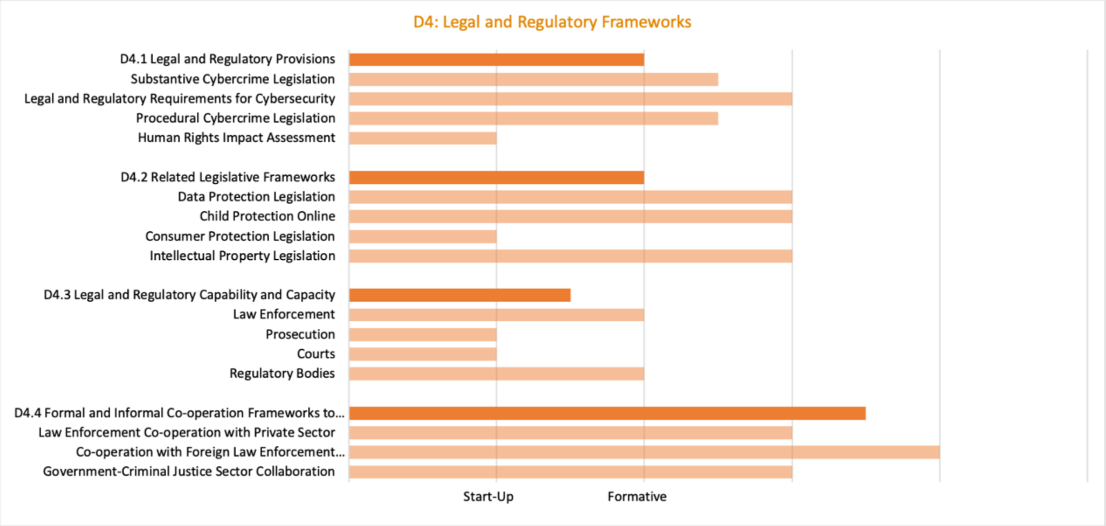
Mongolia has a patchwork of different cybersecurity awareness programs and activities that are being administers by a range of different entities in an un-coordinated manner. At a strategic level, improving public cybersecurity awareness and organizing campaigns, trainings and seminars to provide knowledge and understanding on cybersecurity is one of the major goals of the 2022 National Cybersecurity Strategy. There was consensus that more consistency and strategy was needed to effectively increase public awareness of cybersecurity, and more work is needed in this area to improve perversely low awareness levels. Comprehensive cybersecurity awareness training programs for executive level leaders in the private or public sectors were not identified by focus group discussions or desktop research. Many people expressed a strong desire to see tailored awareness raising programs for executive level decision makers to help overcome this entrenched opposition to cybersecurity spend and prioritisation.

Qualifications for tertiary degrees related to cybersecurity are available from several of Mongolia’s leading universities. Despite the recognised demand for skilled cyber professionals, the availability of formal education courses and demonstrated interest from students, it is difficult for Mongolia’s higher education institutions to provide the equipment and staff necessary to deliver graduate outputs that meet industry expectations. Universities have reported difficulties in hiring and retaining their own education staff due to high demand and salaries for their skillsets in the private sector and abroad, and challenging workloads that make the positions unattractive. A limited supply of physical teaching environments that facilitate attack and defence simulations, digital forensics training and other more technical trainings have further restricted educational outputs.

Outside of the higher education sector, multiple structured and ad-hoc cybersecurity training programs are available in Mongolia. The programs are implemented by a wide variety of education providers, including vocational centres, private cybersecurity training centres, and international capacity building partners. Training for law enforcement personnel in particularly occurs frequently, especially with support from international partners. Focus group discussions indicated that government and private sector enterprises routinely engage with these trainings opportunities, when they can afford it, and that there is a high appetite for cybersecurity professional training overall within Mongolian organisations. Nevertheless, difficulties training and retaining cybersecurity staff are particularly prevalent in the public sector, which is constrained by inflexible salary bands, ministerial silos, and a lack of competitive advantages compared to the private sector. The Mongolian government is undertaking some efforts to prevent the ongoing drain of human resources and improve recruitment within the public sector, but more needs to be done to overcome this challenge. Outside of government, private sector employers also face challenges finding a sufficient supply of skilled cybersecurity professionals to meet their needs, despite their advanced maturity levels. Many have reported struggling to find and retain resources due to fierce competition between domestic and international employers.

Mongolia's NCS includes a goal of empowering security qualified human resources. Under this goal, 'implementing a program to support the training, research and academic work of cybersecurity researchers' is a core activity. Furthermore, under the *Law on Cybersecurity 2021*, the 'state central administrative agency in charge of digital development and communications' is mandated to 'conduct new technical, technological, innovation, research and development activities in areas of cybersecurity.' In practice, no substantive actions have been taken to facilitate localised research and development activity in Mongolia.

Legal and Regulatory Frameworks



The *Criminal Code 2015* legislates substantive cybercrime provisions related to the confidentiality, integrity and availability of computer data and systems. It also included offences against children and includes provisions that apply such protections to the online environment. Mongolia's has comprehensive cybercrime criminal procedure law provided under the *Law on Criminal Procedure 2017.* Each cybercrime offence established under Mongolian law includes the necessary measures to ensure that these offences are punishable by effective, proportionate and dissuasive sanctions. Despite the law permitting a variety of punishments, it was noted in focus group discussions that when cases go to court and are successfully prosecuted, they sometimes only result in a small fine for the criminal.

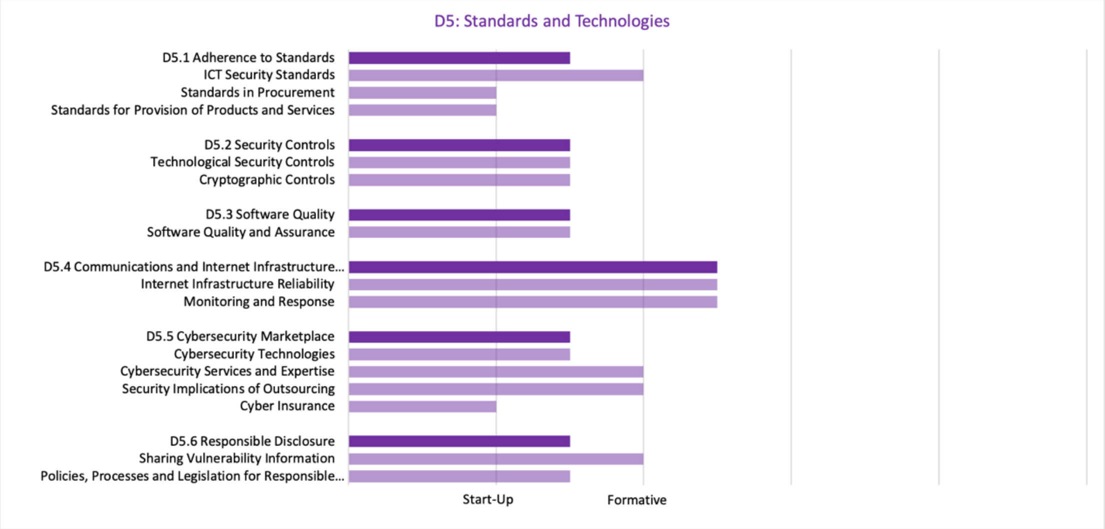
The *Law on Cyber Security 2021* has established comprehensive cybersecurity requirements for critical infrastructure operators and other specified stakeholders. Additional obligations for all legal persons defined in the *Law on Cybersecurity 2021*, including CII, are specified in the *General Procedure on Cyber Security*. Whereas the law and accompanying general procedure have undoubtedly facilitated several advancements in Mongolia's legislative and governance environments, there are ongoing challenges in in the implementation and adoption of the updated legislative and regulatory framework that are undermining further national progress.

The *Law on Personal Data Protection 2021* regulates the collection, processing, use and security of personal data. The National Human Rights Commission is granted the powers and responsibility to oversee compliance with the law. Overall, the law centralizes maintaining and protecting the human rights and freedoms of Mongolian citizens within the broader data management framework. The *Civil Code 2002* outlines the general conditions of sales within consumer contracts; however, it does not include specific provisions indicating that it is applicable to the online environment. The *Law on Copyright 2021* established Mongolia's intellectual property legislative framework. The application of the legislative framework to the digital environment is well established.

Mongolia's law enforcement, prosecution and courts have some limited foundational capacity to investigate cybercrime cases; however, gaps in technical, human and financial resources are preventing broader institutional capacities from developing. Crime data from the 'Mongolia Statistics Yearbook 2023' indicates that there is at least limited capacity within Mongolian legal institutions to take cybercrime cases through to completion. These statistics demonstrate that the capacity to process cybercrime cases is growing year-on-year, but does not yet appear to be at a level sufficient to match the growing number of register cybercrimes. This is consistent with the data collected in focus groups discussions, which indicated that the prosecution and judiciary lacked institutional capacity to manage cybercrime cases efficiently and effectively. Within law enforcement, despite their efforts to provide training opportunities and fill their cyber-skills gap, a high rotation of staff has undermined their ability to build human capacity. Fierce competition with other sectors for skilled cybersecurity professionals has undercut the retention rate of trained professionals who are easily attracted to better paying roles elsewhere in the labour market.

The Mongolia government works closely with the criminal justice sector to develop cybercrime laws and strategies, conduct training exercises and exchange information on cybercrimes. The Public CSIRT/CC, which sits beneath MDDIC, and the National CSIRT, which sits beneath GIA, both provide formal mechanisms for collaboration and information exchange between the Mongolian government and the law enforcement on cybercrime. At an international level, Mongolia has the legislative framework to support Mutual Legal Assistance Treaties (MLATs). The National Police Agency reported a significant improvement in recent years in their ability to collaborate with international partners. Mechanisms such as the G7 24/7 network and their relationship with INTERPOL were cited as helping in this regard. Successful cross border investigations with international counterparts and local law enforcement authorities have recently been reported in the media.

Standards and Technologies



There has been identification of international cybersecurity standards and localisation of these standards to the Mongolian environment, for Mongolian organisations to use. Some participants expressed the view that these localised standards need to be updated, as international standards have been since. This aligns with the NCS, which contains an Action to "localise international standards for ensuring cyber security, approve and implement rules and regulations in accordance with them".

The extent to which these standards are followed varies. There is some evidence of growing implementation of the use of international standards and good practices within some sectors, but a lack of detailed data makes it challenging to assess the extent of adherence to standards across sectors. Under the Cybersecurity Law, CII organisations will be obliged to adopt cybersecurity standards; however, adoption is still in progress as the first audit deadlines have not yet passed. The Finance sector is the only sector in which organisations were mandated by the regulator to adopt cybersecurity standards prior to the Cybersecurity Law. In other sectors, there is some adherence to standards. This varies dependent on the maturity of the organisations, and also driven by their requirements to operate internationally.

There is no evidence of measurement of the use of cybersecurity standards by organisations outside of the CII and government. However, it would be beneficial to consider how to promote the use of cybersecurity standards and the General Procedures to other private organisations, and implement schemes to measure uptake.

Security controls are being deployed by some public and private organisations in Mongolia, but this is not consistent across sectors. The existing regulation of the adoption of cybersecurity standards for organisations in the Finance sector also means that these organisations are implementing technological and cryptographic security controls accordingly. Currently, the deployment of technological and cryptographic security controls varies across organisations in Mongolia dependent on their resources and cybersecurity awareness, and their adherence to cybersecurity standards. It was reported that research by academic institutions and private cybersecurity companies has found that the application of security controls in certain sectors in lacking. The healthcare sector was cited as a particular example.

Representatives from government cited concerns about the prevalence of successful attacks, for example, including APT attacks, against government organisations. For government organisations, issues with budget were reported to be creating challenges for the implementation of cybersecurity controls. There is a need to explore how to ensure that government organisations are allocated sufficient budget to implement controls by the Ministry of Finance. Some organisations outside of government also reported concerns about their ability to obtain budget to implement controls. The view was expressed that the leadership of organisations are not consistently prioritising cybersecurity in their allocation of resources. It may be beneficial to explore running initiatives to raise the cybersecurity awareness of organisational leadership.

Software quality requirements are recognised by some organisations. Some participants from private CII organisations described the security reviews and testing processes conducted for software procured, and having mature processes in place for software updates and maintenance. This level of maturity in ensuring the use of high-quality and secure software is not consistent across organisations. Concerns were that some organisations lack the resources or awareness to purchase licenses for software and cybersecurity technologies, leading to the use of unlicensed software.

The view was expressed that software purchased from abroad tends to be better standardised and more reliable. Participants from private organisations noted that in using domestic software, there is a greater need to conduct their own security reviews and testing to rely on it, since it is usually not standardised, and its security depends on the quality of the company developing it. No catalogue for assured software platforms exists to guide organisations in their procurement.

Reliable Internet services were reported to be widely available and used in Mongolia. The Internet infrastructure is formally managed by the Communications Regulatory Commission, which issues licenses to Internet Service Providers (ISPs) and regulates ISPs, for example requiring a specified minimum percentage of ISPs' traffic to be routed through alternative paths to improve redundancy. There is also a requirement for ISPs to provide DDoS protection to clients; however, it was noted that not all ISPs have the resources to comply with this requirement. In relation to redundancy, there is also a Mongolian Internet Exchange Point (IXP) hosted by the NDC, which facilitates traffic exchange amongst ISPs, and which participants stated provides good redundancy in the case of failure of an ISP. It was also reported that discussions are ongoing between ISPs and the Communications Regulatory Commission to create further IXPs.

Large telecommunications organisations have been identified as CII according to the Cybersecurity Law. This creates several requirements, soon to come into force, including the obligation to conduct risk assessments and audits, implement internal cybersecurity procedures and standards, and develop incident-response plans. Currently, the sector is unregulated regarding the implementation of mechanisms for protecting against, detecting and responding to cybersecurity incidents. Their implementation therefore varies across telecommunications organisations.

Participants reported that there are no cybersecurity products produced by Mongolian companies. Cybersecurity products used in Mongolia are supplied by foreign vendors, with some resellers operating in Mongolia. There is an intention to increase the production of local products, noting the potential implications of reliance on foreign technologies, which is reflected in the NCS.

Participants stated that the Mongolian cybersecurity services industry has expanded rapidly in the past three years. Companies are offering services including cybersecurity standards-compliance audits, penetration testing, implementation of Information Security Management Systems (ISMS). Some organisations from the CII reported experience in using local cybersecurity consultancy services. Some participants from government expressed the view that, while it is growing, the supply of cybersecurity-service providers is still not sufficient to meet demand, particularly to fulfil requirements of the Cybersecurity Law. The accompanying procedures to the Cybersecurity Law state that service providers auditing the CII must have a full-time employee certified by a professional association or standards organisation. According to MDDIC, who conducted an evaluation of the eligible service providers, only a small number currently meet this requirement.

Some organisations are outsourcing their IT. For some government organisations, it is mandated that their systems are hosted in the government cloud or directly by the National Data Centre. Other organisations, including some government agencies, may choose to host at the NDC, and some choose to outsource to other third-party cloud services, including international services. The capability of organisations to conduct risk assessments to determine how to mitigate the risks of outsourcing varies according to their maturity. There is some legislation aimed at addressing the risks: a requirement in the Data Protection Law that personally identifiable information of Mongolian citizens must be physically hosted within the nation’s borders. The NDC reported a further plan to develop a policy jointly with MDDIC to clearly outline the different information-classification levels and where they can be hosted.

Cyber-insurance offerings are emerging in Mongolia. The National CSIRT website contains an introduction to cyber insurance, and guidance on choosing the right cyber-insurance product. Participants were not aware of any local companies offering cyber-insurance product, but stated that such products are made available to Mongolian companies by some international providers. Uptake of cyber-insurance products is in the early stages, and the participants consulted during the CMM did not have any experience in using cyber-insurance products.

Within some sectors, mechanisms exist for operators to share threat and vulnerability information with each other. It was reported that there is a banking Information Sharing and Analysis Centre (ISAC), through which financial institutions share threat and vulnerability information. Some organisations in the financial sector also reported subscribing to international cyber-threat intelligence (CTI) feeds. Members of MNCERT/CC, primarily composed of large private-sector organisations, also share information between themselves. The view was expressed that it would be beneficial to have information-sharing mechanisms that can be used by a wider range of organisations in Mongolia, to facilitate the exchange of threat and vulnerability information.

There is some culture of ethical hacking and vulnerability disclosure in Mongolia. Events run on how to conduct bug-bounty programmes have reportedly led to instances of companies openly inviting researchers to search for vulnerabilities in their systems. Some organisations have a responsible-disclosure policy in place, detailing the processes to be followed in the case that a vulnerability in their software or website is disclosed. It was noted that this is dependent on the culture and maturity of the organisation, however, and is primarily seen in private financial institutions. The current lack of consistently implemented responsible-disclosure mechanisms may hinder the effective reporting and remediation of security vulnerabilities by organisations, including government institutions.

There is no legislation in place to protect researchers disclosing vulnerabilities responsibly. Some participants who participate in ethical hacking communities in Mongolia reported a reluctance to approach companies due to fear of repercussions. The view was expressed that it would be beneficial to develop the mechanisms to protect researchers, noting that these mechanisms need to be suited to the Mongolian context.

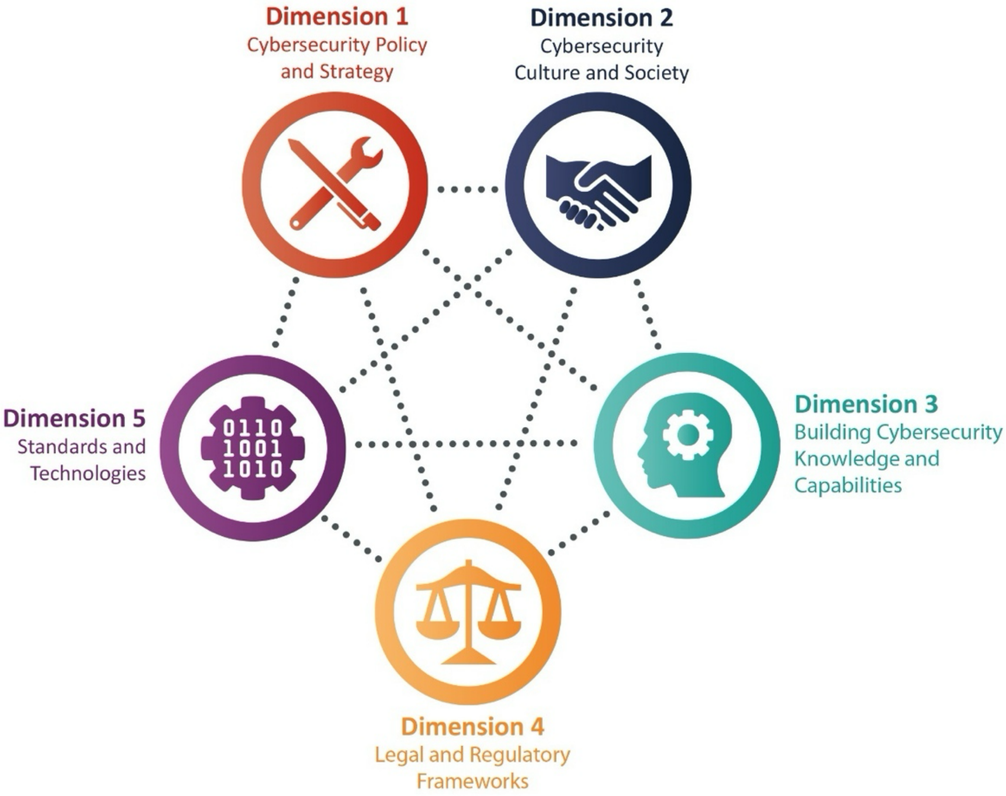
INTRODUCTION

At the invitation of the Ministry of Digital Development, Innovation and Communications (MDDIC) and in collaboration with the Japan International Cooperation Agency (JICA), the Global Cyber Security Capacity Centre (GCSCC) has conducted a review of cybersecurity capacity of Mongolia. The objective of this review was to enable Mongolia to determine areas of capacity in which the government might strategically invest in, in order to improve their national cybersecurity posture.

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were based around the GCSCC Cybersecurity Capacity Maturity Model (CMM)[3] which is composed of five distinct *dimensions* of cybersecurity capacity.

Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five dimensions together with the factors which each presents:


Dimension 1
Cybersecurity Policy and Strategy
Dimension 2
Cybersecurity Culture and Society
Dimension 5
Standards and Technologies
0110
1001
1010
Dimension 3
Building Cybersecurity Knowledge and Capabilities
Dimension 4
Legal and Regulatory Frameworks

[3] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), 2021 Edition," March 2021, https://gcscc.ox.ac.uk/the-cmm#/.

DIMENSIONS	FACTORS
Dimension 1 **Cybersecurity Policy and Strategy**	D1.1 Strategy Development D1.2 Incident Response and Crisis Management D1.3 Critical Infrastructure (CI) Protection D1.4 Cybersecurity in Defence and National Security
Dimension 2 **Cybersecurity Culture and Society**	D2.1 Cybersecurity Mindset D2.2 Trust and Confidence in Online Services D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Online Platforms
Dimension 3 **Building Cybersecurity Knowledge and Capabilities**	D3.1 Building Cybersecurity Awareness D3.2 Cybersecurity Education D3.3 Cybersecurity Professional Training D3.4 Cybersecurity Research and Innovation
Dimension 4 **Legal and Regulatory Frameworks**	D4.1 Legal and Regulatory Provisions D4.2 Related Legislative Frameworks D4.3 Legal and Regulatory Capability and Capacity D4.4. Formal and Informal Co-operation Frameworks to Combat Cybercrime
Dimension 5 **Standards and Technologies**	D5.1 Adherence to Standards D5.2 Security Controls D5.3 Software Quality D5.4 Communications and Internet Infrastructure Resilience D5.5 Cybersecurity Marketplace D5.6 Responsible Disclosure

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each dimension contains a number of *factors* which describe what it means to possess cybersecurity capacity. Each factor presents a number of *aspects* grouping together related *indicators*, which describe steps and actions that, once observed, define the stage of maturity of that aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five stages are defined as follows:

- **start-up:** at this Stage, either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There may be an absence of observable evidence at this Stage;

- **formative:** some features of the Aspect have begun to grow and be formulated, but may be ad hoc, disorganised, poorly defined or simply new. However, evidence of this activity can be clearly demonstrated;

- **established:** the Indicators of the Aspect are in place, and evidence shows that they are working. There is not, however, well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in the various elements of the Aspect. But the Aspect is functional and defined;

- **strategic:** choices have been made about which parts of the Aspect are important, and which are less important for the particular organisation or nation. The strategic Stage reflects the fact that these choices have been made, conditional upon the nation or organisation's particular circumstances; and

- **dynamic:** at this Stage, there are clear mechanisms in place to alter national strategy depending on the prevailing circumstances, such as the technology of the threat environment, global conflict, or a significant change in one area of concern (e.g. cybercrime or privacy). There is also evidence of global leadership on cybersecurity issues. Key sectors, at least, have devised methods for changing strategies at any stage during their development. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this Stage.

The assignment of maturity stages is based upon the evidence collected, including the general or consensus view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Mongolia and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

CYBERSECURITY CONTEXT IN MONGOLIA

Mongolia is a large country situated in East Asia covering approximately 1.5 million square kilometres.[4] It is landlocked between Russian to the North and China to the South. It is home to a population of approximately 3.5 million people: a sparse population compared to its total land mass (approximately 2.2 people per square kilometre). Approximately 2.5 million people live in urban areas. Ulaanbaatar, the capital city, is by far the most populated city, with an estimated population of approximately 1.7 million. Some of the rural population (of approximately 1 million people) is nomadic.[5]

In 2024 there were an estimated 2.9 million Internet users in Mongolia, a significant proportion of which uses mobile broadband technologies. An estimated 2 million people were using smartphones.[6] An estimated 2.5 million people were using social media in 2024.[7] In the Network Readiness Index (NRI), which evaluates nations' capacities to capitalise on digital technologies, Mongolia ranked 88th out of 133 countries.[8] Particularly strong indicators were most of the population being covered by at least a 3G mobile network, the use of social networks, and online access to financial accounts and Internet shopping (with relatively small socioeconomic and rural gaps in the use of digital payments).

Mongolia participates in the Global Cybersecurity Index (GCI) by the International Telecommunication Union (ITU), having recently submitted responses to the questionnaire for the fifth edition, published in 2024. In this edition, Mongolia was ranked in Tier 3 out of 5 ("Establishing") overall in terms of cybersecurity commitment. Its areas of relative strength were "Legal measures" and "Organizational measures". In both of these categories, it scored higher than the average for the Asia Pacific region. "Technical measures" and "Cooperation measures" were areas of relative weakness.

To support Mongolia's increasing digitisation, a number of cybersecurity interventions have been made in the last three years. Key examples include the publication of the Law on Cybersecurity in 2021, the publication of the first National Cybersecurity Strategy (NCS) in 2022, and the assignment of new agencies responsible for cybersecurity: the Ministry of Digital Development, Innovation and Communications (MDDIC) in 2022, the National Cybersecurity Council in 2023, and new national Computer Security Incident Response Teams (CSIRTs) established under MDDIC and the General Intelligence Agency (GIA) in 2023. These interventions are an important foundation for enabling progress towards reaching higher levels of cybersecurity maturity in the country, as is described throughout this report.

[4] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf
[5] https://www.1212.mn/en/statistic/file-library/view/86813402
[6] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf
[7] https://datareportal.com/reports/digital-2024-mongolia
[8] https://download.networkreadinessindex.org/reports/data/2024/nri-2024.pdf

The recommendations we make in this report provide our view on the cybersecurity capacity and capability maturity enhancements that Mongolia ought to consider for prioritisation. In some cases, work is already underway as part of ongoing projects but we still include the recommendation since the capacity is not yet fully achieved. The timing of this CMM review also provides an opportunity to make recommendations that may support upcoming activities such as the enforcement of the Law on Cybersecurity in 2025.

REVIEW REPORT

OVERVIEW

This section provides an overall representation of the cybersecurity capacity in Mongolia. Figure 2 below presents the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' at the perimeter.

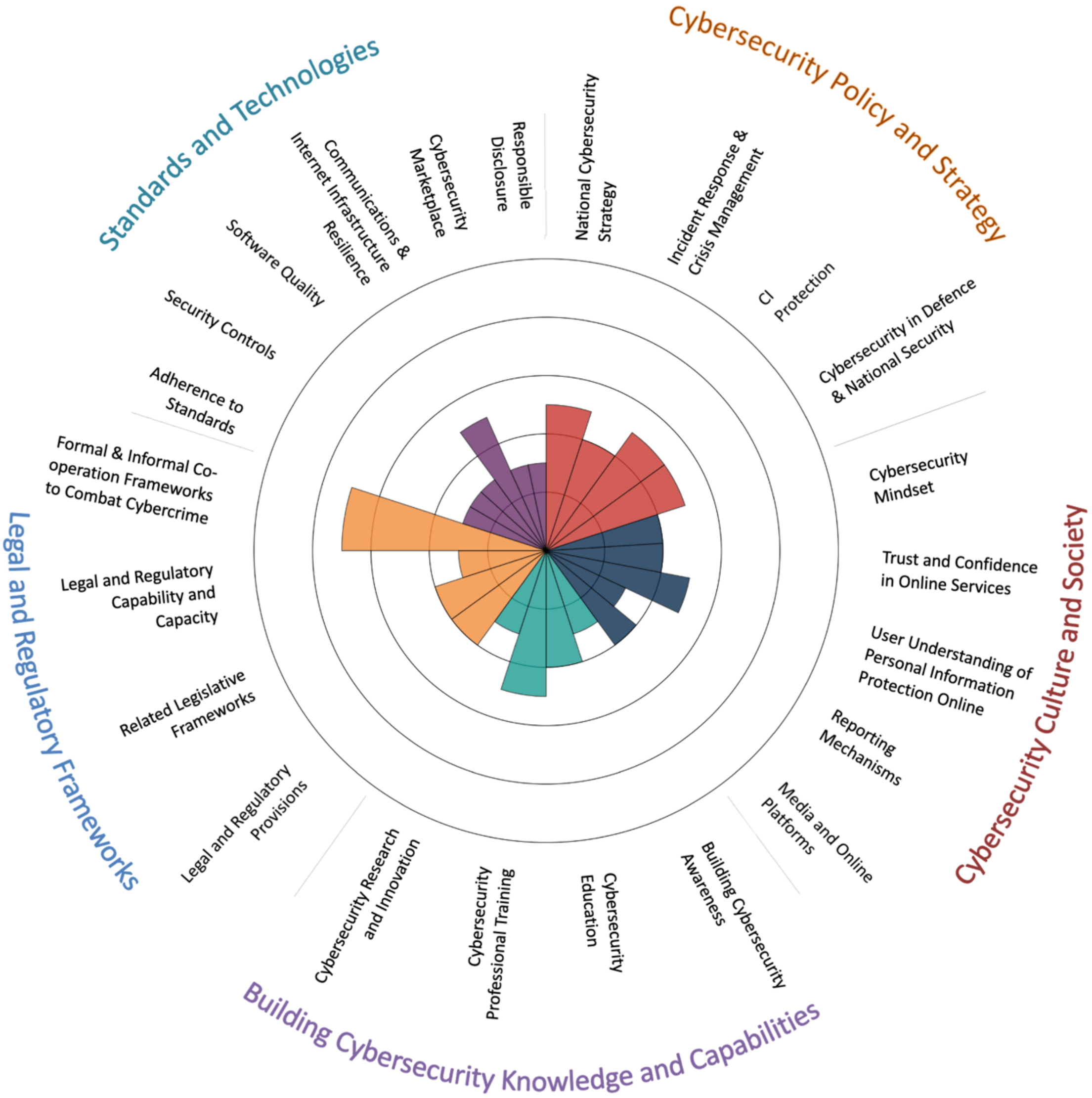
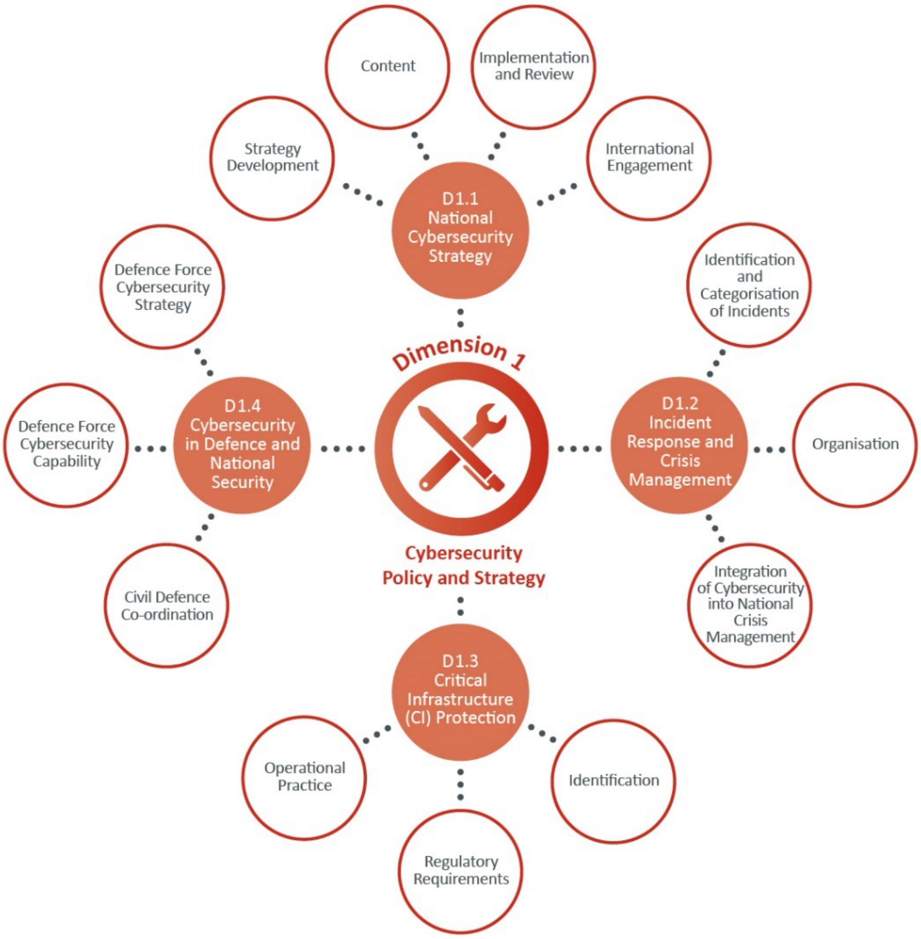


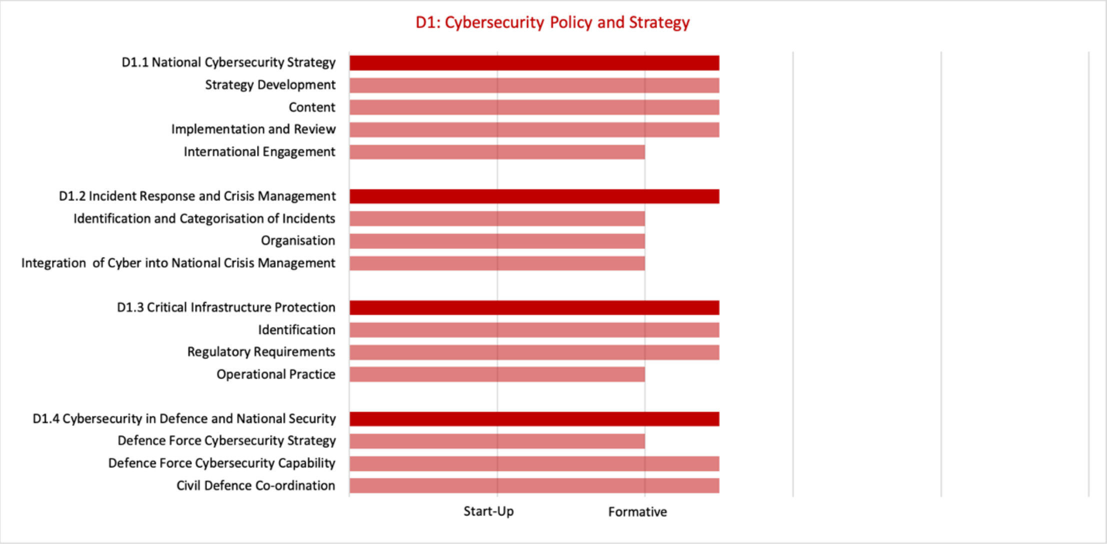
Figure 2: Overall representation of the cybersecurity capacity in Mongolia.

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

This Dimension explores Mongolia's capacity to develop and deliver cybersecurity strategy and enhance its cybersecurity resilience through improving its incident response, cyber defence and critical infrastructure protection capacities. This Dimension considers effective strategy and policy in delivering national cybersecurity capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general.


Content
Implementation and Review
Strategy Development
International Engagement
D1.1 National Cybersecurity Strategy
Defence Force Cybersecurity Strategy
Identification and Categorisation of Incidents
Dimension 1
Defence Force Cybersecurity Capability
D1.4 Cybersecurity in Defence and National Security
D1.2 Incident Response and Crisis Management
Organisation
Cybersecurity Policy and Strategy
Civil Defence Co-ordination
Integration of Cybersecurity into National Crisis Management
D1.3 Critical Infrastructure (CI) Protection
Operational Practice
Identification
Regulatory Requirements

OVERVIEW OF RESULTS



D 1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key cybersecurity government and non-governmental actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities.

Stage: Formative to Established

The first national cybersecurity strategy (NCS) was approved on 28th December 2022 by Decision no. 493 of the Government of Mongolia.[9] It followed the approval of the Law on Cyber Security in December 2021, which provided (through Article 10.1.1) for the development of an NCS[10] and the formation of a National Cyber Security Council[11]. It also followed the establishment of the Ministry of Digital Development, Innovation and Communications (MDDIC), the ministry responsible for cybersecurity at the national level through its Regulatory Department of Cybersecurity Policy Implementation, in 2021.[12]

A working group was created to develop the NCS, consisting of MDDIC, the General Intelligence Agency (GIA), and the General Staff of the Armed Forces. Various wider stakeholders were consulted including representatives from universities and civil society. The development of the NCS was supported by research conducted by MDDIC and GIA: a survey of over 600 government entities and critical information infrastructure (CII) organisations to

[9] https://legalinfo.mn/mn/detail?lawId=16532522757001

[10] https://legalinfo.mn/mn/claw/16390365491061/1646096916023354

[11] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf

[12] https://mddc.gov.mn/eng/%d0%b1%d2%af%d1%82%d1%8d%d1%86-%d0%b7%d0%be%d1%85%d0%b8%d0%be%d0%bd-%d0%b1%d0%b0%d0%b9%d0%b3%d1%83%d1%83%d0%bb%d0%b0%d0%bb%d1%82-2/

establish susceptibility to attack; a survey into the cybersecurity awareness level of the general public; and research into the NCS of other countries in Asia and Europe.

The development of the NCS was therefore based on some understanding of the cybersecurity risks faced by the nation. The view was expressed that the background research conducted does not yet constitute a full national cybersecurity risk assessment. Such an assessment would provide an analysis of the specific cybersecurity risks that confront Mongolia as a nation and the potential impact on the government, on citizens and on business of these risks being realised; it would help to enable the Government to prioritise its interventions. It would be beneficial to identify what is additionally needed to obtain a full picture of the national cybersecurity risk, and how this and other pre-existing research can contribute to this. The NCS itself contains an activity to conduct a national cybersecurity risk assessment, to support development of a "*cyber-attack protection plan and implement continuous improvement controls*". The insights gained from the risk assessment should also be used to inform future NCS updates.

The NCS states that its overarching vision is that "*The security, confidentiality and availability of information of the government, citizens and legal entities in the cyber environment will be ensured at the national level*".[13] Its strategic goals are to: "*Improve the legal framework for cybersecurity, create a unified management system, ensure cyber security of critical information infrastructure, improve flexibility, improve public awareness of cyber security, improve human resource capacity, external and internal. The goal of this strategy is to ensure the security, privacy and availability of information in the cyber environment at the national level through the development of cooperation.*" These strategic goals are to be implemented within the following five objectives:

1. *To strengthen the legal framework and management system to ensure cybersecurity*
2. *To ensure cybersecurity of organisations with critical information infrastructure*
3. *To improve the capacity of human resources, prepare new ones, and retrain them*
4. *To expand cooperation to ensure cybersecurity*
5. *To build the flexibility of cybersecurity and the ability to respond to attacks.*

Within each of these objectives, detailed actions are specified. This includes the establishment of the National Cyber Security Council, which has since been created with the "*functions of providing unified management and coordination of activities to ensure cyber security, organizing implementation, exchanging information, and smoothing the activities*", the establishment of national Cyber Security Incident Response Teams (CSIRTs) and other actions to protect the CII organisations; actions to mitigate cybercrime; and actions to raise public awareness of cybersecurity. The NCS also contains actions to support wider policy objectives, which include improving the legal frameworks for child protection and for the protection of human rights in the cyber environment.

The NCS recognises the need to keep track of risks resulting from the use of emerging technologies through the Action: "*to identify vulnerabilities and threats resulting from the use of advanced technologies such as big data, artificial intelligence, the Internet of Things, cloud technology, and machine learning, and improve the ability to reduce risks*". The CSIRTs will

[13] https://legalinfo.mn/mn/detail?lawId=16532522791411&showType=1

have a role to play, as is described in D1.2, and it will be important to ensure that their insights are used to update the NCS and Action Plan.

The NCS is designed to be implemented in two phases, with Phase I spanning 2022-2025, and Phase II 2026-2027. Within the NCS, outcomes are defined against which the progress of each Objective can be evaluated. These outcomes are specific and measurable against Key Performance Indicators (KPIs). For example, for Objective 1 on strengthening legal regulations, a listed indicator is the number of cybersecurity regulations adopted. These KPIs include the unit of measurement for each indicator, the foundation level (as of the date of NCS approval), the target levels for the end of implementation Phases I and II, and, where relevant the sources of information to be used to measure progress for the indicator. These information sources include planned government research (e.g., surveys of the population); academic research, and international sources such from the International Telecommunication Union (ITU) and Forum of Incident Response and Security Teams (FIRST).

Alongside the NCS, an Action Plan has been developed by MDDIC, GIA, and the General Staff of the Armed Forces. The document is confidential and was not shared with the CMM research team. Participants reported that it follows the government official format for strategy action plans, assigning the primary responsible parties for each action and noting any necessary collaborators. It was reported that the responsible parties are government entities, with the Ministry of Education taking the primary responsibility for actions relating to raising public cybersecurity awareness, for example.

According to the NCS, coordination of the programme to implement the NCS is the responsibility of the government and the National Cyber Security Council. The NCS implementation progress has not yet been subject to evaluation; the first evaluation is planned for the end of implementation Phase I (2025) against the metrics and targets defined in the NCS. The NCS states that MDDIC will be the evaluation department, and will present the results to the Cyber Security Council. Participants reported that if the defined targets are not reached, then the Office of the Cyber Security Council will take follow-up actions and make recommendations for adjustment.

The National Cyber Security Council is a recent establishment, was established according to the Rules of the Council are given in Appendix 01 of Government Resolution No. 42 dated February 1st 2023. The aim is for the Council to meet every quarter and in emergency situations. It was reported, however, that few meetings have been achieved so far due to challenges with availability of members.

The membership of the Council is wide-ranging: it is led by the Prime Minister, the Minister of Digital Development and Communications, and the Head of the General Intelligence Agency. It is composed of the following member organisations: Minister of Justice and Attorney General; State Secretary for Digital Development and Communications; Deputy Chief of the National Police Department; First Deputy Chief of the General Staff of the Mongolian Armed Forces; Head of the National CSIRT; Head of the Public CSIRT/CC; Head of the Armed Forces Center for Combating Cyber Attacks and Violations; Director of the National Data Center; Director of Information and Communication Network LLC; Head of the Office of the Cyber Security Council; and Director of the Communications Regulatory Commission of Mongolia.[14]

[14] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf

This membership should help ensure that it has the necessary visibility and authority to effectively coordinate the NCS implementation programme and act to address any shortfalls.

It will, however, be important to continuously assess the effectiveness of the Council in its current form in coordinating and monitoring the NCS progress. It will be of particular importance to ensure that the Council has sufficiently regular meetings and visibility to identify urgent risks, dependencies, and budget shortfalls in the implementation progress of the NCS during Phases and ensure any issues are addressed. It may also be beneficial to consider a mechanism to engage other stakeholders, such as the private sector and civil society, in the ongoing NCS governance and progress monitoring.

The government organisations assigned responsible for NCS Actions oversee their own budget, and request the necessary budget for delivery in their own ministry budget or secure it from elsewhere. Decision no. 493 of the Government of Mongolia states that "*The members of the government, governors of provinces and capital cities must take measures to include the funds required for the implementation of the goals and activities included in the "National Cyber Security Strategy" in the annual state budget, attract private sector investments, and finance them with foreign loans and aid funds.*"[15] As the NCS states, these budgets are to be resourced through central and local government budget, as well as "*loans and grants from donor countries, international banks and financial institutions , and private alliance investments*".

The monetary resources required to deliver the full NCS implementation programme have been estimated by MDDIC. Representatives from MDDIC reported estimates of the proportions that are achievable through government budget, and of the remainder that is required from elsewhere. It was not clear that all monetary resources required to deliver the programme have yet been secured from external sources. There were also some challenges raised by participants relating to securing funds for cybersecurity from government, with government budgets for cybersecurity not always being approved by the Ministry of Finance. A shortage of cybersecurity professionals was widely cited as being a further factor creating challenges for the implementation of the NCS.

The NCS contains relevant Actions towards expanding international engagement, within Objective 4: "*to cooperate with international and regional organizations that do not conflict with Mongolia's fundamental national interests in the field of cyber security and crime fighting, to seek opportunities to become members of international organizations and join conventions*". It plans to measure the growth in membership of international organisations for cybersecurity at the end of Phase I.

Representatives from MDDIC and GIA participate in international discussions on cybersecurity policy, including at the United Nations (UN) Cybercrime Convention and UN fora on cyber-threat intelligence (CTI) sharing, at the Organization for Security and Co-operation in Europe (OSCE), and at the Cybersecurity Alliance Mutual Progress Network.[16] It was reported that there is a committee dedicated to joining the Budapest Convention, and preparations are being made for this.

[15] https://legalinfo.mn/mn/detail?lawId=16532522757001

[16] https://www.cybersec-alliance.org/camp/membership.do

There is some coordination supporting attendance: GIA reported attending the UN Cybercrime Convention supported by consultations with MDDIC and the Cybersecurity Council. It would be beneficial to formalise the country's engagement objectives, through an assessment (involving all necessary stakeholders) of how the various international debates on cybersecurity policy and related issues affect the country's interests and international standing.

Some Mongolian organisations are participating in international operational collaboration bodies. Police representatives reported participation in the G7 24/7 network for sharing information on cybercrime. MNCERT/CC and the National CSIRT (NCSIRT) are members of APCERT and FIRST, and it was reported that the Public CSIRT/CC is also in the process of joining APCERT. While the NCSIRT is a more recently established institution and joined these bodies more recently, MNCERT/CC reported long-term membership with regular attendance including providing feedback at meetings and being part of the operational members' network. It was reported that, while attendance by MNCERT/CC has been voluntary up until now, with the new CSIRT structures there is a hope for more coordination in these matters between these entities.

Mongolia also has some bilateral agreements with other countries. This includes a Memorandum of Understanding (MOU) between MDDIC and Israel's National Cyber Directorate to exchange information on cybersecurity policies, incidents and best practices, and to cooperate in the field of cybersecurity capacity building. It also includes a cooperation agreement between the United States and Mongolia in 2019 which includes cybersecurity capacity building from MITRE to support the development of an Armed Forces CSIRT and to provide training to the critical information infrastructure (CII) organisations. There is also significant cybersecurity capacity-building support to Mongolia from the Japan International Cooperation Agency (JICA), the United Nations Development Programme (UNDP) and the World Bank.

D 1.2 INCIDENT RESPONSE AND CRISIS MANAGEMENT

This Factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, co-ordinate, and operationalise incident response, and whether cybersecurity has been integrated into the national crisis management framework.

Stage: Formative

There are four national-level CSIRTs in Mongolia. The Cyber Security Law in 2021 made provisions for the establishment of the National CSIRT, Public CSIRT/CC, and Armed Forces CSIRT.[17] Under the Law, incident response in for critical infrastructure organisations in Mongolia is divided between the National CSIRT, established in 2023 under the General Intelligence Agency (GIA), and the Public CSIRT/CC, established in 2023 under MDDIC.[18]

The Law states that it is the responsibility of the National CSIRT to "*detect, terminate and respond to cyber-attacks and violations directed at the information systems of state-owned legal entities with critical information infrastructure and organizations connected to the state information consolidated network, and provide support in the restoration of the targeted information systems*". In other words, it is responsible for protecting government networks and systems, and state-owned CII organisations. The Public CSIRT/CC is responsible for providing these services to entities not stipulated in the former; in other words, private CII and other organisations and citizens. Mongolia also has a long-standing non-governmental organisation (NGO) CSIRT, MNCERT/CC, established in 2014.

According to the Cybersecurity Law, it is the responsibility of the National CSIRT to maintain a database of cybersecurity incidents nationwide. The National CSIRT's operating procedures have been defined and were provided to the CMM research team.[19] They state that "*details of cyber-attacks and violations shall be registered in the Cybersecurity Incident Database and updated regularly*". They state the requirements that apply to the registration of information about cyber violations in the Cybersecurity Incident Database, which include the date and location of the breach, the source and cause, further information about the symptoms, and information about the current situation of the systems affected by the breach.

The Law (Article 21) stipulates the following relevant functions of the National CSIRT: "*conduct analysis, accumulate databases, develop statistical information and surveys, and distribute recommendations and information pertaining to information on cyber-attacks and violations nationwide*" and "*for the purposes of categorizing, processing, information regarding cyber-attacks and violations registered nationwide, and transferring such information to the relevant authorities, operate a team consisting of representatives of relevant organizations*".

The Public CSIRT/CC's rules have also been defined and were provided to the research team.[20] They state that the Public CSIRT/CC has the responsibility to create "a database of cyber-

[17] https://legalinfo.mn/en/edtl/16531350476261

[18] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf

[19] Annex 2 of Government Resolution No. 318 dated August 30, 2023 OPERATING PROCEDURES OF THE NATIONAL CENTER FOR FIGHTING CYBER ATTACKS AND VIOLATIONS

[20] Government No. 08 of 2023 Appendix 1 of Resolution No. 319 dated March 30 "PUBLIC CENTER FOR FIGHTING CYBER ATTACKS AND VIOLATIONS" STATE BUDGET INDUSTRY DEPARTMENT RULES

attacks and violations". The Cybersecurity Law further stipulates that the Public CSIRT/CC must share information with the National CSIRT ("*cooperate and exchange information with the centres stipulated in article 20.1.1, and legal entities stipulated in article 20.2 of this law*").

In practice, both the National CSIRT and Public CSIRT/CC are relatively new establishments, and it was reported that these databases are not yet fully functional. The Database has to-date only registered incidents within the scope of the National CSIRT, and the effectiveness of the exchange of information from the Public CSIRT/CC to the National CSIRT has not yet been fully tested. This will be critical to ensuring that the information registered in the Cybersecurity Incident Database provides a comprehensive picture of the incidents nationwide, especially given that the responsibility for public and private CII is divided between these two CSIRTs. Obtaining this comprehensive picture will support identification and prioritisation of incidents that risk causing national-level impacts. It will also support a more comprehensive understanding of the threat that the country is facing, and full assessment of the national cybersecurity risk, which some participants noted is not yet fully understood.

Some organisations have internal mechanisms for identifying and categorising incidents, and reporting these to the National or the Public CSIRT/CC. This capability varies dependent on the maturity of the organisations, with large organisations in the Finance and Telecommunications sectors generally having the strongest capabilities. Participants reported challenges with incident detection and management by government institutions, with many institutions not having the capabilities to detect incidents themselves, or to respond to incidents and address the vulnerabilities, resulting in reported instances of incidents repeatedly re-occurring within some public institutions.

There are requirements on all CII organisations stipulated in the Cybersecurity Law to have incident-detection systems in place, and to report incidents to the National CSIRT or the Public CSIRT/CC; in particular, the following requirements:

- *Have an information system for the detection, registration, and termination of cyber-attacks and violations*
- *Notify the relevant centre against cyber-attacks and violations immediately of failure of normal, uninterrupted operations of the information systems and infrastructure due to cyber-attacks and violations*
- *Notify the relevant centre against cyber-attacks and violations immediately of failure of normal, uninterrupted operations infrastructure due to planned inspections and audits, damages and events and circumstances of force majeure to networks and systems outside of their own infrastructure.*

As is detailed further in D1.3, the Law is in the initial stages of implementation, and not all CII organisations are yet meeting these requirements.

The capabilities of the National CSIRT and Public CSIRT/CC have not yet been fully tested, since they are relatively new. It remains to be assessed whether the current structures have the necessary resources, skills and processes required to address the range of cyber-incident scenarios that the country is likely to face. Some participants from the private sector cited a view that these government agencies may not have sufficient capabilities to fully respond to all necessary incidents, especially given the pace of technology development, and that more cooperation with the private sector to leverage their technical capacities in this regard might be beneficial.

The Public CSIRT/CC reported that it is currently building capabilities and human resources. Services were provided by MNCERT/CC at the inception of the Public CSIRT/CC to begin building capability. Public CSIRT/CC does not monitor any networks of its constituents (including the private CII), but provides "*recommendations on the security of information systems and information networks of citizens, legal entities, and private sector organizations with critical information infrastructure*" (as stated in the Public CSIRT/CC rules). Public CSIRT/CC also stated that it does not directly support incident response, but notifies victims of potential threats and compromises to which they need to respond.

The National CSIRT reported that of 166 public CII organisations, 56 are connected to the state-owned information network, which National CSIRT monitor and do attack detection for, and perform risk assessments for. They are also responsible for regulating the activities of the other public CII organisations, and supporting incident response. Some concerns were voiced by participants on the capacity of the National CSIRT to support this substantial number of CII organisations, with potential budgetary and staffing shortages cited. Furthermore, it was reported that the public CII has been subject to several Advanced Persistent Threat (APT) attacks. Some concerns were noted about the capacity of the National CSIRT to respond sufficiently rapidly to such attacks, in coordination with the other CSIRTs. Unlike the Public CSIRT/CC, the National CSIRT is not permitted to outsource its operations. It is important that governance mechanisms for the ongoing NCS programme are sufficiently well connected, by gathering input from a range of stakeholders, to ensure that the establishments such as the CSIRTs are functioning effectively and identify any gaps.

Incident-management coordination between the National CSIRT and its public CII constituents is developing. In terms of incident response, state-owned CII organisations are obliged by law to go via the National CSIRT. Representatives from CII organisations reported that, while these responsibilities are provided for in the Law and operating procedures, the mechanisms for incident-management coordination between the CSIRTs and their constituents are early and have not yet been thoroughly tested. The CII representatives present in the CMM sessions reported not yet having experienced any incident-related interactions with the National CSIRT, but having received some advisory notes on infected machines, for example. There was some awareness of the National CSIRT's hotline for reporting incidents and requesting assistance.

Some organisations from the public and private sectors have internal cybersecurity response mechanisms in place, dependent on their maturity. Some cybersecurity service providers reported the view that many CII organisations they consult to currently lack the internal organisational policies to manage cybersecurity incident response. This is supported by the reported findings of cyber drills run my MNCERT/CC with CII organisations, which found that while Finance and Telecommunications sector organisations tend to have the equipment and expertise to manage cybersecurity incidents, organisations in other sectors are lacking. There is a requirement in the Cybersecurity Law for critical-infrastructure organisations to "*Adopt and implement an action plan in case of cyber-attacks and violations"*. As noted above, these requirements of the Law have not yet been implemented by all CII organisations. The Law also requires all CII organisations to have cybersecurity personnel, which has not yet been fully implemented in all organisations but, it is perceived, will improve incident-response capability within CII organisations.

MNCERT/CC also plays a significant role in supporting the cybersecurity of Mongolian organisations (across the economy, both public and private sectors). MNCERT/CC[21] is an NGO operating since 2014 among private member organisations including banks, mobile operators, and major Internet Service Providers (ISPs). It is composed of full-time employees and volunteers. Their services include providing threat intelligence, training, and cyber drills for members (testing incident response against scenarios). They also organise an annual cybersecurity conference, awareness campaigns, and capture-the-flag (CTF) competitions. It is also open for any entity to report an incident, including citizens and non-CII organisations. MNCERT/CC is perceived as being a highly capable entity running since 2014 with skilled cybersecurity experts. It is subscribed to data feeds from various international vendors and uses this track threats that may impact on Mongolian organisations, and MNCERT/CC distributes relevant data to its members via a MISP platform.[22] It has provided some consultancy assistance to the Public CSIRT/CC, including creating reports on the national threat landscape. MNCERT/CC representatives reported plans to develop a platform for its community members to write knowledge-sharing pieces, and suggested that coordinating this with the national and public CSIRTs would be beneficial.

Some representatives from private CII organisations noted that in the case of a cybersecurity incident they would first approach Public CSIRT/CC according to the Law, but would also approach MNCERT/CC for technical assistance. In the case that MNCERT/CC is aware of an incident, or has threat intelligence such as malware reports, that may affect the national or public CSIRTS and their CII constituents, notification is made via the Cybersecurity Council (this is the official channel). It was reported that prior to the Law, sharing of information to necessary parties would have been done through informal channels. Some concerns were raised that under the new structure, it is not clear whether this currently always results in the notifications reaching the necessary CII organisations and CSIRTs.

The National Data Centre (NDC) also plays a role in responding to incidents. Since it hosts the systems of many government agencies, it has previously supported incident detection and response (prior to the Cybersecurity Law) and has continued to do so since the Law, filling a perceived gap in the capability of the National CSIRT to respond to all necessary incidents. NDC representatives stated that given the recency of the Law and new CSIRT establishments, some organisations whose systems they host are still reliant on them for security response. It was noted that this is stretching the resources of the NDC beyond its remit, and it was perceived that the level of involvement from and capabilities of the National CSIRT to provide greater incident-response support would be improving with the new Law. NDC reported having some advanced capabilities including Advanced Persistent Threat (APT) incident-response capacity, advanced malware-analysis capacity, and threat-intelligence generation and sharing.

There may be resource and skills constraints for the national and public CSIRTs to meet the needs of the full range of constituents assigned to them. It is important to identify how CSIRTS can collaborate more effectively using their joint resources, and how to leverage other

[21] https://mncert.org/#/en
[22] https://misp.alert.mn/users/login

elements of the ecosystem, including potentially MNCERT/CC, the NDC, and elements of the private sector. Formalising these relationships, which have been occurring on an ad-hoc basis including through consultancy agreements, may improve their reliability.

It was reported that the issue of coordination between CSIRTs is an issue currently up for discussion by the Cybersecurity Council. Some views were expressed by participants that trust in the National CSIRT may need building further for it to effectively fulfil its role, particularly given its relationship to the Intelligence Agency.

There is some sharing of threat and vulnerability information between the national incident-response bodies and other public and private organisations. Within the NCS is an Action "*to create a legal environment for mutual exchange of information about cyber-attacks and violations by public and private organizations*". Some public CII organisations reported having received threat information from the National CSIRT. It was reported that a platform for CTI sharing between public-sector organisations is in development by the National CSIRT, but is not yet complete. There is also opportunity for exchange of threat information and good practice through monthly meetings and an annual conference hosted by MNCERT/CC for its members.

It was noted that, while there is sharing of information occurring, it is not always reliably reaching all necessary parties, and this is resulting in repetitions of the same incidents over again. Concerns were also cited about the processes that are used to notify the relevant organisations of incidents or vulnerabilities. Participants stated that currently, according to the Cybersecurity Law, this information must be labelled confidential, and, according to Mongolia's laws on information classification, as a result must be sent on paper and viewed only by the officially named recipient at the organisations. This is slowing down the receipt of important information by the organisations, and the restriction of the information to a single person hampers fast remediation.

Some participants from CSIRTs noted the need to clearly define the communications protocols between CSIRTs to be followed during incidents response, and intentions to develop traffic light protocols and PGP communication methods to improve communications between CSIRTs and to their constituents. It is important to establish mechanisms to ensure that threat and vulnerability information shared reaches the national incident-response bodies and public and private-sector organisations that it needs to in a timely manner. This aligns with Objective 5 of the NCS, which includes an Action to "*activate cooperation between centres for combating cyber-attacks and violations and introduce technological solutions for information exchange*".

Some national incident-response bodies are members of international CSIRT networks, facilitating regular sharing of threat and vulnerability information, and operational good practices, with international partners. MNCERT/CC is a longstanding member of APCERT[23] and FIRST[24]. It also has contracts with international threat-intelligence groups such as Shadowserver. The National CSIRT (NCSIRT) reported having joined FIRST and APCERT in 2023, and it was reported that the Public CSIRT/CC is also in the process of joining APCERT.

Within Objective 5 of the NCS is an Action "*to develop the capacity to protect the cyber space at the national level during emergency situations*". A national cyber crisis response plan was

[23] https://www.apcert.org/about/structure/members.html

[24] https://www.first.org/members/teams/mncert-cc

approved in September 2024. Its development was led by the GIA, in consultation with MDDIC. The content of the plan is confidential and was not provided to the research team. Participants stated that in the event of a national crisis scenario with a cyber component, it is the responsibility of the National Cybersecurity Council to create a working group to lead the response. The Plan states that managing the crisis will be the lead responsibility of the CSIRT responsible for the entities being attacked, with the others CSIRTs providing support, and that in the case of a lack of human resources, additional technical skills may be requested from international partners. It also contains clauses stating that it must be regularly exercised.

It was reported that this plan is not yet integrated into broader national crisis management and is treated as a separate IT issue. Furthermore, since it has only recently been finalised, the national cyber crisis response plan has not yet been exercised or used in action. It was noted, however, that several exercises were conducted during the drafting of the plan, to refine the procedures within it. There have also been several joint exercises conducted in the past between the national and public CSIRTs, MNCERT/CC and other entities; MNCERT/CC have conducted cyber drills for Public CSIRT/CC constituents, private CII organisations, through their consultancy agreements with the Public CSIRT/CC. In this drill, the constituents involved were required to a cyber incident, and the ability of the Public CSIRT/CC to coordinate the information (distributing information received from one CII organisation to the others necessary) was tested. It was also reported that MNCERT/CC have conducted cyber drills involving the NDC and the police.

The Plan itself reportedly states that cyber drills must be conducted regularly between the CSIRTs. While there have been drills already conducted with various groups, it will be important that exercises are conducted against the newly finalised national crisis-management plan, involving all relevant stakeholders. This needs to include organisations outside of the cybersecurity establishments who might also be involved in responding to a crisis scenario, such as the CII organisations, to ensure that their dependencies and contingency arrangements are understood. This will help ensure that the necessary processes and relationships are in place to deal with the range of crisis scenarios that the nation may face, and that the capabilities of the responsible organisations are sufficient. Participants noted a concern that while the resources to support the necessary collaborations in the case of a crisis are growing, they may not be sufficient.

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This Factor studies the government's capacity to identify CI assets, the regulatory requirements specific to the cybersecurity of CI, and the implementation of good cybersecurity practice by CI operators.

Stage: Formative to Established

The list of CII sectors is defined in the Cyber Security Law 2021:

Organisations with critical information infrastructure shall include organisations of the following nature of business:

- *Organisations with electricity production, distribution, transmission, and monitoring control systems;*
- *Organisations with clean and waste water, heating source, centralised grid, and distribution and monitoring control*
- *Tier two and three health organisations*
- *Laboratories for research on highly contagious of infectious diseases of humans and livestock*
- *Producers of medicine, and toxic and hazardous chemicals*
- *Banks and financial institutions with consolidated digital systems for payment, settlement, and transactions*
- *Operators in communications, and information technology that are natural monopolies and exercise a dominant position*
- *Organisations with air, railway, waterway, and auto-road transportation coordination and control systems*
- *Organisations that import, producers, and distributors of fuel*
- *Organisations that produce, store, and distribute strategic food stuff*
- *Information and operational management centre*
- *National public radio and television*
- *Organisation in charge of main and supporting information systems and base information databases*
- *Organisation in charge of data centres, their branches and resource centre operations*
- *Organisation in charge of border port control and administration systems*
- *Organisation mining minerals of strategic significance*
- *Organisation in charge of registration, monitoring, and consolidated information systems relating to passengers and transportation vehicles that are crossing the national borders*

Within these sectors, the specific CII organisations have been identified, and the list of operators was published in 2022. There are 216 identified public and private CII organisations, listed within "List of Organizations with Critical Information Infrastructure", which was approved by the Mongolian government in 2022 according to provision 10.1.5 of the

Cybersecurity Law.[25] A working group was formed to lead the definition of the CII, and the process of identifying the specific organisations involved approaching the relevant ministries to identify the relevant organisations within their sectors (e.g., the Ministry of Food and Agriculture reported being consulted on which companies are strategically important for food and agriculture production in Mongolia).

CII operators present in the CMM sessions were aware of their status as CII organisations, and the requirements they are subject to. Some participants noted that organisations falling under parliament (such as the General Election Committee) have not yet been included in the CII list and have requested inclusion to MDDIC.

It will be important that the list of CII organisations is regularly reviewed to ensure that it is up to date against changes in the country's circumstances, and changes in the technological and geopolitical environments. It would also be beneficial to identify dependencies of CII sectors and organisations on each other, and on infrastructures in other countries, in order that these dependencies can be managed.

CII operators are mandated to meet certain cybersecurity obligations. These obligations include adopting internal procedures for cybersecurity; an action plan for cyber-attacks; having an officer charged with ensuring cybersecurity; having cybersecurity risk assessments conducted every year and information-security audits every two years, and breach reporting. Specifically, the Cyber Security Law (Article 19) places the following obligations on CII organisations.

- *Adopt internal procedures for ensuring cybersecurity*
- *Adopt and implement an action plan in case of cyber-attacks and violations*
- *Introduce standards to ensure information security*
- *Have an officer or unit on staff in charge of ensuring cybersecurity*
- *Have cybersecurity risk assessments conducted every year, and where modifications are made to the information systems and information networks have such assessments done partially for each case, and fully if required by the relevant authorities, and take measures in accordance with the conclusion, recommendations, and requirements issues in relation thereto.*
- *Have information security audits conducted every two years*
- *Plan and implement management, organisational, and technical measures necessary for ensuring the information system and information network security*
- *Have an information system for the detection, registration, and termination of cyber-attacks and violations*
- *Store information system action log for the time period stipulated in the common procedure for ensuring cybersecurity*
- *Submit the cybersecurity risk assessment and information security audit reports to the relevant centre against cyber-attacks and violations within one month of receipt*
- *Comply with the requirements issued by the relevant authorities, and take measures to eliminate the violations and errors detected*
- *If cyber security risk assessments are to be conducted by foreign citizens and foreign legal entities, the intelligence agency shall be consulted*

[25] https://legalinfo.mn/mn/detail?lawId=16530379619711&showType=1

- *Have an action plan in place for ensuring the normal, uninterrupted operation of the information system and infrastructure, and for restoration thereof in case of damages and interruptions*
- *Notify the relevant centre against cyber-attacks and violations immediately of failure of normal, uninterrupted operations of the information systems and infrastructure due to cyber-attacks and violations*
- *Notify the relevant centre against cyber-attacks and violations immediately of failure of normal, uninterrupted operations infrastructure due to planned inspections and audits, damages and events and circumstances of force majeure to networks and systems outside of their own infrastructure.*

According to the Law, CII organisations must adopt standards to ensure cybersecurity. MDDIC reported conducting public discussions involving public and private organisations following the publication of Law, to establish which cybersecurity standards should be mandatory for these entities to follow, but due to a failure to reach consensus deemed it infeasible to mandate adherence to any specific standard. The "General Procedures on Cyber Security", enacted in 2023, are a follow-up policy to the Cybersecurity Law, which provide detail on internal procedures that can be followed by these entities. CII organisations are obliged to adopt internationally recognised cybersecurity standards, as well as the General Procedures.

The General Procedures were drafted by MDDIC. It was reported that it is designed to align with the ISO27001 and NIST 8000 cybersecurity standards, to incorporate the minimum common ground. To support the drafting, MDDIC reported conducting surveys in 2021 and 2022 including government and municipal offices, and CII organisations, to identify common issues. Other standards to be followed are also detailed in the General Procedures, including ISO27005 for conducting risk assessments.

Further to this, internal procedures to ensure cybersecurity must be adopted by government entities ("*state-owned legal entities*"), information-technology providers ("*Legal entities providing information technology services in the processing, storing, distributing, computer analytics, and ensuring the normal operations through shared information systems within the cyber space*"), and CII operators. The General Procedures therefore also serve to define the internal cybersecurity procedures to be followed by government entities and technology providers.

Formal processes have been defined to evaluate CII operator compliance with the requirements of the Cybersecurity Law. The Law states that audits and risk assessments must be carried out by service providers registered with MDDIC. The "*Information security audit registration and audit procedure*" has been published[26] and include details on how service providers can register to conduct audits, and on the scope of the audit reports. It states the service providers must have a full-time employee certified by a professional association or standards organisation. The audit reports are then to be provided to the GIA (for public CII) or MDDIC (for private CII), who are responsible for regulating compliance. MDDIC reported that it has recently established a monitoring department for this purpose. It was stated that penalties for non-compliance would be according to the laws for public servants, which could include fines.

[26] https://legalinfo.mn/mn/detail?lawId=16760195603671&showType=1

Participants noted that the enforcement of the Cybersecurity Law is not fully in place yet, since the accompanying procedures on internal policies and audit have only recently been finalised, and the accompanying procedure on risk assessment has not yet been published. The process of issuing licenses for audits commenced in 2023, a first set of audit companies have recently been licensed by MDDIC, and audits are beginning. It was reported that enforcement of compliance will begin in 2025, with the Law's first audit deadline set for August 2025. MDDIC has been conducting some training and awareness raising around the Law and the General Procedures, and reporting having already reached over 600 public-sector employees. Some representatives from CII organisations reported that this support received from MDDIC on how to draft internal policies has been useful. There were reports from some CII organisations of having begun work towards implementing the requirements of the Law, including seeking the approval of their organisation's management to create a separate information security role or department, and developing internal policies.

The implementation of good cybersecurity practices is therefore not yet consistent across the CII organisations. The NCS includes metrics for measuring the progress of CII cybersecurity practice. In some more mature sectors, there is already compliance with cybersecurity standards, and sharing of threat and vulnerability information and best practices between operators.

The view was expressed by several participants, including CII operators and cybersecurity service providers, that the Finance sector is the most mature in terms of cybersecurity practice. This is supported by the findings from the cyber drills previously conducted by MNCERT/CC, involving various CII institutions (see D1.2.3), which reportedly indicate the highest cybersecurity maturity in the Finance and Telecommunications sector. It was reported that in many other CII sectors, there is a lack of the necessary equipment and expertise to protect against and manage cybersecurity incidents.

Organisations in the Finance sector are already regulated for cybersecurity by the Central Bank through the "*Bank Information Technology Criteria Procedure*".[27] Participants from the Finance sector reported the requirement to comply with the International Organization for Standardization (ISO) 27001 standard in order to obtain a banking licence, as well as others dependent on the nature of their operation, such as the Payment Card Industry Data Security Standard (PCI DSS) for card operations. It was also reported that there is a banking Information Sharing and Analysis Centre (ISAC), through which financial institutions share threat and vulnerability information.

In some other CII organisations, for example within the transportation sectors, some organisations are obliged to comply with international regulations such as the General Data Protection Regulation (GDPR) of the European Union (EU) to operate internationally. Participants reported that in some CII sectors, the implementation of cybersecurity good practices is lacking. Healthcare was cited as a particularly important example, given the sensitivity of the data involved, according to research conducted by Mongolian academic institutions, and the views of cybersecurity service providers.

The view was also expressed that cybersecurity practices within some government institutions are lacking, and that these institutions tend not to be as advanced as private institutions, with

[27] https://www.mongolbank.mn/file/beb8a25d6bc7b7f718f2a9a71f0c2b39/files/2018_03_06_A57.pdf

challenges noted relating to the implementation of cybersecurity controls, and the detection and management of cybersecurity incidents. In particular, issues were reported relating to the budget that government institutions have to implement cybersecurity controls, and the shortage of skilled cybersecurity personnel in the public sector.

It is intended that the provisions of the Cybersecurity Law will raise the level of cybersecurity across CII organisations. It is important to note, however, several potential challenges raised that may need to be managed to ensure effective implementation of the Law.

The first area of challenge is the capacity of the identified CII organisations to implement the requirements of the Law. Some organisations consulted expressed concerns about their capacity to meet these requirements.

Organisations from a range of sectors including government, transportation and mining reported concerns relating to the budgets that they have available for cybersecurity, and their ability to persuade the both the management of private organisations, and the Ministry of Finance in the case of public institutions, of the importance of investing in cybersecurity. Concerns were expressed relating to legacy technologies being used in some institutions, and the ability to purchase licenses for software and cybersecurity technologies. On the other hand, it was noted that the Cybersecurity Law may provide leverage to improve cybersecurity budgets within these organisations.

Concerns were also reported relating to the number of skilled cybersecurity personnel these organisations have internally to implement the requirements, and more broadly the shortage of skilled cybersecurity personnel in the country available to hire and the ability hire these personnel into public-sector roles (see further detail in D3). It was noted that support or a different approach might be needed for small organisations: representatives responsible for checking compliance with the Law expressed the view that it may not be reasonable to expect the demands of the Law from such organisations given constrained resources.

The second area of challenge relates to relevant stakeholders' understanding of the Law. Some cybersecurity service providers reported confusion about their authorisation to perform audits of the CII. There was also some confusion reported on logistical matters such as where reports should be submitted, and when the audit cycle begins.

Some views were also expressed that further detail on elements of the Law would be beneficial. CII organisations and audit companies expressed views that more specificity on the standards that must be followed would be helpful. It was the view of MDDIC that, given the lack of consensus in the discussions, it is best to leave this open until the best standards prevail in the market. The view was also expressed that the option given in the Law to have either a cybersecurity department or officer reduces leverage to request a cybersecurity team from organisational management, which is deemed necessary in larger organisations. Some private organisations reported a concern that it is not clear how the confidential information required to be reported by the Law (e.g., audit reports) will be handled, raising concerns about privacy, which may be creating a reluctance to provide detailed information.

It will be important to ensure that stakeholders have a clear understanding of the requirements, in order to ensure smooth implementation of the Law. It would also be beneficial to convene discussions with the relevant CII stakeholders to gain feedback on the Law and areas that may benefit from further detail.

The third area of challenge is the capabilities of the relevant stakeholders to enforce compliance with the Law. Some concerns were noted about the number of local cybersecurity service providers that meet the licence requirements of MDDIC would be sufficient to implement audits for the entire CII. MDDIC reported having recently evaluated the number of local companies with the necessary accredited personnel, and finding that it may be insufficient to meet the CII audit demand of the Law. There were also some concerns raised that some private CII organisations may lack trust in the relevant government institutions' ability to securely handle their confidential reports, which might hinder the reporting process. For the smooth implementation of the Law, it will be critical to identify how to upskill the relevant stakeholders and build trust where necessary.

There are already some plans to convene stakeholders to discuss the implementation of the Law, including through the Annual Cybersecurity Forum run by the Cybersecurity Council. Representatives reported that topics for discussion would include the challenges around audit and the clarity of the Law's requirements.

In summary, the Cybersecurity Law and its accompanying procedures create strong progress towards the protection of the CII. It will be critical to ensure continue to monitor CII organisations' capabilities to interpret and implement the requirements of the Law, to ensure that any shortfalls can be addressed, and support is provided where needed. The NCS itself includes metrics for measuring the progress of CI cybersecurity practice, including the "growth rate of CII organisations that have adopted specialised cybersecurity risk-based practices", and the "growth rate of organisations that have established a recovery and continuity management system", which should help with monitoring progress. It will also be important, as compliance with the Law becomes enforced, to test the effectiveness of the planned regulatory approach.

D 1.4 CYBERSECURITY IN DEFENCE AND NATIONAL SECURITY

This Factor explores whether the government has the capacity to design and implement a strategy for cybersecurity within national security and defence. It also reviews the level of cybersecurity capability within the national security and defence establishment, and the collaboration arrangements on cybersecurity between civil and defence entities.

Stage: Formative to Established

A defence force cybersecurity strategy has not yet been published, and participants did not report any such strategy being under development. Article 14 of the Cyber Security Law places several requirements on the organisation responsible for the cybersecurity of the armed forces. This might be considered as providing the strategic objectives at a high level:

14.1.1. organize the implementation of cyber security legislation in the defence sector;

14.1.2. in times of peace ensure cyber security and the security of defence information systems and information networks, and where necessary provide support in the activities of ensuring cyber security of the nation;

14.1.3. unless otherwise stipulated in the law, verify and certify the equipment and software of the information systems and information networks used in the defence command units and organizations;

14.1.4. organize trainings for defence command units and organizations on ensuring cyber security, and submit recommendations related thereto;

14.1.5. exchange information and collaborate with foreign and domestic organizations of the same function in the area of ensuring cyber security capacity and readiness.

Participants stated that there is no documentation defining the operational doctrine and rules of engagement for cyber defence. It was understood that in the case of international incident response, the National CSIRT would lead.

It is unclear whether the potential impact of cybersecurity on national security and defence has been assessed. Making this assessment is important to supporting the development of a strategy for cybersecurity in Defence, and related operational doctrine and rules of engagement. This analysis should include risks to the ability of the country's military and other national security assets to operate in a contested cyber environment. It should also include assessment of the dependence of national security and military entities on the cybersecurity of other parts of the CI, so that this can be addressed in the defence cybersecurity strategy.

A more detailed defence force cybersecurity strategy should be developed, supported by this assessment. It is also important to ensure that cybersecurity considerations inform other elements of national security and defence strategy, where relevant.

An Armed Forces Cybersecurity Command has been established. Within this structure, the Armed Forces Centre for Combating Cyber Attacks and Violations was inaugurated in 2021, with support from the North Atlantic Treaty Organization (NATO).[28] The establishment of this

[28] https://www.nato.int/nato_static_fl2014/assets/pdf/2021/2/pdf/210208-sps-inauguration-mongolia.pdf

centre was provided for in the Cybersecurity Law, alongside the establishment of the national and public CSIRTs, with the aim of strengthening the country's cyber-defence capabilities, and protecting the networks of the Armed Forces.

There is ongoing training of the cybersecurity command and staff of the Centre. It was reported that the Mongolian National Defence University established a cybersecurity training programme two years ago for personnel from agencies including the armed forces, intelligence agencies, and border control agency. A number of training programmes have reportedly been run since in collaboration with other countries such as India. It was reported that there remains a shortage of trained specialists, and work is ongoing with other countries including the United States (US), India, Korea and Japan, and through NATO partnerships, to prepare specialist staff. No evidence was provided that the sufficiency of the current capabilities has been tested.

Participants in the CMM sessions were not aware of cybersecurity being embedded in wider operational and command training within the armed forces. There are mechanisms in place to facilitate collaboration with allies on training, as noted above. It was unclear from participants in the session whether mechanisms to facilitate collaboration with allies where joint responses are required are in place.

The Cybersecurity Law also assigns the responsibility of the armed forces to "*where necessary provide support in the activities of ensuring cybersecurity of the nation*". Collaboration on cybersecurity between civil and defence entities in the event of a national crisis has been formalised through the national cyber crisis response plan, approved in 2024. Participants stated that the plan requires the CSIRTs (National, Public and Army) to collaborate in the event of a crisis through a joint task force. Representatives from the armed forces stated that they possess the capabilities to provide support. The plan is new and has not yet been tested, but the intention is to conduct regular exercises against it. As such, there is not yet clear evidence of the effectiveness of collaboration between civil and defence entities.

No evidence was provided that the dependencies of the military on civil and CII infrastructures have been assessed. It will be important to establish mechanisms to assess these dependencies, and to assure the ability of civil and CII operators to provide these services.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Government of Mongolia. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1.1 Identify what further work is needed to obtain a full picture of the national cybersecurity risk, and how pre-existing research might contribute to this. This might involve consultation with relevant stakeholders from groups including the CI, national security community and private sector. It should also account for the cybersecurity risks arising from the use of emerging technologies within critical infrastructure, and the wider economy and society.

R1.1.2 Develop a process to regularly refresh the risk assessment in light of a changing threat and technology landscape. Use the information to update the NCS and implementation plan.

R1.1.3 Define outcome-oriented metrics that can be used to monitor the impact that the programme is having on risk and harm reduction. Use these metrics to continuously refine the Action Plan, and to inform funding and priority decisions.

R1.1.4 When evaluating the progress of the NCS at the end of Phase I, test the effectiveness of the planned mechanisms in place to allow strategy owners to monitor achievement of outcomes and address implementation issues. Identify any improvements needed to these mechanisms.

R1.1.5 Ensure that the regular meetings of the Cybersecurity Council are effective at identifying and addressing any urgent challenges or budget shortfalls in the implementation progress of the NCS between the end-of-Phase evaluations. It may also be beneficial to consider a mechanism to engage other stakeholders, such as the private sector and civil society, in the ongoing NCS governance and progress monitoring. This could help increase the bandwidth of the Council, and through input from a wider range of perspectives support the identification of any implementation issues in the various elements of the programme.

R1.1.6 Ensure that there is regular evaluation of the financial resources necessary to deliver the NCS action plan, and that escalation mechanisms are in place for budget shortfalls (enabling trade-off decisions to be made).

R1.1.7 Ensure review and renewal processes for the next NCS are formally in place. These processes should describe how to identify lessons learnt from the current implementation of the strategy.

R1.1.9 Consult with relevant stakeholders to define Mongolia's specific objectives in relation to international debates on cybersecurity. Use these objectives to coordinate the engagement of Mongolian representatives in these debates. Ensure that there is regular validation that the objectives in this area are clear and understood by all participants involved, and that there is a process in place to monitor the achievement of objectives.

INCIDENT RESPONSE AND CRISIS MANAGEMENT

R1.2.1 Test the ability of the distributed system of CSIRTs to function according to the new cyber crisis plan in the event of a major cross-sector cyber incident or crisis. Practical and table-top exercises, involving all organisations that might be involved in responding to a crisis scenario, might help to clarify these processes. It is important that this capability is tested against the wide range of potential cybersecurity scenarios that the country could face, and that exercises take account of changes in the technology and threat landscape. Based on continuous evaluation of lessons learned from these tests, it might be valuable to:

- explore how to enhance the capabilities of the individual CSIRTs, including considering how capabilities available in the private sector might be leveraged to bolster capabilities;
- explore how to enhance the procedures and relationships required for coordination.

R1.2.2 Verify that the information registered to the Cybersecurity Incident Database provides a comprehensive view of incidents nationwide. This is reliant on effective communications channels between the public and national CSIRTs, given that the responsibility for public and private CII is divided between these two CSIRTs.

R1.2.3 Ensure that processes are in place to use the information registered in the Cybersecurity Incident Database to identify, categorise, and initiate response to national-level cyber incidents. Test the effectiveness of these processes; this assessment might be included in the tests described in D1.2.1. Further, it is important to ensure that visibility of cybersecurity incidents in Mongolia is sufficiently coordinated to allow analysis of threat trends, risks, harms and losses that can inform national strategy and the allocation of resources to cybersecurity activities.

R1.2.4 Explore how to enhance the channels for sharing information between the CSIRTs and to other parties (including organisations that may be impacted by a given incident), to ensure that threat and vulnerability information reaches all necessary parties in a timely manner. This might include developing communication methods such as traffic-light protocols and knowledge-sharing platforms, and might draw on the several years' experience of MNCERT/CC.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.3.1 As the Law comes into force, monitor the progress of CII operator compliance with regulatory standards and incident and vulnerability disclosure, and the effectiveness of the planned processes to evaluate compliance. R1.3.2, R1.3.3 and R1.3.4 provide more detail on the elements of this recommendation.

R1.3.2 Monitor the capabilities of the identified CII organisations the implement the requirements of the Cybersecurity Law, and ensure that progress is included in the Council's Key Performance Indicators (KPIs). The planned audits might be supplemented by consultations with CII stakeholders to identify any capability concerns. Explore approaches to supporting the range of CII organisations to ensure that the requirements of the Law can be met. This might include:

- Providing guidance and support to public and private CII organisations to improve incident-detection and response capabilities.
- Providing support on how to increase the budget for cybersecurity technology and staff within private organisations. This might include guidance on how to pitch cybersecurity-budget needs to organisational leadership, or cybersecurity awareness-raising targeting leaders.
- Providing support to public-sector organisations in obtaining budgets for cybersecurity from the Ministry of Finance. It was suggested that creating a separate cybersecurity classification within which public-sector organisations can request budget might be beneficial.
- Identifying what support might be needed to enable smaller organisations to meet their requirements given resource constraints. This might include developing guidance on internal cybersecurity procedures appropriate for smaller organisations, for example.
- Identifying which organisations are able to contribute to providing support.

R1.3.3 Convene discussions with CII stakeholders to obtain feedback on the Law, noting that some stakeholders in the CMM expressed concerns about the clarity and level of detail of the Law, some of which are described in D1.3. It will be important to ensure that stakeholders have a clear understanding of the requirements, in order to ensure smooth implementation of the Law.

R1.3.4 Ensure that the stakeholders involved in enforcing the Law have the necessary capabilities and relationships to do so effectively. Ensure that this is also included in the Council's KPIs. This might include:

- Assessing the sufficiency of the supply of cybersecurity service providers to meet the license requirements to provide risk assessments and audit to all CII organisations.
- Monitoring the relationships of the national and public CSIRTs with their constituents, to ensure that there is sufficient trust and communication to support effective reporting.
- Ensuring that the GIA and MDDIC have sufficient capabilities and resources to regulate compliance.

R1.3.5 Put in place regular review processes to ensure that the list of identified CII organisations can adapt to changes in the country's circumstances, and changes in the technological and geopolitical environments.

R1.3.6 Establish a process to identify dependencies of CII organisations on other CII and non-CII organisations, and on infrastructures in other countries, to understand potential supply-chain and systemic risks and improve the ability to quickly identify risk aggregation. Formally document these dependencies and the approach to managing them.

CYBERSECURITY IN DEFENCE AND NATIONAL SECURITY

R1.4.1 Assess the potential impact of cybersecurity threats on national security and Defence and develop a strategy addressing these risks. Define relevant operational doctrine and rules of engagement to support this strategy.

R1.4.2 Establish mechanisms to assess the dependencies of the military on civil and CII infrastructure. Ensure that reliability and capability of civil and CII infrastructure operators to deliver these services.

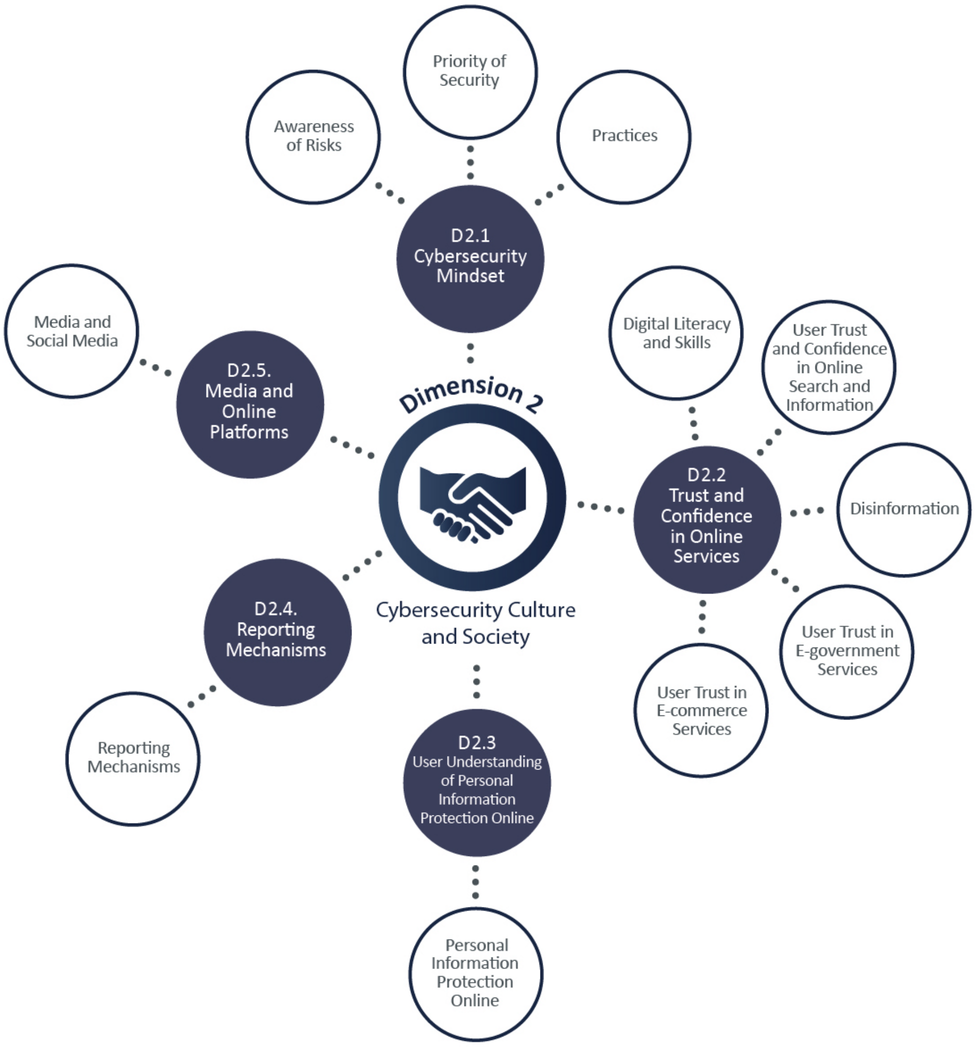
R1.4.3 Test through exercises whether the current capabilities of the defence forces are sufficient:

- To defend the networks and systems of the armed forces;
- To support and collaborate with civil entities in the event of a national crisis;
- To collaborate with allies to share information and respond to incidents.
- Use the findings to inform resource allocation and training priorities.

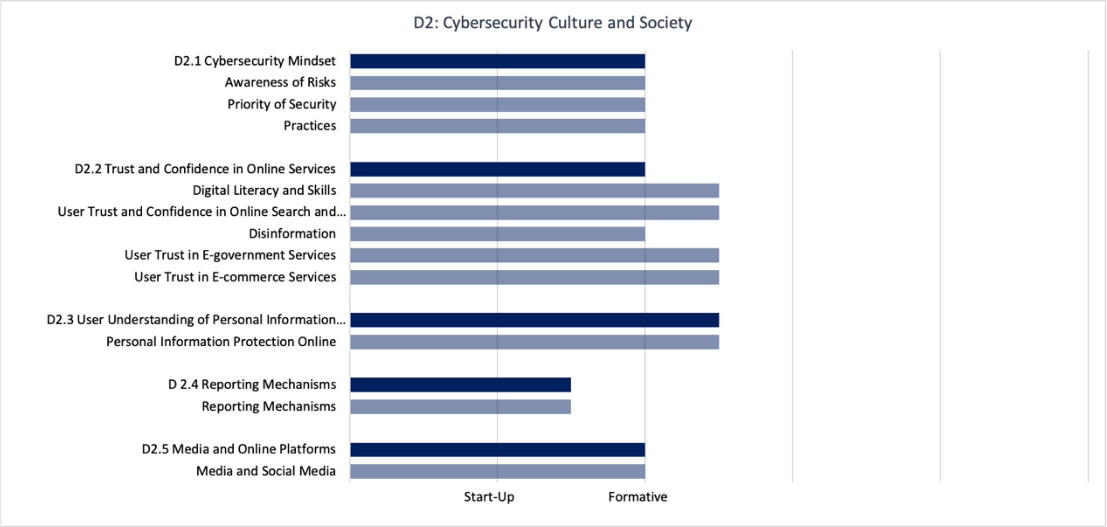
R1.4.4 Embed cybersecurity awareness materials into the wider operational and command training within the armed forces.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

This dimension reviews important elements of a responsible cybersecurity culture such as the understanding of cyber-related risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online. Moreover, this Dimension explores the existence of reporting mechanisms functioning as channels for users to report cybercrime. In addition, this Dimension reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour.


Priority of Security
Awareness of Risks
Practices
D2.1 Cybersecurity Mindset
Media and Social Media
D2.5. Media and Online Platforms
Dimension 2
Digital Literacy and Skills
User Trust and Confidence in Online Search and Information
D2.2 Trust and Confidence in Online Services
Disinformation
Cybersecurity Culture and Society
D2.4. Reporting Mechanisms
User Trust in E-government Services
User Trust in E-commerce Services
Reporting Mechanisms
D2.3 User Understanding of Personal Information Protection Online
Personal Information Protection Online

OVERVIEW OF RESULTS



D 2.1 CYBERSECURITY MINDSET

This Factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society at large. A cybersecurity mindset consists of values, attitudes and practices–including habits of individual users, experts, and other actors–in the cybersecurity ecosystem that increase the capacity of users to protect themselves online.

Stage: Formative

Mongolia has an evolving understanding of the risks associated with digital transformation and cybersecurity. This was evident in discussions with a central group of well-informed government and private sector stakeholders. Within focus group discussions, numerous law enforcement stakeholders, regulators, service providers, financial institutions, business leaders and education experts discussed in detail the various cyber harms they are aware of that require ongoing mitigation. These include electronic fraud, data compromises, cyberbullying, and disinformation to name a few. At a strategic level, leading civil servants and representatives from the private sector were capable of comprehensively outlining the risks cybersecurity poses to national security, economic prosperity, digital development, privacy and social cohesion.

Levels and of awareness and prioritisation have increased substantially since 2021 and the introduction of the new national cybersecurity legislative framework, outlined in Factor 4.1. Many of the mandatory requirements of this framework have required critical infrastructure operators, and particularly the leaders within these organisations, to not only learn about, but invest in cybersecurity. Especially in in relation to human resources, technology and infrastructure. Even before these laws, several stakeholders from the public and private sector indicated that they had been taking, or planning to take, voluntary steps to improve their cybersecurity posture. Moreover, some of these stakeholders have chosen to take additional measures after the law was implemented, such as adopting international cybersecurity standards, demonstrating a concrete commitment to managing cybersecurity risks. The National Cybersecurity Strategy 2022 and its implementation plan provide further evidence of the government's awareness and prioritisation of cybersecurity. Research into awareness levels in Mongolia was conducted as part of the NCS development process and used to inform the strategies objectives. Focus groups indicated that wider research into citizens knowledge of cybersecurity has been conducted by a range of different local authorities and academic institutions, and international partners, such as UNDP.

Despite a recognised degree of awareness amongst these stakeholders, widespread awareness of cybersecurity risks has not been achieved within the broader government, civil society, or the general public. The improvements to cybersecurity awareness and prioritisation instigated by the introduction of the new laws have not been felt universally, with some key stakeholders still knowing little about the laws. Focus group discussion revealed that outside of the government ministries responsible for managing cybersecurity, most government officials and workers did not understand how cybersecurity related to them and not just the IT department. Several stakeholders in focus groups went as far to say that there is an embedded culture amongst many civil servants that information and cybersecurity are not important, and cybersecurity training and development is preferably avoided. Within the private sector, excluding the financial institutions, service providers and specialist information technology companies, the issue is not yet comprehensively understood by most private firms.

Poor awareness levels amongst politicians, senior managers and other government employees were raised as an ongoing challenge undermining the security of both the public and private sector. Even the most knowledgeable stakeholders expressed difficulties keeping up with the rapid pace of modern digital transformation, including recent developments in the field of artificial intelligence. Given the responsibility these stakeholders have to handle critical information and make key decisions, improving their cybersecurity awareness levels should be prioritised as a focal point of national cybersecurity maturity development. For example, low levels of cybersecurity awareness amongst organisations leaders have been found to be particularly impactful at a budgetary level. As a result, increases to the resources allocated to Information Security and Cybersecurity initiatives are often not approved. It is reportedly common for information security professionals to have their requests for more cybersecurity budget, or new technical equipment, denied by their leadership or financial departments. The existing financial processes do not include a separate classification for cybersecurity which is purportedly exacerbating this issue (discussed further in Factor 5.2).

Overall, a cultural shift is required to ensure that digital security and information protection are viewed as the responsibility of every government employee, and not just those in IT roles. Given the scope of work required to fully protect digital systems across the country, it must be acknowledged that it is impossible for designated cybersecurity professionals to manage the issue alone. Simply expanding the number of working cybersecurity employees in an organisation will not address the issue if other workers are not suitably upskilled and made aware of their shared responsibility to facilitate greater security. Comprehensive awareness training programs and routine briefings for senior decision makers should be considered as potential measures to address this challenge.

There is a similar degree of variance in the use of the safe cybersecurity practices as there is in the awareness and prioritisation of cybersecurity. Under the *Law on Cybersecurity 2021*, CII's must conduct annual and bi-annual cybersecurity risk assessments and information security audits with independent approved suppliers and adopt their subsequent recommendations. They must also follow the requirements of the *General Procedure on Cyber Security*, which are outlined further in Factor 4.1. In practice, these requirements are not currently being enforced and CII's adherence to them in patchy. Some CII operators reported having completed their first risk assessment, implemented its recommendations, and are preparing for their first security audit. Whereas other CII operators expressed confusion over what they were required to do and when they needed to have practices implemented by. In the private sector, the financial institutions and internet service providers are leading the way with the implementation of safe cybersecurity practices. While they do not have identical approaches, many of these organisations have already adopted safe cybersecurity practices to comply with international compliance requirements (discussed further in Factor 5.2).

Beyond this leading group of stakeholders, focus groups revealed that most users are not following safe cybersecurity practices. Poor password management, the use of private emails and messaging software for official information sharing at work and not using two factor authentication were commonly discussed poor cybersecurity practices. Frequent attacks through social engineering and phishing provide further evidence that users are not implementing safe practices. High rates of electronic fraud and increasing cybercrime rates in Mongolia provided further indication that the public is failing to comprehensively follow safe cybersecurity practices.

D 2.2 TRUST AND CONFIDENCE IN ONLINE SERVICES

This Factor reviews critical skills, the management of disinformation, the level of users' trust and confidence in the use of online services in general, and of e-government and e-commerce services in particular.

Stage: Start-up to Established

Mongolia has a growing rate of digitally literate internet users who regularly use online social media platforms and e-services as part of their daily routines. This activity is enabled by a robust network of ICT-infrastructures that facilitate user connectivity (discussed further in Factor 5.4). There are several programs in place that support digital and media literacy skills development, including active programs in Mongolian primary and secondary schools and vocation centres, initiatives with international development partners such as UNDP[29] and UNESCO[30], and targeted civil servant training through the e-Mongolia Academy.[31] Combined, high rates of digitally connectivity and widespread digital-literacy education opportunities mean that a growing number of users feel confident using the internet.

Evidence of high rates of trust and confidence in online services are supported by data collected through ad hoc assessments of digital literacy rates, and users' online activities and digital competencies. These include assessments by the Accelerator Lab of UNDP Mongolia[32], UNCTAD[33] and the World Bank.[34] According to the `World Bank Global Findex Database 2021, 99% of people have access to mobile phones, 97% have made or received a digital payment and 93% have made a digital online payment.[35] A significant portion of this digital economic activity is taking place in the domestic market through well-established e-commerce and e-government services. These include online banking, retail, event sales, business services and the governments' e-Mongolia platform, which comprises hundreds of government services at the national and local levels, and is used by millions of Mongolian citizens.[36] E-government in particular is a strategic priority of the Mongolian government which is trying to build an 'e-Nation' through its 'Vision-2050' national development plan. The development of e-governance services has received significant support for international partners, including from the World Bank[37] and the Asian Development Bank.[38]

[29] https://www.undp.org/mongolia/blog/experimenting-learning-and-innovating-improve-digital-inclusivity-and-literacy-mongolia

[30] https://www.unesco.org/en/articles/ministry-education-unesco-and-icdl-asia-launches-teachers-digital-skills-training-pilot-project

[31] https://blog-pfm.imf.org/en/pfmblog/2023/02/e-governance-and-e-treasury-systems-advance-in-mongolia

[32] https://www.undp.org/mongolia/blog/iterating-mongolian-version-digital-literacy

[33] https://unctad.org/publication/mongolia-etrade-readiness-assessment

[34] https://www.worldbank.org/en/publication/globalfindex/Data

[35] https://www.worldbank.org/en/publication/globalfindex/Data

[36] https://www.telecomreviewasia.com/news/interviews/2791-mongolia-to-take-digital-development-to-a-new-level/

[37] https://www.worldbank.org/en/news/press-release/2022/06/06/mongolia-new-project-helps-the-government-go-digital-and-grow-the-economy

[38] https://www.adb.org/sites/default/files/project-documents/55211/55211-001-tar-en.pdf

Leading stakeholders from the private and public sectors managing key digital services recognize the need to protect them with strong security measures, and in the case of CII, are required to do so under law (Factor 4.1). Despite this, it was acknowledged that the security of each system is depended on the management of those systems and some organizations have implemented higher security controls than others (discussed further in Factor 5.2). The government has taken steps through the implementation of the *Law on Electronic Signatures 2021* to establish greater security controls and improve trust in digital transactions. While there are surveys on digital literacy and use of technologies, there were none identified that examined trust in e-commerce or e-government services specifically.

At a user level, high rates of digital literacy and uptake of digital services in Mongolia are not accompanied by the routine use of safe cybersecurity practices, or widespread awareness of how to stay safe online. Most Mongolian internet users are reportedly unable to identify legitimate and illegitimate websites and digital services from each other and were described as “gullible” and even “digitally silly” by some focus group participants. Poor cyber literacy skills, stemming from poor levels of awareness, were identified as a significant challenge and risk to ongoing prosperous digital development in the country (discussed further in Factor 2.1). Furthermore, focus group discussions highlighted that there is an urban and rural divide between the rates of digital service adoption, with proportionately fewer people in rural areas using e-services. It was suggested that this did not stem from a lack of connectivity, but rather limited access to inform rural users on how to use new e-services. In general, it is perceived by many Mongolians that people living in rural areas and other vulnerable populations are the least proficient at protecting themselves online.

Focus group discussions indicated that mis and disinformation are present challenges in Mongolia that are being amplified by online platforms. Some steps have been taken by leading civil society and non-governmental actors to help address the issue. Specifically, the Nest Centre for Journalism Innovation and Development created a fact-checking network in 2023 to provide Mongolian citizens with a resource for addressing misinformation.[39] The ‘Mongolian Fact Checking Centre’ as it is now known is the only group in Mongolia accredited by the International Fact Checking Network.[40] Outside of these efforts, broader efforts by the government or platform providers were not identifiable. Online mis and disinformation are not outlined as priorities in any available strategic government documents.

[39] https://www.nestmongolia.org/facts-first-mongolia-7

[40] https://meedan.com/post/meedan-and-nest-center-launch-mongolias-first-fact-checking-tipline

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This Factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protecting personal information online, and whether they are sensitive of their privacy rights.

Stage: Formative to Established

Privacy is a fundamental human right of the Mongolia people under the Constitution of Mongolia. Mongolia has a robust data privacy framework that was established through the *Law on Personal Data Protection 2021* (discussed further in Factor 4.2). It includes provisions for the collecting, processing, using and security of personal data that all 'Data Controllers' must follow. The law applies equally to the analogue and digital environments. One of the key obligations under these provisions is for all 'Data Controllers' to approve and enforce internal data collection, control and security policies. In force since 2022, these policies are now widespread in Mongolia. MDDIC and the National Human Rights Commission have oversight over the implementation of the law. Through its security and oversight provisions, the law has established clear measures to try and balance privacy and security needs. Mongolia has frequent and robust public debates about striking a balance between security and protecting human rights as part of its routine policy making processes. At various points these debates have included discussions on digital rights and security protections. Some of these debates emerged in focus group discussions with local constituents.

At a user level, people do not know what measures they can or should take to protect their personal information online. Focus groups demonstrated that some users and stakeholders within the public and private sectors have a limited understanding of how digital data is stored and how they can better protect their own information, but this knowledge is not widespread beyond a core group of well-informed people. Culturally, it was suggested that the Mongolian population is not generally aware of how their digital data is used online, and most of the ordinary people in Mongolia are not well aware of the data privacy rights they are provided in the legislation outlined above. On a practical level, only a limited number of internet users in Mongolia follow safe cybersecurity practices and most do not take the necessary steps to secure their online data.

D 2.4 REPORTING MECHANISMS

This Factor explores the existence of reporting mechanisms that function as channels for users to report Internet-related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

Stage: **Start-up to Formative**

Reporting mechanisms for cybersecurity incidents, cybercrimes and other cyber harms are established in Mongolia and operating with some degree of coordination. The National Police Authority, National CSIRT and Public CSIRT/CC are all provided with a mandate under the *Law on Cybersecurity 2021* to receive information pertaining to cybercrimes, cyber-attacks and other violations from their various constituents. The National Police Authority typically interfaces with the public, while the National CSIRT interfaces with state-run institutions and the Public CSIRT/CC interfaces with private sector CII. Stakeholders in Mongolia stated that they are aware of these reporting mechanisms, with some confirming that they have formally integrated reporting to their affiliated entity into their incident response processes. Outside of these entities, the e-Mongolia platform has a child protection reporting mechanism that may also be used for offences committed via digital means.[41] In addition to this, there is also a special dialup phone number people can use to report any child-related offences.[42] Amongst commercial banks, there is also a private reporting mechanism which allows them to exchange information with each other.

Focus group discussions with various stakeholders confirmed that while there is a desire for these established reporting mechanisms to work closely together, they currently do not operate in a coordinated manner. Instead, for the most part, the different reporting mechanisms are siloed from each other. Article 20.3 of the *Law on Cybersecurity 2021*, the Public CSIRT/CC is mandated to share information with the National CSIRT on cyber-attacks and violations, but in practice information exchanges occur in an ad hoc fashion. Some focus group participants also expressed difficulties with getting users to utilize the reporting mechanisms, especially children. Shame and limited levels of awareness were attributed as the key reasons for users choosing not to report incidents. There is limited evidence that users employ existing social media channels to inform each other of cybersecurity incidents.

Information on metrics of reported incidents is generally unavailable. However, under the *Law on Cybersecurity 2021,* the National CSIRT is required to register and regularly update details of cyber-attacks and violations in a 'Cybersecurity Incident Database'. This provides some indication that some metrics of reported incidents are in place.

[41] https://www.ekids.mn/#/index
[42] https://108.mn

D 2.5 MEDIA AND ONLINE PLATFORMS

Stage: Formative

This Factor explores whether cybersecurity is a common subject of discussion across mainstream media, and an issue for broad discussion on social media. Moreover, this Factor looks at the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Traditional and digital media outlets publish coverage of cybersecurity matters sporadically. This includes coverage of international cybersecurity awareness month, cybersecurity events, cybersecurity policy developments, cybercrime cases and more.[43] In some instances, media coverage has incorporated information on how readers and viewers can implement proactive and actionable cybersecurity measures to protect themselves online. Focus group stakeholders inferred that while the media may cover cybersecurity on an ad hoc basis, it is not typically seen as an issue of great importance to most journalists. Stakeholders further suggested that the media is not usually engaged in cybersecurity awareness campaigns, and this has prevented greater improvements to national awareness levels.

As discussed in Factor 2.4, it is perceived that there is limited use of social media to discuss cybersecurity incidents. Many internet users feel the same apprehension towards cybersecurity that is felt by journalists. Despite this, there are some documented cases of organizations using social media to promote cybersecurity awareness campaigns.

Mongolia has an accepting attitude toward whistleblowers. This culture of acceptance has grown as its democracy has matured. Whistleblower protection legislation current sits before the Mongolian parliament which would enshrine this culture into law.[44] However, there are some concerns that delays in the adoption of this legislation, and regressions in the protection of protesters and press freedoms more widely, may undermine the progression of a positive whistleblower culture in Mongolia.[45]

[43] https://www.zindaa.mn/3hh1
https://news.mn/r/2373711/?fbclid=IwY2xjawG6fJ5leHRuA2FlbQIxMQABHZjlsohDaTlb_geFXBXNPOhjVkshaxx4SYMufxrxkN4kMYcqTtS5vFfb_w_aem_aEn7mV15PrsgdCCbE1DSdw
[44] https://montsame.mn/en/read/316173
[45] https://uncaccoalition.org/uncacparallelreportmongolia/

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *Cybersecurity Culture and Society*. These aim to provide possible next steps to be followed to enhance existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

CYBERSECURITY MINDSET

R2.1.1 In order to improve general levels of cybersecurity awareness and elevate the prioritisation of cybersecurity, implement the awareness-raising and training actions outlined in **R3.1.1** and **R3.3.1**. Ensure to include specific activities related to improve cybersecurity knowledge amongst senior executives, civil servants, CII and vulnerable and disadvantaged groups.

R2.1.2 Develop a cybersecurity e-learning and assessment portal that enhances cybersecurity awareness and skills among all civil servants across the Mongolian government. The portal should provide training, interactive modules, and assessments tailored to various roles and responsibilities, fostering a culture of cybersecurity and ensuring compliance with national and organisational standards.

R2.1.3 To improve the adoption of safe cybersecurity controls and improve cybersecurity practices by users, implement the security control measures outlined in each of the **R5.2** recommendations. Consider how Security Operating Procedures (SOPs) and Acceptable Use Policies (AUPs) may also be utilised to improve cyebrsecurity practcies within the civil service.

R2.1.4 To help facilitate a more resilient national cybersecurity mindset, leading cybersecurity stakeholders in Mongolia should take steps to establish a growth mindset within the cybersecurity ecosystem that encourages organisations and users to learn from their mistakes and each other, and rewards closer collaboration and cooperation between stakeholders.

R2.1.5 Ensure metrics are defined and surveys conducted, in order to gain a full picture with respect to the mind-set among users, the public sector and private sector.

TRUST AND CONFIDENCE IN ONLINE SERVICES

R2.2.1 Invest in further support for stakeholders such as the e-Mongolia Academy, RAGDS and the Public CSIRT/CC to continue to conduct digital literacy trainings and improve accessibility to e-government and e-commerce services, with a particular focus on vulnerable, disadvantaged and rural communities. Coordinate with broader training initiatives recommended in **R3.3.1** and cybersecurity awareness raising activities recommended in **R3.1.1**.

R2.2.2 Integrate mis and disinformation modules into awareness building initiatives outlined in **R3.1.1** and digital literacy training outlined in **R2.2.1**.

R2.2.3 Integrate media and information literacy educational modules into awareness building initiatives outlined in **R3.1.1** and digital literacy training outlined in **R2.2.1**. These modules should teach citizens how to critically evaluate online information, recognise biased or false content, and understand the role of media in shaping public perception.

R2.2.4 Implement measures to enhance the security framework of e-government to help mitigate the risks of digital fraud and cybercrime, in connection with the security control measures outlined in the **R5.2** recommendations.

R2.2.5 Conduct nation-wide surveys with a focus on digital trust. Use these findings to guide the development of policies and initiatives aimed at building trust in digital systems and improving internet security awareness. Coordinate with activities recommended in **R3.1.1**.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.3.1 In coordination with any human rights impact assessments undertaken in relation to R4.1.10, routinely re-assess Mongolia’s digital privacy and cybersecurity legislation with respect to the privacy rights of users. Ensure that an appropriate balance in maintained between security and privacy within the legislative framework.

R2.3.2 Undertake efforts to gradually raise internet users' awareness of digital privacy issues and their rights under Mongolian law. Consider linking these efforts to the broader national cybersecurity awareness initiative outlined in **R3.1.1**.

REPORTING MECHANISMS

R2.4.1 Implement measures to build trust and confidence between different entities with ownership of reporting mechanisms to facilitate improved information sharing and coordination.

R2.4.2 Undertake initiatives to raise awareness amongst internet users and CSIRT constituencies of available reporting mechanisms.

- Take steps to clearly define the appropriate place to go based on the type of issue being reported.
- Consider using various platforms, including social media, television, and community outreach programs, to inform users on how and where to report cybersecurity incidents, data breaches, and suspicious activities.
- Encourage engagement by making the reporting process simple, accessible, and transparent.

R2.4.3 Ensure data for all reporting avenues is collated in metrics and surveys, in order to gain a full picture of any reporting activities. Where appropriate, consider how information collected through different reporting mechanisms (volume, types of incidents reported, and user demographics) may be used to help identify trends, improve response strategies, and assess the effectiveness of awareness campaigns and reporting mechanisms.

MEDIA AND ONLINE PLATFORMS

R2.5.1 Encourage media to report not only on major cybersecurity incidents but also on best practices and increase their personal cybersecurity awareness. This may involve providing them with greater insights into cybersecurity developments where appropriate and more material to help develop stories (e.g. through press releases, interviews with leading officials, event invitations etc.).

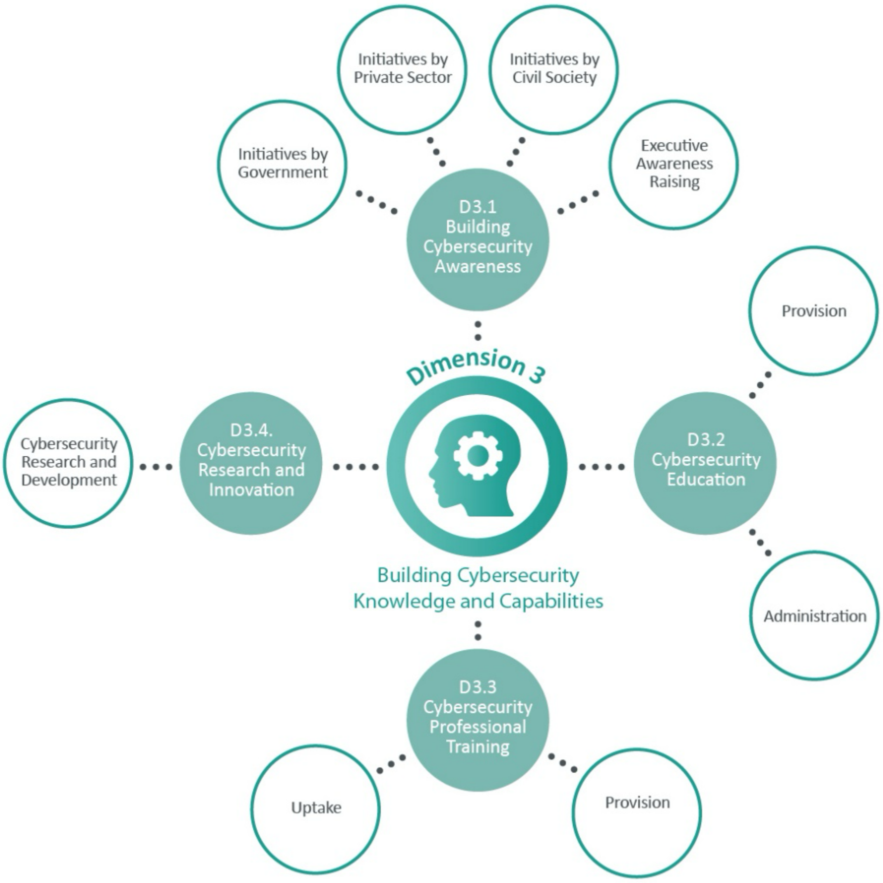
R2.5.2 Consider methods of more strategically integrating media stakeholders into awareness initiatives discussed in **R3.1.1**.

R2.5.3 Consider methods of more strategically integrating social media platforms into awareness initiatives discussed in **R3.1.1**.

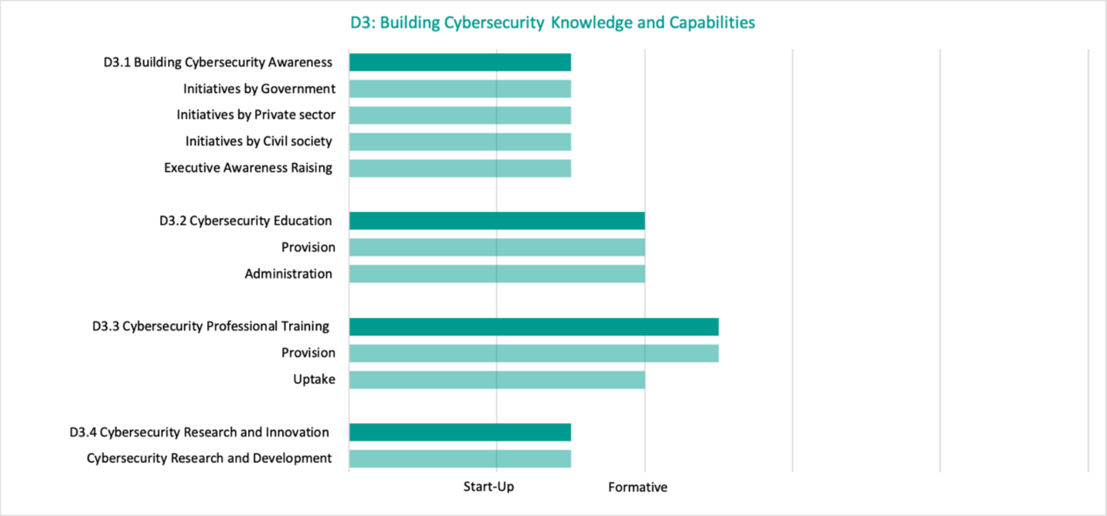
R2.5.4 Revisit draft whistle blower legislation and consider methods of successfully progressing legislated whistle blower protections.

DIMENSION 3
BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

This Dimension reviews the availability, quality and uptake of programmes for various groups of stakeholders, including the government, private sector and the population as a whole, and relate to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes, and professional training programmes.


Initiatives by Private Sector
Initiatives by Civil Society
Initiatives by Government
Executive Awareness Raising
D3.1 Building Cybersecurity Awareness
Provision
Dimension 3
Cybersecurity Research and Development
D3.4. Cybersecurity Research and Innovation
D3.2 Cybersecurity Education
Building Cybersecurity Knowledge and Capabilities
Administration
D3.3 Cybersecurity Professional Training
Uptake
Provision

OVERVIEW OF RESULTS



D 3.1 BUILDING CYBERSECURITY AWARENESS

This Factor focuses on the availability of programmes that raise cybersecurity awareness throughout the country, concentrating on cybersecurity risks and threats and ways to address them.

Stage: **Start-up to Formative**

Mongolia has a patchwork of different cybersecurity awareness programs and activities that are being administers by a range of different entities in an un-coordinated manner. These include government run campaigns by the Communications Regulatory Committee, the Regulatory Agency on Government Digital Services, the National Police Agency, MDDIC, and the national and public CSIRTs.[46] Between them, these campaigns have targeted a range stakeholder groups perceived to be more vulnerable, including children, young adults, people over 40, stay at home parents, and small and medium enterprises. They have included a variety of different content, including television advertisements, in-person presentations, engagements with influencers, and other social media materials.

At a strategic level, improving public cybersecurity awareness, and organising campaigns, trainings and seminars to provide knowledge and understanding on cybersecurity is one of the major goals of the 2022 National Cybersecurity Strategy. From a legislative standpoint, the Ministry of Digital Development, Innovation and Communications (MDDIC) has a mandate to raise awareness of cybersecurity issues and legislation through the *Law on Cybersecurity 2021*.

[46] https://crc.gov.mn/list/internetijn-s-lzhee-jlchilgee/mn?show=104
https://www.facebook.com/ekids.mn/
https://gogo.mn/r/o3d8j

In the past year the ministry has conducted a series of trainings on the *General Procedure on Cyber Security*, and numerous campaigns targeted at SMEs.[47] However, for the most part, MDDIC has delegated this responsibility to the Public CSIRT/CC to fulfil this role. Focus group discussions raised mixed opinions on the quality and frequency of the Public CSIRT/CC's awareness activities. There was consensus that more consistency and strategy was needed to effectively increase public awareness of cybersecurity. More broadly there was agreement that despite these positive efforts, more work is needed in this area to improve perversely low awareness levels. Therefore, despite the strategic prominence of raising cybersecurity awareness, it may be concluded that within government there is still work to done to develop a coordinated awareness raising framework that is proportionate to existing demand, sustainable and effective.

Outside government, the private sector has conducted a range of different awareness raising activities for cybersecurity. These include a collaboration between the National University of Mongolia Student Club and the banking sector to conduct in-person awareness raising events, and general advocacy by public banks promoting safe cybersecurity practices.[48] Prominent examples of this can be seen of the YouTube page of one of the nation's largest banks which has developed multiple high quality digital literacy and security videos for its customers and the broader public.[49] Focus groups revealed that it is common for many private sector enterprises, who are perceived to have a higher level of comprehensive cyber maturity overall, to have internal awareness programs and portals available to their staff.

Within civil society, MNCERT/CC, a community CSIRT, has been actively engaged in improving cyber literacy and awareness through information sharing and other designated activities for over a decade.[50] While not specifically an awareness activity, each year MNCERT/CC also holds Mongolia's biggest cybersecurity conference which helps to facilitate cybersecurity discussions and improve cyber knowledge amongst a range of different stakeholders.[51] Furthermore, many of Mongolia's international development partners have also conducted cybersecurity awareness programs, including JICA, UNDP and USAID. In 2022 USAID funded the "My Online Information is Mine campaign" which involved a collaboration with Mongolian pop artists in partnership with We Think Digital by Meta and the Faro Foundation.[52] More recently, UNDP through its acceleration lab, has been working to raise cybersecurity literacy and awareness amongst Mongolian stakeholders with a thematic focus of 'leaving no-one behind.' Separately, they have also implemented a nationwide awareness campaign that involved online learning resources, cybersecurity games, webinars, workshops and community outreach programs. One of the numerous activities being undertaken by JICA is a program to try and try and develop a cybersecurity awareness collaboration project, bringing together different stakeholders in this space. It is believed that this project is in its initial stages and that JIVA has experienced some difficulties in its implementation.

[47] https://www.youtube.com/watch?v=coBpQk-sVkQ&list=PLuEgz5swNEEbCuqPam1qFh_f435jyCsYh

[48] https://news.mn/r/2373711/?fbclid=IwY2xjawG6fJ5leHRuA2FlbQIxMQABHZjlsohDaTlb_geFXBXNPOhjVkshaxx4SYMufxrxkN4kMYcqTtS5vFfb_w_aem_aEn7mV15PrsgdCCbE1DSdw
https://www.youtube.com/watch?v=q9Vx7AvHVKo

[49] https://www.youtube.com/@KhanBank.officialv

[50] https://cscouncil.gov.mn/en/cybersecurity-professionals-participated-itactic-training

[51] https://mnsec.mncert.org/event/

[52] https://www.usaid.gov/asia-regional/press-releases/feb-28-2022-usaid-launches-cybersecurity-awareness-campaign

Comprehensive cybersecurity awareness training programs for executive level leaders in the private or public sectors were not identified by focus group discussions or desktop research. Some limited awareness building opportunities were discussed in focus groups, namely a one-off program to take some leaders from various government ministries to Japan to learn from Japanese experts and ad hoc trainings by GIA, but nothing comprehensive. It is widely believed by many cybersecurity employees that their leaders lack a strategic understanding of the issue and the challenges confronting their operations. Multiple focus group participants reported facing resistance from their organisational leaders on issues relating to cybersecurity. It was stated that leadership generally did not want to increase the cybersecurity budget or support more substantive training opportunities. Many people expressed a strong desire to see tailored awareness raising programs for executive level decision makers to help overcome this entrenched opposition to cybersecurity spend and prioritisation.

Evidently there are a lot of individual awareness building programs being undertaken in Mongolia; however, they lack strategic coordination, are often duplicative and are not successful in overcoming a prevalent and persistent awareness gap amongst the Mongolian populace (Factor 2.1). Focus group discussions repeatedly raised the issue of limited funding for public awareness campaigns as an obstacle in this area, in addition to poor awareness amongst executive level decision makers. A lack of outcome-orientated metrics that could be used to evaluate the impact of awareness campaigns was also identified within focus group discussions. Furthermore, no evaluations of existing campaigns appear to have been completed and mechanisms for updating campaigns according to performance or recipient feedback are not in place. Focus group participants expressed a need for improved cybersecurity data collection practices that may be used to inform more contextualised and effective awareness campaigns. Finally, despite including specific goals aimed at raising cybersecurity awareness levels, the national strategy does not include an implementation plan for awareness raising activities.

D 3.2 CYBERSECURITY EDUCATION

Stage: **Formative**

This Factor addresses the availability and provision of high-quality cybersecurity education programmes and sufficient qualified teachers and lecturers. Moreover, this Factor examines the need to enhance cybersecurity education at national and institutional levels and the collaboration between government and industry to ensure that educational investments meet the needs of the cybersecurity education environment across all sectors.

Improving the capacity of human resources, preparing new ones and retaining them are a central component of Mongolia's National Cybersecurity Strategy 2022. Several of the activities listed in the strategy for doing so are directly related to the expanded provision of cybersecurity education, including an aspiration to provide knowledge on cybersecurity in the curriculum of education institutions at all levels. Growing demand for cybersecurity professionals is universally recognized amongst all stakeholders in Mongolia who are constantly trying to compete with each other for human resources. This demand is reflected in both national university enrolment indicators and focus group discussions. In some instances, it was reported that demand for cyber skillsets was so high that private sector organizations, the General Intelligence Agency (GIA) and National Police Agency were offering advanced employment contracts to high-performing students in their second and third years of study. Despite this, Mongolia does not have a nationally coordinated strategy between the government, industry and the education sector to improve the supply of cybersecurity professionals.

Qualifications for tertiary degrees related to cybersecurity are available from several of Mongolia's leading universities, including the Mongolian University of Science and Technology (MUST), Mongolia International University (MIU), and the National University of Mongolia (NUM) and the National Academy of Governance. MUST has been offering an undergraduate 'Information Network' program since 2002 and has more recently commenced a 'System Security' program, both under the Department of Information Networks and Security. Between the courses they have graduated hundreds of undergraduate students.[53] A specific cybersecurity master's program (2 years) has recently been approved at MUST and is being supported by MDDIC and JICA through a grants program.

NUM, through the Department of Information and Computer Science, offers 'Information Systems', 'Information Technology', 'Computer Science' and 'Software Engineering' undergraduate programs.[54] The Department of Electronic and Communication Engineering also offers a 'Computer Networking' course enables students to select up to 40% of their courses from cyber-related-subjects, and graduate with a minor in cybersecurity. The university delivers its trainings in a specialised 'Network, Systems and Cybersecurity Laboratory'. Furthermore, NUM offers a range of doctoral and master's courses in these same subject areas and has three full-time lecturers specialising in cybersecurity and information

[53] https://www.sict.edu.mn/en/210

[54] https://registration.num.edu.mn/Admission/Programs/2

security, and one contract lecturer. MIU provides a computer science undergraduate program and a software engineering program, both of which include computer security components.[55] MIU also has a master's level software engineering program that has a 'security-sensitive software' component.[56] The National Academy of Governance has been delivering training courses in the field of information security based on content from a university in South Korea. Their courses were updated in 2024 with an enhancement of the university's cybersecurity program. Finally, the National Defence University provides a cybersecurity program that trains resources for the militaries cyber command unit.

Focus group discussions indicated that vocational training centres in Mongolia do offer cybersecurity training opportunities that attract enrolments from across the labour market. Stakeholders reported that some cybersecurity education is provided to Mongolia primary school and vocational students through a broader information technology curriculum; however, this information could not be verified through desktop research. It was further reported that primary school children are taught some general information about cybersecurity, such as knowledge about the legislative framework and privacy rights, but not security directly. Focus groups and desktop research failed to identify the inclusion of cybersecurity within the curriculum of secondary school education.

Despite the recognised demand for skilled cyber professionals, the availability of formal education courses and demonstrated interest from students, it is difficult for Mongolia's higher education institutions to provide the equipment and staff necessary to deliver graduate outputs that meet industry expectations. Universities have reported difficulties in hiring and retaining their own education staff due to high demand and salaries for their skillsets in the private sector and abroad, and challenging workloads that make the positions unattractive. A lack of widespread physical teaching environments that facilitate attack and defence simulations, digital forensics training and other more technical trainings have further undermined educational outputs. The expense of developing and operating such facilities is too much for the higher education sector to support themselves without government or industry support. Previous research form United Nations on ICT skills in Mongolia indicates that this has resulted in largely theoretical course curriculums that are not producing industry ready graduates.[57]

To overcome staffing challenges some higher education institutions, such as MUST, have developed two-plus-two programs which enable students to split their universities studied between two different universities. This allows the universities to effectively pool their staff resources and fill teaching capacity gaps. MUST has two-plus-two programs operating with the Mongolian National University of Defence and overseas universities in Korea, Japan and Taiwan. These programs have proven popular with students and the model has been extended to include master's programs (one-plus-one). There have been some reported difficulties in encouraging students to return from abroad after they have completed their studies which may undermine the success of these programs.

Additional educational capacity building support is being provided by international partners such as JICA, UNESCO and the UNODC; however, this support is not currently coordinated.

[55] https://miu.edu.mn/computer-science/
https://miu.edu.mn/software-engineering/
[56] https://miu.edu.mn/master-se/
[57] UN eTrade readiness assessment (p. 59)

JICA’s “Project for Development of Human Resources in Cybersecurity” stands out in this area as being of particular relevance and importance to the education sector. Launched in 2023, it has three goals: build a collaboration network among industry, academia, and government for cybersecurity human resource development; develop and organise cybersecurity educational programs for students and working professionals; and develop and organise cybersecurity educational programs for public servants.[58] Within this work JICA has undertaken work to analyse the necessary cybersecurity skills needed in Mongolia today, modernise cybersecurity curriculums at the tertiary level, and implement train-the-trainer activities. The scope and importance of this work highlights the significance of international capacity building partners in the education sector and need to incorporate them into broader higher education strategic planning.

[58] https://cybilportal.org/projects/project-for-development-of-human-resources-in-cyber-security/

D 3.3 CYBERSECURITY PROFESSIONAL TRAINING

This Factor addresses and reviews the availability and provision of affordable cybersecurity professional training programmes to build a cadre of cybersecurity professionals. Moreover, this Factor reviews the uptake of cybersecurity training, and horizontal and vertical cybersecurity knowledge and skills transfer within organisations, and how this transfer of skills translates into a continuous increase of cadres of cybersecurity professionals.

Stage: Formative to Established

As discussed in Factor 3.2, Mongolia's National Cybersecurity Strategy recognises the development of cybersecurity human resources as an area of strategic importance. The strategy outlines a national goal of 'preparing the human resources of organisation with special functions to combat cybercrime and terrorism' and implementing 'short, medium and long-term training for the empowerment and qualification of human resources to ensure cybersecurity'.[59]

Multiple structured and ad-hoc cybersecurity training programs are available in Mongolia and positioned to help fulfil this goal, including some that offer internationally recognised cybersecurity certificates. The programs are implemented by a wide variety of education providers, including vocational centres, private cybersecurity training centres and institutes, and international capacity building partners. These include trainings provided by ICT Training[60], InfoSec Plus[61], system Center[62], Empasoft Institute of Technology[63], NUM (partnership with EC-Council and ACT, and CISCO Academy) and the National Information Technology Park. The cost of each training opportunities varies, and some training institutions cited a notable shortage in organisations capable or willing to afford the high costs of training materials and examination fees for international certification.

Training for law enforcement personnel in particularly occurs frequently. The University of Internal Affairs even has a special academy for training law enforcement officers, as discussed in Factor 4.3. On top of these trainings, several professional training programs have also been conducted in partnership with JICA, India, CISA, Carnegie Melon and MITRE, through the coordination of MDDIC. JICA in particular has provided extensive training support for academic and professional staff in cybersecurity, including programs that incorporate train-the-trainer exercises.[64] The National CSIRT has also separately provided specialised cybersecurity trainings for their constituents.[65] Within civil society, MNCERT/CC reportedly

[59] Mongolia National Cybersecurity Strategy, p.2.

[60] https://www.ict-training.mn/courses#Security

[61] https://www.infosecplus.mn/

[62] https://systemcenter.io/

[63]https://empasoft.ider.edu.mn/home_english/#COMPUTER-NETWORK-AND-INFORMATION-SECURITY

[64] https://openjicareport.jica.go.jp/pdf/1000050862.pdf
https://cscouncil.gov.mn/en/japanese-experts-lead-cyber-security-training

[65] https://cscouncil.gov.mn/en/cybersecurity-professionals-participated-itactic-training

conducts frequent cybersecurity drills and delivers training programs for its member organisations. Such closed community specialised training programs received positive endorsement from focus groups participants. Finally, some more mature private and public organisations are reported to have established in house cybersecurity training programs.

Many of the trainings which MDDIC has organised with international partners have required CII to attend. Each of these trainings has included approximately 50-100 participants. MDDIC has communicated that they only have the capacity to hold at most one such training per month, and the sheer number of critical infrastructure operators means that progress is slow. It was widely reported that many of the trainings occurring in Mongolia have been designed based on international security standards and models of best practice, such as ISO 27001. However, some providers reported difficulties keeping their material up to date because of challenges with translation. Metrics that evaluate the uptake and impact of training opportunities have not been established or used to evaluate their effectiveness.

Focus group discussions indicated that government and private sector enterprises routinely engage with these trainings opportunities, when they can afford it, and that there is a high appetite for cybersecurity professional training overall within Mongolian organisations. Recent changes to the cybersecurity legal and regulatory framework, including the introduction of *Law on Cyber Security 2021* and *General Procedure on Cyber*, have helped to fuel demand for these programs. The legislative requirements for critical infrastructure operators to employee cybersecurity staff, and conduct regular risk assessments and information security audits, has helped to raises the prioritization of cybersecurity and importance of training amongst senior organizational leadership. Some institutions, such as the General Intelligence Agency (GIA) are even required by law to conduct cybersecurity training exercises for relevant staff (article 13.1.2).

Nevertheless, despite some improvements of the degree to which leaders in Mongolia priorities cybersecurity due to recent legislative reforms, focus groups participants expressed that it can still be difficult to receive approval to attend trainings. It was reported that organisational leaders are concerned with staff absences, training costs, and a general apprehension at funding staff to participate in development programs that will simply enable their workers to find new employment opportunities with better salary options. Consequently, it was reported that organizations leaders favour training programs that are short and cheap, as opposed to more substantial investments into long-term staff upskilling.

Difficulties training and retaining cybersecurity staff are particularly prevalent in the public sector, which is constrained by inflexible salary bands, ministerial silos, and a lack of competitive advantages compared to the private sector. It was believed by many focus group participants that the positive training measures being introduced across the government are being used by employees as a launching pad into roles in the private sector or abroad, rather than successfully filling internal skills shortages. The cybersecurity skills shortage is so severe that once employees receive recognized cybersecurity certifications or prolonged career experience, they immediately become attractive employees within the broader labour market. These dynamics are making it incredibly difficult for government entities, including the CSIRTs and state-owned critical infrastructure operators, to retain their staff long-term. Attracting new staff to the civil service is further complicated by lengthy application processes that many young people find unattractive. To become a civil servant, prospective employees need to pass multiple exams and undertake extensive processing, which not only slows down recruitment times, but motivates interested applications to search for easier application options. In the past the traditional benefits of the public sector were attractive to employees, but this is no longer the case for the current generation.

In light of these challenges, the Mongolian government is undertaking some efforts to prevent the ongoing drain of human resources and improve recruitment within the public sector. For example, MDDIC has instigated a train-the-trainer program that will facilitate the targeted transfer of cybersecurity knowledge between employees, leveraging localized expertise. To date they have trained 100 trainers. Furthermore, through the leadership of MDDIC, the government has implemented a new employment classification for information security professionals that enables them to sit outside the civil servant classification. This new classification allows these professions to be paid more and avoid the traditional application processes, but not receiving the traditional civil service entitlements. While this new employment framework is promising and indicates that the government is trying to implement measures that resolve their skills and retention issues, under this framework each government agency is only entitled to two such employees. Focus group participants expressed concern that this was insufficient to allow them to hire enough resources to fill their existing skills shortages. MDDIC confirm that expanding the quotas of this classification scheme will be a difficult process which would likely require all of the original quotas to first be filled. At present, the scheme has received positive uptake by some agencies and been ignored by others. Beyond of this classification scheme, MDDIC has confirmed that they're investigating the feasibility of establishing a specialized information security pay bonus within government, similar to the existing bracket bonus in place for government workers who manage sensitive information. Under this proposed scheme information security professionals would be paid 30% on top of their existing salaries to manage cybersecurity issues.

Outside of government, private sector employers also face challenges finding a sufficient supply of skilled cybersecurity professionals to meet their needs, despite their advanced maturity levels. Many have reported struggling to find and retain resources due to fierce competition between domestic and international employers. Particular areas of the private sector, such as banking and finance, are equipped with a more sophisticated cybersecurity workforce. This is typically because they can afford to pay their employees above market rate and are not constrained by extensive bureaucracy. With this being said, focus groups indicated that money is not the only motivating factor in employee's decision of employer. Structured career progression, quality of leadership and work cultures were also identified by stakeholders as strong influencing factors on their employment decisions. Overbearing workloads for cybersecurity professionals working in understaff teams was another commonly identified reason why employees chose to leave or change jobs.

In addition to challenges retaining staff and the questionable benefits of training programs, the consistency and quality of training opportunities were also criticised by focus group participants. Currently, it is common for skills to be built on the job through unstructured learning.[66] Dedicated long-term training programs for cybersecurity professionals in the civil service do not exist, and both management and workers are therefore faced with the ongoing challenge of identifying and funding new training opportunities. Assistance form international

[66] UN e-Mongolia Assessment, p. 59

partners is highly welcomed as most Mongolians believe the quality of educators to be superior to the local training options. MDDIC has done their best to strategically coordinate international training opportunities; however, any efforts to do so are complicated by the sporadic nature of these opportunities which are not dependable form a planning perspective. Some international training partners, such as JICA with the support of MDDIC, have conducted needs assessments of the economy and tailored their training programs to try and tactically fill local knowledge gaps.

Nevertheless, despite their clear qualities and benefits, utilising only international training suppliers cannot sustain the degree of educational uplift required to address the existing Mongolia cybersecurity skills gap. Efforts by domestic training providers to improve their localised training capacity have been undermined by difficulties in translating and applying international standards and best practices. Combined, the higher education sector, vocational sector and network of professional development opportunities currently available in Mongolia are struggling to produce the quality and quantity of cybersecurity professionals needed to meet the national demands or accomplish its strategic objectives.

D 3.4 CYBERSECURITY RESEARCH AND INNOVATION

Stage: **Start-up to Formative**

This Factor addresses the emphasis placed on cybersecurity research and innovation to address technological, societal and business challenges and to advance the building of cybersecurity knowledge and capabilities in the country.

Mongolia's NCS includes a goal of empowering security qualified human resources. Under this goal, 'implementing a program to support the training, research and academic work of cybersecurity researchers' is a core activity. Furthermore, under the *Law on Cybersecurity 2021*, the 'state central administrative agency in charge of digital development and communications' is mandated to 'conduct new technical, technological, innovation, research and development activities in areas of cybersecurity.' The strategy and legislation combined indicate that the Mongolian government has a high-level desire to expand its research expertise in cybersecurity and advance domestic innovation in the area.

In practice, some stakeholders have contributed to cybersecurity research and development activities in Mongolia. Academics from Mongolian universities have published studies on cybersecurity and information security in international journals and some universities are emphasising research innovative research into cybersecurity. However, evidence of wide-ranging cybersecurity research and innovation in Mongolia remains limited.

Focus group discussions indicated that Mongolia's higher education institutions are constrained by inadequate technical and human resources which restrict their ability to more robustly conduct R&D activities, as outlined in Factor 3.2. No active research consortium with international or regional partners or networks could be identified, nor could any research or career performance metrics related to R&D. Outside of academia no evidence was found to indicate that private sector companies are active in cybersecurity R&D.

RECOMMENDATIONS

Following the information presented on the review of the maturity of *Building Cybersecurity Knowledge and Capabilities*, the following set of recommendations are provided to Mongolia. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

BUILDING CYBERSECURITY AWARENESS

R3.1.1 Under the leadership of the Cyber Security Council, establish a coordinated national cybersecurity awareness program for the Mongolian public. This program should:

- Establish a steering committee or other identified body with robust community support*,* to coordinate and scale cybersecurity awareness activities in Mongolia and help to avoid ethe duplication of initiatives. This entity should be tasked with taking responsibility of the activities and actions listed below.
- Conduct an evidence-based assessments of national awareness gaps that consolidates existing research of digital literacy and awareness levels in Mongolia, and draws from the cybercrime data collected in the Cybersecurity Incident Database (National CSIRT).
- Facilitate ongoing consultations with active awareness raising stakeholders from government, law enforcement, the private sector, civil society and international partners to ensure the cohesive implementation of initiatives in areas that address national awareness gaps and accomplish the goals of the NCS.
- Develop and promote a wide variety of materials through various modes of communication.
  - Ensure these materials are contextualised to align with the media consumption patterns of targeted audiences.
  - Include specific components for improving awareness amongst vulnerable populations (e.g. low-income, migrant, remote, elderly, and people with disabilities) and small businesses.
  - Ensure materials are culturally and linguistically appropriate for all audiences.
- Incorporate activities and messaging that are designed to facilitate behavioural changes amongst targeted audiences in addition to raising awareness of cybersecurity.
- Enhance and complement the work JICA has commenced to facilitate greater coordination of awareness activities.
- Develop a national cybersecurity portal (single point of contact) to store and continuously promote awareness-raising materials from all prior and existing campaigns.

R3.1.2 Develop a targeted cybersecurity training and awareness raising program for executives and other senior decisions makers in the government and private sector. Consider attaching appropriate certifications and incentives to these programs to attack participation from targeted stakeholders.

R3.1.3 Develop a targeted cybersecurity training and awareness raising program for people from rural areas. Consider partnering with local leaders to help tailor programs to the rural context and assigning designated training units or ambassadors to help facilitate this work. Coordinate these activities with the digital literacy trainings for rural communities recommended in **R2.2.1**.

R3.1.4 Develop a targeted cybersecurity training and awareness raising program for civil servants from across the Mongolia government to enhance their cybersecurity skills and capabilities and improve the overall cyber resilience of the public sector. Coordinate with the e-learning and assessment portal recommended in **R2.1.2**.

R3.1.5 Provided long-term funding to support the organisation and delivery of the national cybersecurity awareness program. Consider allocating funding for human resources to conduct coordination activities.

R3.1.6 Create a national Metrics System to collect data on cybersecurity education and use it to support the review and revision of education activities. This can include statistics on supply and demand for cybersecurity awareness.

CYBERSECURITY EDUCATION

R3.2.1 Task the leading education authority for primary and secondary schools, in coordination with leading cybersecurity entities, to review and revise national school curriculums in order to incorporate foundational cybersecurity awareness and security content.

R3.2.2 Identify ways of further clarifying and promoting cybersecurity career paths to students at school and university level, to ensure that a lack of awareness of the career options does not block future enrolments in cyber-related higher education courses.

R3.2.3 Implement measures to encourage people from non-Computer Science degrees (or STEM degrees) to undertake courses in cybersecurity.

R3.2.4 The Mongolian government and higher education sector should work together to implement measures that remove or reduce financial barriers to enrolment in cybersecurity courses. Consider the use of scholarships, bursaries, industry co-funding, and other similar measures to help reduce the cost burden on prospective students and increase the appeal of cybersecurity courses.

R3.2.5 Investigate co-funding models between academia, the private sector and government to improve the IT learning environment in Mongolian schools and higher education institutions that are necessary to educate industry ready cybersecurity graduates.

R3.2.6 Further enhance and expand two-plus-two programs as a means of overcoming limitations in the domestic education sectors capabilities, while implementing provisions that ensure students return to work in the domestic job market. E.g. scholarship funding contingent on returning from abroad.

R3.2.7 Invest in training programs for cybersecurity academic staff to boost the capability and supply of cybersecurity educators in Mongolia. These programs should build on JICA's existing efforts in this area and incorporate train-the-trainer provisions.

R3.2.8 Implement programme review processes and outcome-oriented metrics to review the supply and demand for cybersecurity courses as well as the supply and demand for cybersecurity graduates in the country.

R3.2.9 In alignment with the goals outlined in the NCS and using the above recommendations, develop a national cybersecurity education strategy that established a long-term shared vision for improving the provision and administration cybersecurity education, designates stakeholders responsible for delivering the different components of the strategy and allocates sustainable funding to implement the strategy.

CYBERSECURITY PROFESSIONAL TRAINING

R3.3.1 Under the leadership of the National Cyber Security Council, develop a sustainably funded national cybersecurity human resource training initiative between the government, industry, international partners and academia to improve the quality and supply of cybersecurity professionals. The program should undertake the following measures:

- Establish a steering committee or other identified body with robust community support, to identify, coordinate and scale existing cybersecurity training programs in Mongolia and implement the follow actions.

- Compile an evidence-based analysis of the cybersecurity skills gaps in Mongolia's professional workforce, either through existing research or a new assessment, to identify priority areas for training investments.
- Establish a national cybersecurity human resource development strategy and implementation plan through broad consolation with relevant stakeholders for addressing the identified skills gaps.
- Coordinate and build upon existing professional training programs and expertise to administer the strategies implementation plan and avoid the duplication of initiatives.
- Integrate cybersecurity modules into existing digital literacy programs in schools, vocational centres and community groups.
- Help translate the latest international cybersecurity standards to the Mongolian context in order to improve the quality of domestic education opportunities. Align with **R4.1.4** and **R5.1.2.**
- Ensure the appropriate people are attending the right training courses to maximise the efficiency and effectiveness of programs.
- Investigate mechanisms for reducing or removing cost barriers to training to incentivise increased participation rates. Align with **R3.2.4**.

R3.3.2 As stated in **R3.1.4**, create a national Metrics System to collect data on cybersecurity education and use it to support the review and revision of education activities and curriculums. This can include statistics on supply and demand for cybersecurity awareness.

R3.3.2 Invest in existing or new training programs designed to strategically address well recognised skills bottlenecks. These may include gaps in CII, the civil service, law enforcement and senior management.

R3.3.3 Support MDDIC's existing efforts to facilitate special salary exceptions for cybersecurity professionals that would enable the government to compete with private industry for scarce skills. Consider means of improving agency awareness and uptake of existing specialized cybersecurity quotas, and potential salary uplifts for specialized cybersecurity works.

R3.3.4 To help improve the retention of staff in the civil service, develop structured and transparent career pathways for cybersecurity professionals that include embedded training opportunities and salary progression. Consider working with mission critical cybersecurity human resources to create tailored career plans that suit the person goals and contexts. Consider how incentives such as support for the acquisition of international certification, connected to requirements to remain in employment, may be incorporated into these plans.

R3.3.5 To help improve the retention of staff in the civil service, implement management and workload allocation processes that prevent overburdening of human resources and professional burn out. In leading cybersecurity agencies, such as MDDIC and GIA, further support organisational management fill all available recruitment positions and consider expansions to the number of allocated employees were necessary.

R3.3.6 Seek to enhance public-private partnership in the area of cybersecurity as a means of cross sectoral knowledge sharing and capability development. It may be beneficial to offer secondments from the private sector to public-sector cybersecurity roles.

CYBERSECURITY RESEARCH AND INNOVATION

R3.4.1 Provide funding for MDDIC to conduct R&D activities in the area of cybersecurity as outlined under the Law on Cybersecurity 2021.

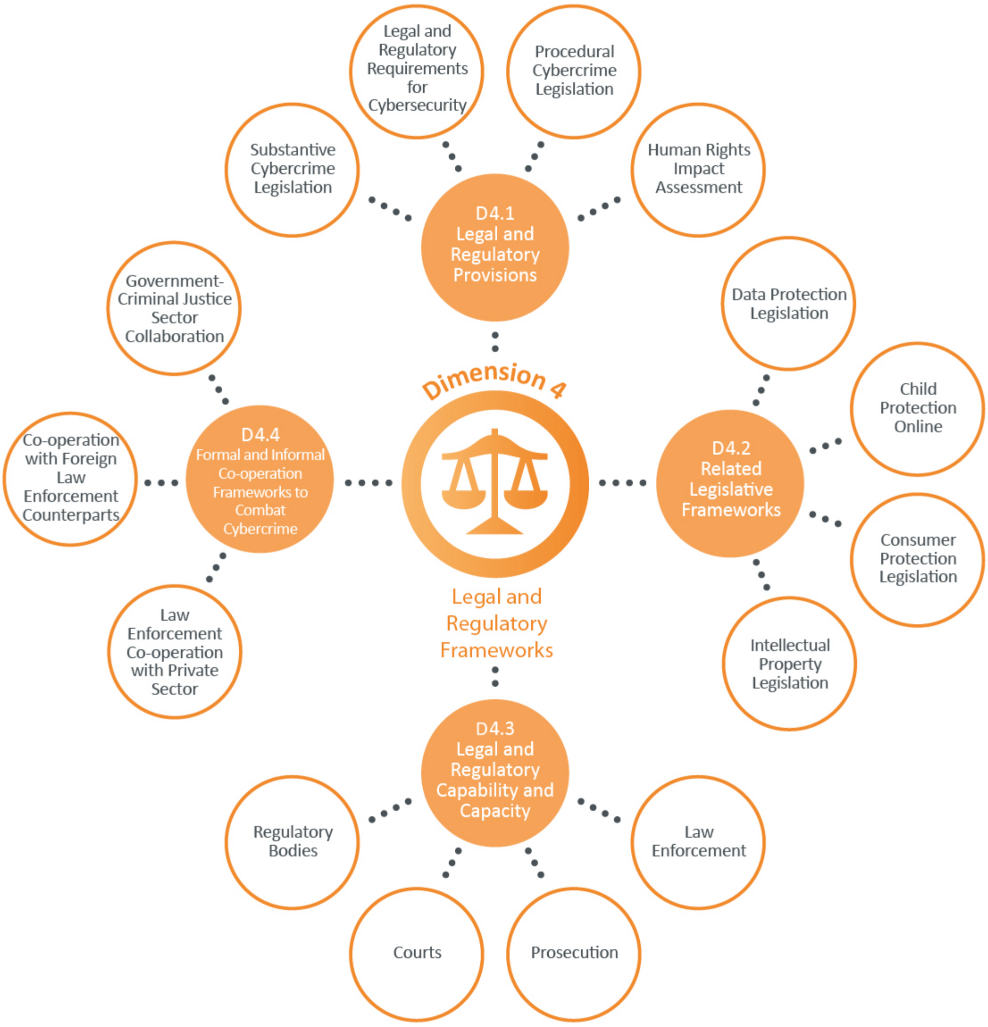
R3.4.2 Provide funding through the form of research grants to academic institutions to support cybersecurity research as specified in the NCS.

R3.4.3 The Mongolia government should consider providing support to researchers in academic institutions to help commercialise their produces and grow the local cybersecurity marketplace.

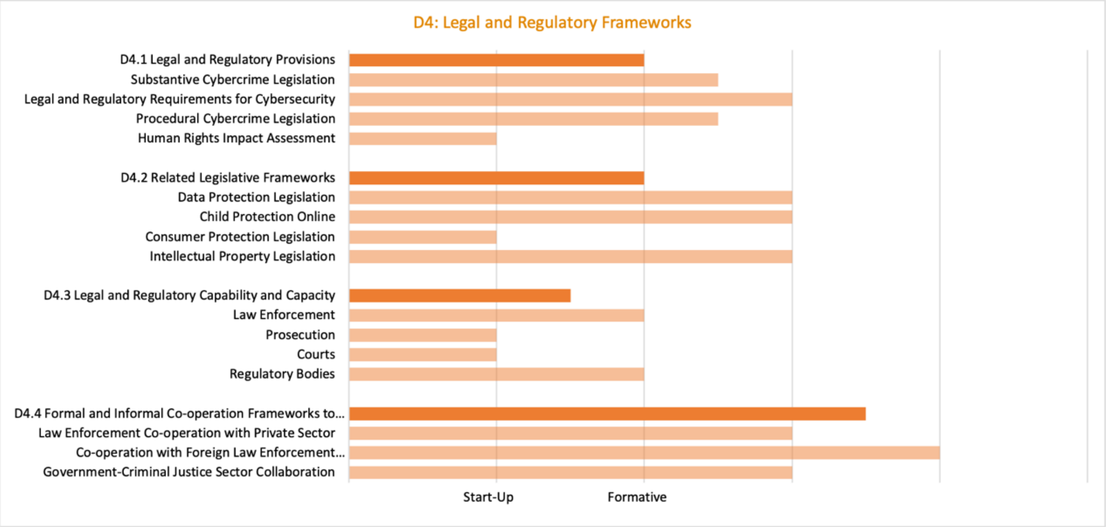
R3.4.4 Develop initiatives to identify the types of cybersecurity research projects that are of the most national and strategic need and consider providing support such projects.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This Dimension examines the government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation and related legislation. The capacity to enforce such laws is examined through law enforcement, prosecution, regulatory bodies and court capacities. Moreover, this Dimension observes issues such as formal and informal co-operation frameworks to combat cybercrime.


Dimension 4
Legal and Regulatory Frameworks
D4.1 Legal and Regulatory Provisions
Legal and Regulatory Requirements for Cybersecurity
Procedural Cybercrime Legislation
Substantive Cybercrime Legislation
Human Rights Impact Assessment
D4.2 Related Legislative Frameworks
Data Protection Legislation
Child Protection Online
Consumer Protection Legislation
Intellectual Property Legislation
D4.3 Legal and Regulatory Capability and Capacity
Regulatory Bodies
Law Enforcement
Courts
Prosecution
D4.4 Formal and Informal Co-operation Frameworks to Combat Cybercrime
Government-Criminal Justice Sector Collaboration
Co-operation with Foreign Law Enforcement Counterparts
Law Enforcement Co-operation with Private Sector

OVERVIEW OF RESULTS



D 4.1 LEGAL AND REGULATORY PROVISIONS

This Factor addresses various legislation and regulatory provisions relating to cybersecurity, including legal and regulatory requirements, substantive and procedural cybercrime legislation, and human rights impact assessment.

Stage: **Start-up to Established**

Substantive Cybercrime Legislation:

The *Criminal Code 2015* legislates substantive cybercrime provisions related to the confidentiality, integrity and availability of computer data and systems under articles 26.1 and 26.2. Established provisions within these articles include illegal access; data interference; system interference; misuse of devices and illegal interception. The law has established strict liability for illegal attacks on information systems, information networks, integrated state information networks, and critical information infrastructure containing state-classified information. In the past responsibility for investigating these crimes rested solely with the Police. However, with changes in the law, GIA is now mandated to investigate incidents involving attacks on state networks, CII organisations and matters related to state secrets.

The *Criminal Code 2015* also includes provisions for 'computer-related offences' within articles that criminalize related fraud and forgery offences more broadly. For example, in relation to computer-related forgery, article 23.2 criminalizes 'Making and Using Forged Documents', including 'non-physical' documents. The article explicitly mentions documents that inauthentically attribute the right to own, use or dispose of wealth. In relation to computer-related fraud, article 17.3 of Chapter 17 'Crimes Against Property Rights' criminalizes misleading others by using documents, items or electronic devices. Furthermore, article 18.7 of Chapter 18 'Economic Crimes' criminalizes the 'Preparation and use of counterfeit currencies, securities and settlement instruments', including through electronic cards or other means of payment, and falsified financial documents. Similarly, article 18.18 criminalizes computer-related fraud committed by operators and payment services providers towards Mongolia's 'National Payment System'.[67] Finally, while not explicitly defined in relation to the digital environment, the *Criminal Code 2015* also includes several content related offences that may apply to online activities. These include article 13.12 'illegal stalking', article 13.14 'spreading false information' and article 14.1 'discrimination'.

Each cybercrime offence established under Mongolian law includes the necessary measures to ensure that these offences are punishable by effective, proportionate and dissuasive sanctions. Sanctions include both financial penalties and the deprivation of liberty that are adjustable in proportion to the severity and nature of the crime. The enforcement the *Criminal Code 2015* and the cybercrime provisions within it are supported by the *Law on Prevention of Crimes and Violations 2019* which establishes measures that may be taken by authorities to eliminate the causes and conditions of specific crimes and violations. It was noted by some focus group participants that they believe prosecuted cybercrime cases typically only result in a small fine for the criminal. In practice the severity of cybercrime punishments are dependent on several contextual factors and the accuracy of these claims are unverified; however, it is notable that there was a common sentiment felt by some participants that criminal punishments may not be successfully dissuading cybercriminals.

Desktop research and focus groups discussions for this review failed to identify substantive provisions within Mongolian law that cover 'attempting and aiding or abetting' or suitably establish corporate liability in relation cybercrimes (i.e. ensuring that legal persons can be held liable for cybercrime offences committed for their benefit). For this reason, it may be determined that the country does not have measures in place to exceed minimal substantive cybercrime baselines outlined in international treaties. There is also a lack of evidence to suggest that the country has sought to adapt its substantive cybercrime legislation to take into account threats from emerging technologies such as artificial intelligence, machine learning or quantum computing.

At the time of review, Mongolia has not ratified regional or international instruments on cybercrime; however, the country is seeking to take steps to implement best practice legal measures from international instruments such as the Budapest Convention. Focus group discussions revealed a committee was established in 2023 with the mandate of preparing Mongolia to accede to the Budapest Convention. This committee is under the administration of the Vice minister of Justice and includes representatives from the law enforcement community and MDDIC.

Legal and Regulatory Requirements for Cybersecurity:

The *Law on Cyber Security 2021* has established comprehensive cybersecurity requirements for critical infrastructure operators and other specified stakeholders. In force since 2022, the law requires the legal persons stipulated in articles 16, 17, and 19 to comply with the *General Procedure on Cybersecurity*, conduct periodic cyber security risk assessments, and undertake

[67] Established by the *Law on National Payments System 2017*, the 'National Payment System' is an integrated payment system overseen by the Mongolian Central Bank that facilitates the transfer of electronic funds between participating entities in Mongolia. (Source: https://www.mongolbank.mn/en/p/1301)

information security audits. Articles 7, 8 and 9 of the law outline the specific requirements for these activities. Relevant criminal and civil liabilities for the law are stipulated in the *Criminal Code 2015*, *Law on Prevention of Crimes and Violations 2019*, *Law on Civil Service 2017*, and *Labor Law 1999*.

Particularly in relation to Critical Information Infrastructure (CII) operators, Article 19 of the *Law on Cybersecurity 2021* defines what entities are classified as CII and what requirements they must follow. These include, but are not limited to: adopting internal procedures for ensuring cybersecurity; adopting and implementing an action plan in case of cyber-attacks and violations; having an officer or unit in charge with ensuring cyber security; having a risk assessment conducted every year; having an information security audit conducted every two years; and notifying the relevant centre against cyber-attacks and violations immediately of failure of normal, uninterrupted operations of the information systems and infrastructure due to cyber-attacks and violations.

Additional obligations for all legal persons defined in the *Law on Cybersecurity 2021*, including CII, are specified in the *General Procedure on Cyber Security*. These range from requirements for organising cybersecurity management, to protecting against and detecting cyber-attacks and violations, through to recovering information systems and networks. In creating the procedure, MDDIC sought to align its contents with international standards, including NIST and ISO. MDDIC has also designed the procedure to allow entities to build upon it using their choice of additional regulations. Article 1.3 states that “in the case of overlapping of regulatory requirements, international standards, regulations and procedures requiring highest degree of compliance shall prevail.” Therefore, it functions as a baseline national standard for entities within its scope, not a ceiling. MDDIC has conducted a series of trainings events with CII to help explain the new laws and requirements.

The decision to enable CIIs to select their own international standards has received a mixed reaction by stakeholders, according to focus group discussions. Some are comfortable doing so and happy to not have been prescribed a specific standard by government, while others have advocated for a more consistent approach and criticised the government for being unable to provide clearer directions. One of the challenges to the lighter approach that the government has taken is the lack of international standards that have been translated into the local context and language. This has made it difficult for entities who wish to elevate their security standards, and build upon the requirements of the baseline procedure, to do so in practice. The NCS identifies the localisation of international standards as a national goal; however, desktop research and focus group discussions did not identify any immediate plans for overcoming this issue. See Factor 5.1 for more details.

One of the principal objectives and subsequent benefits of the *Law on Cybersecurity 2021* was to provide a formalised system of cyber governance. The law established different mandates of governing entities responsible for cybersecurity within Mongolia, including the Cyber Security Council, the state central administrative agency in charge of digital development and communications (MDDIC), Government Intelligence Agency (GIA), state security organizations of the armed forced, and the National Police Agency. Chapter 4 of the law, ‘Combating Cyber Attacks and Violations’, further defines the scope and responsibilities of the three national centres against cyber-attacks and violations (CSIRTs): the National Centre, Public Centre and Armed Forces Centre. This has defined a clear ‘Cyber Security System’ that focus group participants stated was a welcome advancement compared to the previous governance structure.

Whereas the law and accompanying general procedure have undoubtedly facilitated several advancements in Mongolia's legislative and governance environments, there are ongoing challenges in in the implementation and adoption of the updated legislative and regulatory framework that are undermining further national progress. In practice, focus group discussions identified that many organisations subject to the *Law on Cybersecurity 2021* and *General Procedure on Cyber Security* have not implemented the requirements of either, and do not have the capacity to do so in the short to medium term. This is partially due to their recent nature, with the law taking effecting in 2022 and the procedure due to take effect in the second half of 2025. However, it is equally to do with limited capacity of entities in the scope of the law to execute their responsibilities, and the capacity of the broader Mongolian cybersecurity industry to service their needs.

Budget and human resourcing are two significant barriers that are preventing the successful operationalisation of the framework, as outlined in Factor 3.2 and 3.3. The introduction of the law and the procedure has significantly increased the demand for cybersecurity professionals in an already limited local skills market. The annual cybersecurity risk assessment, bi-annual information security audit, and requirement to have 'an office or unit of staff charged with ensuring cybersecurity', amongst other obligations, were referenced by CII representatives as burdensome and even infeasible due to broadscale human resourcing and budgetary constraints. Their expressed inability to hire the right staff to fulfil their new duties or engage a suitable assessor/auditor to review their performance, has left various stakeholders frustrated and critical of the framework. What staff they do have are often overworked and struggle to fulfil their extensive list of responsibilities, with many experiencing burn out. This is particularly the case within the public sector, which is seen by many existing and prospective employees as an unattractive employer because of the limited renumeration opportunities and extensive workloads. This reflects an imbalance globally between public and private enterprise's ability or willingness to fund and hire skilled cybersecurity labour, and invest in cybersecurity more generally. Furthermore, the absence of a cybersecurity budget line, or suitable funding for technical equipment and scarce cybersecurity skilled labour, compounds these issues.

These challenges extend beyond just CII and government departments, and also apply to stakeholders within the cybersecurity industry who are foundational in the successful implementation of the framework. According to focus group discussions, many of the various organisations in the private sector who are registered to undertake the annual and bi-annual risk assessment and information security audits under the *Law on Cybersecurity 2021* do not have the functioning ability to fulfil these responsibilities due to human resource limitation. While the government does have verification protocols in place to confirm that organisations do have the resourced and expertise to conduct assessments and audits when they register, the dynamic nature of the cyber labour market means that the validity of verifications are not guaranteed to last long.

Mongolia is therefore faced with a multifaceted, complex set of challenges to operationalising the new cybersecurity legislative and regulatory framework. The introduction of the framework has driven up demand for already scarce cyber-skilled human resources, and at every level of implementation the short supply of adequate human resources is undermining stakeholders' ability to execute their responsibilities under the framework. This is being compounded by accompanying financial resource constraints that are prohibiting public sector competition with private enterprises for these resources, and stakeholders' inability to This is not to say that the framework is unworkable or must be immediately revised. Indeed, the progress that the government and wider cyber ecosystem has made in a period of short time in the legislative and regulatory environment is substantial; particularly given their own staffing and budgetary challenges. Rather it is to highlight that proactive measures should be taken now to ensure that implementation challenges are strategically addressed to avoid long-term stagnation and disillusionment in this area. With its strong foundations in place, Mongolia must continue to refine and improve this framework to make it more efficient and effective.

Outside the *Law on Cyber Security 2021*, there are additional components of the digital domain that are subject to regulations through Mongolia's broader legislative framework. The *Law on Electronic Signatures 2021* has established a legal framework for the use of digital signatures, electronic seals and electronic documents that also includes security requirements for this technology. Articles 6 and 7 cover the use of public and private keys for encryption and decryption of signatures and seals, while article 8 includes requirements concerning the digital signature tools used in this process. Article 9 comprises time registration provisions for establishing data integrity. Chapter 7 of the law outlines a regulatory system for the public key infrastructure that enables the technology which delegates dual regulatory responsibility to MDDIC and the Communications Regulatory Commission. Under this framework, these entities must develop documents outlining security controls for creating, using and storing public key certificates; developing public key infrastructure standards and monitor the implementation of these rules.

Furthermore, the *Law on Communications 2001* regulates Telecommunications and Internet Service Providers. The law gives the 'Communications Regulatory Commission' (CRC) responsibility for creating conditions for efficient and fair competition in the communications market. Article 9 of the law outlines the regulatory commissions powers, which include certifying network equipment and developing communications standards, amongst other things. However, specific provisions related to security, or mandating the communications regulator to regulate digital security amongst telecommunications or internet service providers, are not included in the law. Desktop research and focus group discussions failed to identify any standards issued by the CRC related to information or digital security. In spite of this, as classified CII, communications providers are mandated to follow the requirements stipulated in the *Law on Cybersecurity* 2021. The CRC has issued content related regulations that instruct service providers to prohibit several classifications of content on their platforms. These restrictions cover pornography, terrorism, religion base cruelty, public disorder copyright and more.[68]

The Central Bank of Mongolia has regulatory responsibly for Mongolia's banking sector and the 'National Payment System' under the *Law on Central Bank 1996* and the *Law on National Payment System of Mongolia 2017*. The Financial Regulatory Commission (FRC) has regulatory responsibility for non-banking financial service providers in Mongolia such as insurers, professionals participating in the securities market, real estate agents and more under the

[68] General Regulatory Conditions and Requirements of the Digital Content Service (2011)

Law on the Legal Status of Financial Regulatory Commission 2005. It was suggested in focus group discussions that both of these entities had released information security regulations that required entities within their scope to follow particular international standards; however, desktop research failed to produce any evidence to support this. To conduct their business internationally financial institutions in Mongolia have to comply with international security standards. Those compliance requirements have produced institutionalized information security competencies within the financial sector, which was well recognized in focus group discussions, and documented online.[69]

Procedural Cybercrime Legislation:

Mongolia's has comprehensive cybercrime criminal procedure law provided under the *Law on Criminal Procedure 2017*, including evidentiary and investigation requirements. Specifically, the procedural law comprises provisions for the collection and utilization of electronic evidence (Chapter 16, 21 and 22), the expedited preservation of stored computer data and traffic data (Chapter 22), production orders (Chapter 22), search and seizure of stored computer data (Chapter 24), real time collection of traffic data (Chapter 26), and the interception of content data (Chapter 26). Furthermore, the law includes jurisdiction provisions in Chapter 2 that may extend jurisdictional scope over criminal activities which outside of the state in certain circumstances (Article 2.1.2). In such circumstances jurisdiction must be determined by the Chief Justice of the Criminal Chamber. Focus group discussions and desktop researched failed to determine if these provisions have been applied to cybercrime offences established under the *Criminal Code 2015*. In some of the provisions outlined above, their application to the digital environment and subsequently cybercrime is inferred in the legislation, but not concretely established. There is a lack of jurisprudence available to the research team to confirm or deny their application.

Chapter 42 of the *Law on Criminal Procedure 2017* outlines the legal requirements for cross-border investigations and information exchanges, including in cybercrime cases. It states that such international cooperation can occur within the bounds of bilateral and mutual legal assistance treaties (MLATs) or other international agreements or treaties. While Mongolia is not part of any international cybercrime agreements or treaties, it does have MLATs in place with several countries that may therefore facilitate international cybercrime cooperation at a procedural level. Under the *Criminal Code 2015* article 1.7 foreign citizens who commit crimes in Mongolia may be extradited if there are sufficient grounds to assure their safety in their destination country. Under the same article Mongolian citizens cannot themselves be extradited to a foreign country for criminal investigation, which is consistent with article 15 of the Constitution of Mongolia.

Human Rights Impact Assessment:

Chapter 2 of the Constitution of Mongolia includes provisions for human rights and freedoms in the country. Under article 16, Mongolian Citizens are explicitly afforded the right to freedom of expression, thought, information, liberty, safety, privacy, religion, and political association, amongst other things. Furthermore, *Law on the National Human Rights Commission of Mongolia 2020* established a 'National Human Rights Protection System' that

[69] https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.swift.com/swift-resource/251951/download&ved=2ahUKEwiV2JXm-4iKAxVUU0EAHdJQCaAQFnoECBcQAQ&usg=AOvVaw1r1TSBQQJFldru_toTJheo

is designed to protect and promote human rights in Mongolia. Part of the commission's responsibilities under Chapter 2 of the law include to put forward opinions on draft laws and administrative decisions conformity with human rights obligations, and monitoring government organisations compliance with human rights responsibilities. The commission has the ability to issue compulsory recommendations to eliminate causes and conditions for violations of human rights and freedoms. Mongolia is also a member of the United Nations and signatory of the Universal Declaration of Human Rights, and in 1974 ratified the International Covenant on Civil and Political Rights. The country is therefore aligned with international human rights standards. Under the NCS Mongolia also has a strategic aim of improving the legal framework for the protection of human rights in the cyber environment.

However, despite this robust legislative and strategic human rights framework, focus groups and desktop research failed to determine if a human rights impact assessment has been conducted in relation to Mongolia's cybersecurity or cybercrime legislation. There is also no indication from the research that relevant human rights experts have been consulted in the development of legislation and regulations. Furthermore, well document instances of political control of information, including the penalisation and imprisonment of journalists, indicate that the government does not always respect the rights of citizens established in the country's human rights framework.[70]

In the cyber domain, concerns for the human rights implication's of the *Law on Cybersecurity 2021* were raised in focus group discussions with public and private sector CII. Stakeholders expresses reservations over the degree of oversight the law gave different leading agencies over the data they managed and if this was advisable. Article 22 of the law tasks the Public Centre (Public CSIRT/CC) with detecting and responding to cyber-attacks in public CII, conducting research into attacks and sharing information with the National Centre (National CSIRT). The National Centre was given similar powers and responsibilities under Article 21 of the law. These powers made several stakeholders uncomfortable on digital privacy grounds. These concerns were fuelled by the national history with authoritarian communist rule which has fostered a deep distrust amongst some members of society towards government institutions. It is necessary to note that Mongolia has strong data protection laws, discussed in Factor 4.2; however, the laws apply to data controllers (ISPs) and do not apply the cybersecurity law.

[70] https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/mongolia/

D 4.2 RELATED LEGISLATIVE FRAMEWORKS

This Factor addresses the legislative frameworks related to cybersecurity including data protection, child protection, consumer protection, and intellectual property.

Stage: Start-up to Established

Data Protection Legislation:

The *Law on Personal Data Protection 2021* regulates the collection, processing, use and security of personal data. It applies to all legal and non-legal entities and individuals who wish to engage in any of the aforementioned activities, and applies equally to all activities that are assisted with the use of hardware or software. Article 4 of the law establishes two data categories, 'personal data' and 'sensitive information'. Personal data refers to "data and other information which can directly or indirectly identify or potentially identify a person." Sensitive information refers to "information in regard to a person's race, ethnic origin, religion," etc.

Articles 6 and 7 outline when and how state or private entities, or individuals, may collect data, and when they can use it. Under all circumstances they must have the consent of the data subject before they can collect, store or use their data for the available purposes specified in law. Requirements for consent are outlined in Article 8 of the law and include such provisions as listing the specific data that will be collected, informing the subject how long the data will be held and what it will be used for, how to withdraw their consent, and so on.

The *Law on Personal Data Protection 2021* also assigns the lead agencies responsible for implementing and monitoring compliance with the law. Under article 25, the 'State Central Administrative Body in charge of Digital Development and Communication', MDDDIC at this time, has been assigned responsibility for implementing the law, raising public awareness of its provisions, and providing assistance to data controllers who are subject to its requirements. Furthermore, article 20.2 states that MDDIC must approve technological and security procedures for the collection, processing and use of data, including instructions for assessments and storage technology requirements. The first general procedure of this kind, the 'Information Security Requirement' procedure, was adopted by MDDIC in 2023.[71] These requirement outlines several principals that data controllers must follow, along with a series of technological security requirements and server processing requirements.[72]

Separately, under article 24, the National Human Rights Commission is granted the powers and responsibility to oversee compliance with the law. In addition to also providing public awareness, receiving and responding to complaints from data subjects, and providing

[71] https://www.dlapiperdataprotection.com/index.html?t=security&c=MN
[72] https://www.dlapiperdataprotection.com/index.html?t=security&c=MN

recommendations to organizations on their data management, with the purpose of preventing violations of human rights and freedoms. Overall, the law centralizes maintaining and protecting the human rights and freedoms of Mongolian citizens within the broader data management framework, with article 5 including general provisions for respecting and protecting human rights.

Furthermore, article 5 of the law includes general security provisions for data protection that entities must follow, including ensuring the ongoing security of data and maintaining its accuracy and integrity. In more detail, under 'Information Security Measures' in article 20, data controllers are required to develop procedures for securing the data they hold and conduct assessments to ensure they are upholding the integrity, confidentiality and accessibility of information systems used for data collection, processing and use. Within this article, data controllers are also required to formulate an action plan in the case they lose data, which must include details of how they will inform data subjects and the relevant authorities. Finally, article 23 enables data controllers to utilize electronic data processing technology but requires that they conduct assessments on its use in cases where there is regular processing of sensitive information, or where the system has decision-making functions which could potentially affect the rights, freedoms and interests of data subjects. The National Human Rights Commission may provide recommendations to these assessments which the data controller must then follow.

Within the legislative framework, data subjects may make complaints to the appropriate authorities if they have concerns over the use of their data. Depending on their nature, violations of the law are dealt with through the *Law on Prevention of Crimes and Violations 2019*, *Law on Civil Service 2017*, *Labor Law 1999* and the *Criminal Code 2015.*

Child Protection Online:

The *Criminal Code 2015* legislates substantive criminal offences against children and includes provisions that apply such protections to the online environment. These are particularly connected to offences related to child pornography and other associated activities. Article 16.8 of the law, 'promoting and inciting adultery to children', criminalises the promoting of obscenity and child molestation to children, and offering children prostitution and sexual intercourse. Article 16.9 criminalises 'promoting of obscenity involving children'; including the preparation, sale, distribution or storage of photos, video recordings or other materials that promote obscenity involving children. The article was amended in 2021 to include a provision that extends this criminalisation to the 'cyber environment'.

Furthermore, the *Law on Children Protection 2016* legislates additional child protections in press and media, and digital environments. According to article 8 of the law, particular legal persons such as parents, schools and state bodies are obliged to protect children from games, books, art, information, advertisements, and other digital environments that may have negative impact on their health, upbringing and maturity. Overall, the legislative framework provides substantive legal protections for children in Mongolia that are in line with international standards for best practice, such as the Budapest Convention. Desktop research and focus group discussions did not find evidence to suggest that the effectiveness of online child protection law is regularly assessed or that the country is seeking to adapt child protection laws to take account of emerging technologies and their use.

Consumer Protection Legislation:

The *Civil Code 2002* outlines the general conditions of sales within consumer contracts in articles 200-2002. Article 42.1 of the code authorise electronic transactions in Mongolia. The *Law on the Consumer Right Protections 2003* governs relations concerning consumer right protections arising from the sale and purchases of good and products, performance of works and the provisions of services. The Department of Consumer Protection of Authority for Fair Competition and Consumer Protection (AFCCP) enforce the law.

The law provides provisions for the protection of consumers from deceptive and fraudulent business practices; however, it does not include specific provisions indicating that it is applicable to the online environment. Additionally, desktop research and focus group discussion found no evidence that Mongolia's consumer protection legislation is being adapted to reflect its application to the online environment. The *Criminal Code 2015* does criminalise digital fraud, as discussed in Factor 4.1; however, there do not appear to be any specific existing provisions governing typical forms of electronic business malpractices, such as spam messaging.

Intellectual Property Legislation:

The *Law on Copyright 2021* established Mongolia's intellectual property legislative framework. Its scope includes scientific, literary and artistic works. The application of the legislative framework to the digital environment is well established. Article 52 of the law requires ISPs, website owners, telecommunications service providers, broadcasting corporations and other entities to prevent copyright infringements on their networks. It stipulates that they must have established methods of receiving and resolving complaints concerning violations of copyright. In the case that any of the entities listed in article 52 of the law fail to fulfil their duties to uphold copyright protections then they may be punished by the 'State Inspector of Intellectual Property.' This entity is understood to be the Intellectual Property Office of Mongolia.

In addition to these provisions, article 53 of the *Law on Copyright 2021* prohibits the deliberate breaking, deactivating, destroying, or damaging the technology protection used by the copyright holder to prevent the unauthorized use of their work. It is also illegal to manufacture, import or promote technology and equipment for commercial purposes that may be used to conduct the previous offence. The *Criminal Code 2015* further prohibits the violations of trademark owners, copyright or related rights under articles 18.16 and 18.17. At the international level, Mongolia is a member of the World Intellectual Property Organization (WIPO) and has signed the WIPO Internet Treaties, has acceded to the Bern Convention for the Protection of Literary and Artistic Works, is a member of the World Trade Organization and party to its Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and is aligned with the provisions in article 10 (offences related to infringements of copyright and related rights) of the Budapest Convention.[73]

The application of intellectual property protections to the online environment is therefore firmly established under law. Mongolia is aligned with international standards and best practices. Research suggests that there is evidence that Mongolia does face difficulties in

[73] https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-11/Mongolia_Digital_Readiness_Assessment.pdf

operationalizing this framework.[74] Desktop research and focus group discussions did not find evidence to suggest that the effectiveness of intellectual property legislation is regularly assessed or that the country is seeking to adapt intellectual property legislation to take account of emerging technologies and their use.

[74] https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-11/Mongolia_Digital_Readiness_Assessment.pdf

D 4.3 LEGAL AND REGULATORY CAPABILITY AND CAPACITY

Stage: **Start-up to Formative**

This Factor studies the capacity of law enforcement to investigate cybercrime, the prosecution's capacity to present cybercrime and electronic evidence cases, and the court's capacity to preside over cybercrime cases and those involving electronic evidence. Finally, this Factor reviews the existence of cross-sector regulatory bodies to oversee compliance with specific cybersecurity regulations.

Mongolia's law enforcement, prosecution and courts have some limited foundational capacity to investigate cybercrime cases; however, gaps in technical, human and financial resources are preventing broader institutional capacities from developing. International supported trainings on cybercrime cases and digital evidence techniques occur sporadically within Mongolia, and have been doing so for several years. This includes programs with the UNODC[75], JICA[76], the International Organisation on Migration (IOM)[77] and more. These programs have, by and large, focused on law enforcement professionals; no equivalent for prosecutors or judges could be identified. In addition to these international training opportunities, the National Police Agency, through the National Police Academy (within the University of Internal Affairs), has a two-year training program on cybercrime for its trainee officers.[78] The 'Cyber Safety Professional Program', one of several specialisation training streams offered by the academy, provides legal and professional knowledge to conduct cybercrime investigations.

A limited amount of available evidence suggests that this training infrastructure has enabled Mongolia law enforcement to conduct several successful cybercrime investigations. These include a joint global operation with INTERPOL in 2024 that helped to take down 22,000 malicious IP addresses around the world, leading to 21 house searches locally[79]; and a 2019 operation that saw the National Police Agency arrest 800 Chinese citizens and confiscate hundreds of computers and mobile phones under suspicion of cybercrime offences. Details of the outcomes of these cases are not publicly available and consequently it is difficult to determine if law enforcement and the prosecution had the capacity to successfully convict the suspected criminals, or if the judiciary was able to effectively process these cases.

Crime data from the 'Mongolia Statistics Yearbook 2023' indicates that there is at least limited legal capacity within Mongolian to take cybercrime cases through to completion. Subsequently it can be affirmed that the prosecution and judiciary have some capacity to prosecute, process and convict cybercrime cases. In 2023, 388 cybercrime cases were registered with the National Police Agency, an increase of 49.8% compared to the year before. From these cases there were 155 offenders registered.[80] Data from the Instance Court of

[75] https://www.unodc.org/roseap/en/2024/05/mongolia-translational-organized-crime/story.html

[76] https://cybilportal.org/projects/countermeasures-against-cybercrime/

[77] https://www.iom.int/project/strengthening-mongolias-cyber-crime-investigations-human-trafficking

[78] https://drive.google.com/drive/folders/1RETJak8qmhR4XP1Ngeqnr1rpCX-S1KkK

[79]https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-cyber-operation-takes-down-22-000-malicious-IP-addresses

[80] P. 371 of National Statistics Report

Mongolia shows that 14 cybercrime cases were resolved in the court in 2023, up from 4 in 2022.[81] Taken together, these statistics demonstrate that the capacity of the judiciary and prosecution to process cybercrime cases is growing year-on-year, but does not yet appear to be at a level sufficient to match the growing number of register cybercrimes. This is consistent with the data collected in focus groups discussions, which indicated that the prosecution and judiciary lacked institutional capacity to manage cybercrime cases efficiently and effectively.

Despite these limited competencies, and an established cybercrime training framework for law enforcement professional, large gaps remain in the overall capacity of legal stakeholders to investigate, prosecute and process cybercrimes in Mongolia. Each institution is experiencing technical, human resource and budgetary deficiencies that are limiting the further enhancement of capacities. With respect to human resources, the prosecution and judiciary have no formalised training programs in place that are designed to help alleviate this challenge. Within law enforcement, despite their efforts to provide training opportunities and fill their cyber-skills gap, a high rotation of staff has undermined their ability to build human capacity. Fierce competition with other sectors for skilled cybersecurity professionals has undercut the retention rate of trained professionals who are easily attracted to better paying roles elsewhere in the labour market. Rather than having an established cadre of skilled cybercrime professionals there is a patchwork of knowledgeable individuals.

This prevailing skills shortage is not an issue that can be solved in isolation with a narrow focus on increased and improved training. Within focus group discussions, law enforcement salaries were criticised as being uncompetitive, with too many bureaucratic restrictions, to retrain or attract the skilled staff needed to conduct skilled cyber roles. Addressing the structural financial constraints that exist within the public sector that apply to law enforcement, such as restrictive and inflexible salary bands, and training the number of people needed to fill the existing national cyber skills gaps will require a multistakeholder approach that is discussed further in Factor 3.3. To ensure the efficient and effective operation of the legal system overall; law enforcement, the prosecution and judiciary must work together to institutionalise cybercrime training practices and overcome these structural financial constraints.

Technological limitations are another factor that are currently undermining the capacity of legal stakeholders to manage cybercrime cases. Focus group discussions indicated that legal institutions are not being sufficiently provided with the technological equipment needed to enable sophisticated cybercrime investigation, prosecution and processing. For example, the *Law on Cybersecurity 2021* stipulates that the National Police Agency must operate a digital laboratory for investigating and fighting cyber-attacks. According to focus groups discussions this has not been established to date. Furthermore, it was reported in focus group discussions that's despite consecutive requests by law enforcement officials for budgetary support for technological equipment to protect the sensitive data they manage, they have never received such support.

From a regulatory standpoint, there are also mixed capability and capacity competencies between regulators. More established regulators, such as the Central Bank and Financial Regulatory Commission have the skills and resources to oversee cybersecurity compliance in their sectors. However, the capacity of the regulators responsible for overseeing the *Law on Cybersecurity 2021* and the accompanying *General Procedure on Cyber Security* remain quite

[81] National statistics report (confirm page no.)

limited. The entities responsible for overseeing compliance with the regulatory baseline established by the *General Procedure on Cybersecurity*, are the National CSIRT, the Public CSIRT/CC, and the risk assessment and audit agencies registered with MDDIC. Focus group discussions presented a variation of capacities between each of these groups. The National CSIRT has was reported to have successfully fulfilled a number of its regulatory responsibilities, such as undertaking risk assessments of public CII, as had some of the registered audit and risk assessment agencies. However, it was reported that other audit and risk assent agencies did not have the necessary competencies requires to fulfil their responsibilities (Factor 4.1).

Overall, there was a strong perception amongst focus group participants that the regulators themselves needed further training to improve their capacity to implement regulations. Frustrations at the regulators limited understanding of what they expected from regulated entities were common, although there was debate over the validity of these claims and which entities were less or more informed. Regardless, a limited understanding of the regulatory framework by various stakeholders appears to be generating challenges in operationalising the regulatory framework. Limited financial resources were cited as equal challenges in this area.

D 4.4 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This Factor addresses the existence and function of formal and informal mechanisms that enable co-operation between domestic actors and across borders to deter and combat cybercrime.

Stage: **Established to Strategic**

Information is regularly exchanged informally between law enforcement stakeholders and the private sector in support of cybercrime investigations. Discussions with the National Police Agency indicated that they have full confidence in the reliability of their relationships with banking, internet and communications providers, and that they frequently exchange information with these providers. Law enforcement expressed concerns that sometimes it takes longer for them to receive information than they would like from the private sector, but that they generally recognize that each stakeholder is working to the best of their ability. To help overcome these challenges and expedite information exchanges between law enforcement and key members of the private sector, the National Police Agency are in the process of developing a secure information exchange system. This formal cooperation mechanism is being developed in coordination with the Communications Regulatory Committee. As a membership-based organization with large representation in the private sector, MNCERT/CC also facilitates the exchange of information between the private sector and law enforcement. As the longest running emergency response team in the country, MNCERT/CC was well recognized in its capability to do so by a wide variety of stakeholders in focus group discussions.

Law enforcement cooperation with the private sector is supported through legislation, including the *Law on Criminal Procedure 2017* (Chapter 22) and *Law on Cybersecurity 2021* (article 15.1.1 and 15.1.2). Greater domestic and international cybercrime collaboration and information exchange is also supported through the NCS which includes the goals of improving information exchange 'infrastructure' between parties, 'activating cooperation' between cybersecurity centres and creating 'conditions for information exchange with international, regional and professional organizations in the field of combating cybercrime.'

At an international level, Mongolia has the legislative framework to support Mutual Legal Assistance Treaties (MLATs), as outlined in Factor 4.1. The application of these treaties to cybercrime cases was confirmed with discussions with law enforcement. The National Police Agency reported a significant improvement in recent years in their ability to collaborate with international partners. Mechanisms such as the G7 24/7 network and their relationship with INTERPOL were cited as helping in this regard. Successful cross border investigations with international counterparts and local law enforcement authorities have recently been reported in the media.[82] The National Police Agency is also part of a joint committee with MDDIC and

[82] https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-cyber-operation-takes-down-22-000-malicious-IP-addresses

others to investigate Mongolia potentially joining the Budapest Convention on Cybercrime, an action that they believe will further assistant them lift their cross-border cybercrime capabilities.

The Mongolia government works closely with the criminal justice sector to develop cybercrime laws and strategies, conduct training exercises and exchange information on cybercrimes. The Public CSIRT/CC, which sits beneath MDDIC, and the National CSIRT, which sits beneath GIA, both provide formal mechanisms for collaboration and information exchange between the Mongolian government and the law enforcement on cybercrime. The capacity of the National and Public CSIRT to detect cyber-attacks and share information with relevant parties is growing and still in need of improvement. However, through them, there is a formal structure in place which can facilitate the regular exchange of information on cybercrime issues between government and law enforcement stakeholders. MNCERT/CC, the Public CSIRT/CC and the National CSIRT are all members of FIRST. The Public CSIRT/CC and National CSIRT are also members of APCERT. Each of these relationships further enhances the networks of these organizations and increases their access to knowledge pertinent to cybercrime cases that be of use to Mongolia law enforcement agencies.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations are provided to Mongolia. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

LEGAL AND REGULATORY PROVISIONS

R4.1.1 Under the leadership of the committee guiding Mongolia's actions to join the Budapest Convention on Cybercrime, undertake a full review of Mongolian substantial and procedural criminal legislation to identify and fill any gaps that may exist between the convention and the Mongolian Legal framework.

R4.1.2 In coordination with **R4.1.1**, take the necessary steps to engage the Council of Europe and be formally invited and then accepted into the Budapest Convention on Cybercrime.

R4.1.3 In coordination with **R4.1.1**, undertake a review of Mongolia's existing substantial and procedural criminal legislation and, if necessary, update existing laws to account for new and emerging technologies, such as AI and quantum computing.

R4.1.4 Task the state central administrative agency in charge of digital development and communications to translating the most up-to-date leading international standards into Mongolian, factoring in considerations of the local context. Align with **R5.1.2**.

R4.1.5 Invest in a coordinated national cybersecurity skills development program for cyber policy and legal expertise that will enable all entities within the scope of the cyber legislative framework to execute their legal and regulatory obligations. Align with **R3.3.1**.

R4.1.6 As stated in the **R1.3.1**, as the *Law on Cybersecurity 2021* comes into force, monitor the progress of CII operator compliance with regulatory standards and incident and vulnerability disclosure, and the effectiveness of the planned processes to evaluate compliance.

R4.1.7 As stated in **R1.3.4**, convene discussions with CII stakeholders to obtain feedback on the Law, noting that some stakeholders in the CMM expressed concerns about the clarity and level of detail of the Law. It will be important to ensure that stakeholders have a clear understanding of the requirements, in order to ensure smooth implementation of the Law.

R4.1.8 Under the leadership of the Cyber Security Council, identify and prioritise the acquisition of skilled cybersecurity professionals for indispensable cybersecurity positions that the broader legislative framework is reliant on. This may include key positions in MDDIC and GIA that are essential for facilitating the successful adoption and operationalisation of the legislation.

R4.1.9 Expand existing training programs on the *Law on Cybersecurity 2021* and accompanying *General Procedure on Cybersecurity* to lift CII awareness of their obligations under the law reduce existing ambiguities about the new cybersecurity legislative and regulatory framework. Align with **R1.3.4**.

R4.1.10 Conduct a Human Rights Impact Assessment of existing substantial and procedural cybercrime legislation to ensure the digital human rights of Mongolian citizens are protected.

RELATED LEGISLATIVE FRAMEWORKS

R4.2.1 Undertake a review of existing consumer protection legislation and take the necessary steps to ensure its comprehensive application to the online environment.

LEGAL AND REGULATORY CAPABILITY AND CAPACITY

R4.3.1 Develop a harmonised national cybersecurity skills development program for law enforcement, prosecution and judicial stakeholders that will improve their collective capacity to investigate, prosecute and process cybercrime and cybersecurity cases. The program should be strategically tailored to address existing capacity gaps and incorporate the available expertise and support of international partners.

R4.3.2 Invest in establishing the 'analytical laboratory' mandated in article 15.1.4 of the Law on Cybersecurity 2021 to ensure that law enforcement have the facilities to efficiently and effectively conduct sophisticated cybercrime investigations.

R4.3.3 Establish incentives to improve retention rates of law enforcement personnel and improve the resilience of the workforce. In coordination with recommendations made in **R3.3.4**, consideration could be given to developing more structured and transparent career pathways for cybersecurity staff that include embedded training opportunities and salary advancements.

R4.3.4 In coordination with **R4.1.5**, invest in improving the capacity of regulators connected to the cybersecurity legislative framework to effectively monitor the implementation.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

R4.4.1 Continue to build the capabilities and relationships between law enforcement agencies, government agencies, the private sector and international law enforcement counterparts to facilitate ongoing information exchanges between these groups. This may include empowering law enforcement stakeholders through participation in national and regional events, facilitating greater participation in training and networking opportunities, initiating public-private partnerships, and agreeing memorandums of understanding.

R4.4.2 Support ongoing efforts between law enforcement and private sector stakeholders to establish a secure information exchange mechanism for cybercrime investigations. Take steps to ensure that any mechanisms that are developed respect the digital human rights of Mongolian citizens. In coordination with **R1.2.4**, consider establishing similar information exchange mechanisms between law enforcement and other key stakeholders in the cybersecurity ecosystem (i.e. CSIRTs).

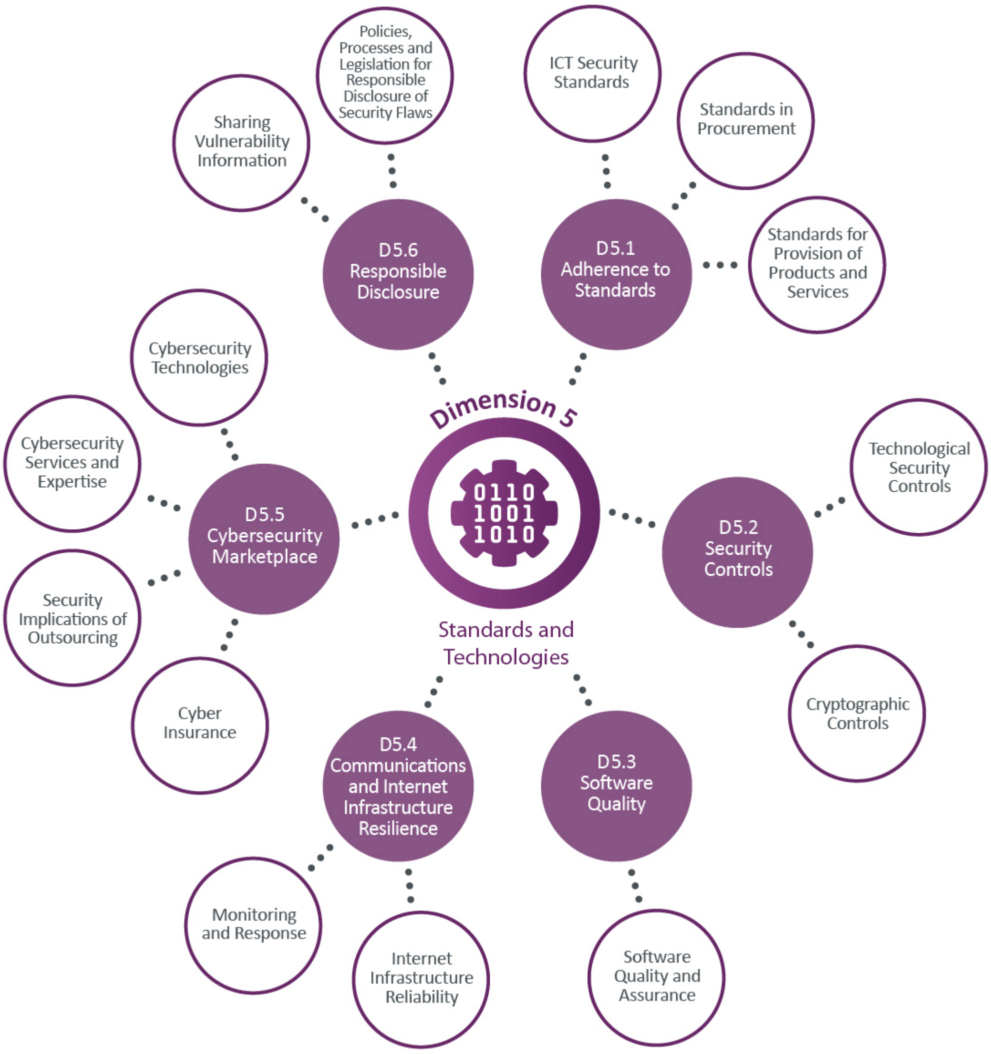
R4.4.3 Review the existing ways that members of the public, businesses and organisations report cybersecurity incidents to law enforcement and consider how the data collected from these reports may be used to obtain a better idea of the nature and volume of specific cybercrimes. Incorporate the lessons learned from this review into future strategic decision making processes.

R4.4.4 Review the collaborative relationship between government actors, law enforcement, prosecutors, judges, the private sector and international counterparts to assess how improvements could be made to enhance the effectiveness of these relationships.

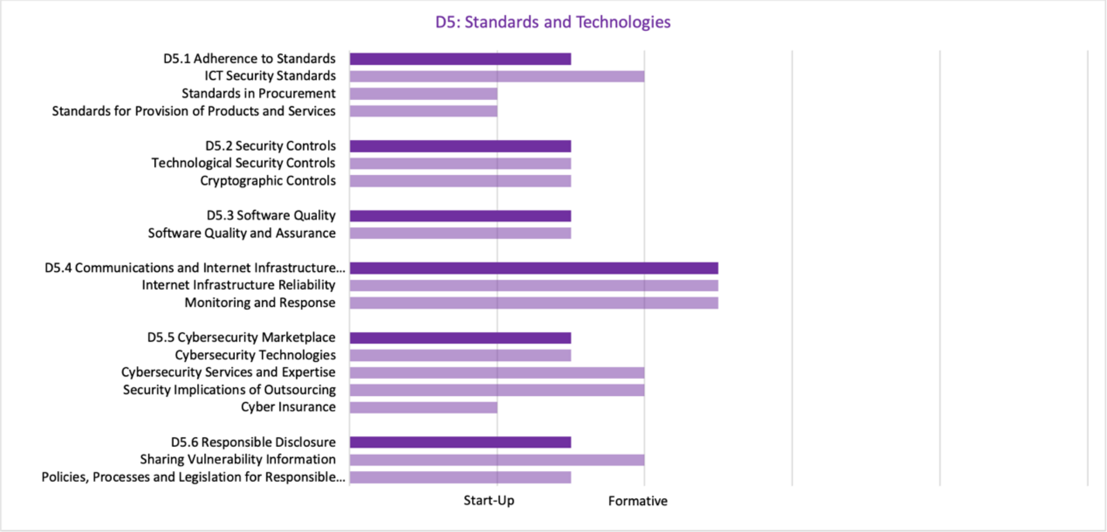
DIMENSION 5

STANDARDS AND TECHNOLOGIES

This Dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The Dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.


Dimension 5
0110
1001
1010
Standards and Technologies
D5.1 Adherence to Standards
ICT Security Standards
Standards in Procurement
Standards for Provision of Products and Services
D5.2 Security Controls
Technological Security Controls
Cryptographic Controls
D5.3 Software Quality
Software Quality and Assurance
D5.4 Communications and Internet Infrastructure Resilience
Monitoring and Response
Internet Infrastructure Reliability
D5.5 Cybersecurity Marketplace
Cybersecurity Technologies
Cybersecurity Services and Expertise
Security Implications of Outsourcing
Cyber Insurance
D5.6 Responsible Disclosure
Sharing Vulnerability Information
Policies, Processes and Legislation for Responsible Disclosure of Security Flaws

OVERVIEW OF RESULTS



D 5.1 ADHERENCE TO STANDARDS

This Factor reviews the government's capacity to promote, assess implementation of, and monitor compliance with international cybersecurity standards and good practices.

Stage: Start-up to Formative

There has been identification of international cybersecurity standards and localisation of these standards to the Mongolian environment, for Mongolian organisations to use. In particular, the following standards were officially approved:[83]

- MNS ISO/IEC 17799:2007 is the Mongolian national adaptation of the international standard ISO/IEC 17799, which is a precursor to ISO/IEC 27002
- MNS ISO/IEC 13335-1:2009 is the Mongolian national standard based on the ISO/IEC 13335-1:2004, which provides guidelines for managing information and communication technology (ICT) security
- MNS 5969:2009, a Mongolian national standard titled "Information Technology—Security Techniques—Information Security Risk Management", which provides organisations with practical recommendations for identifying, evaluating, and managing information security risks
- Five standards from the ISO/IEC 27000 set

Some participants expressed the view that these localised standards need to be updated, as international standards have been since. This aligns with the NCS, which contains an Action to "localise international standards for ensuring cyber security, approve and implement rules and regulations in accordance with them".

[83] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Mongolia.pdf

The extent to which these standards are followed varies. There is some evidence of growing implementation of the use of international standards and good practices within some sectors, but a lack of detailed data makes it challenging to assess the extent of adherence to standards across sectors.

The Finance sector is the only sector in which organisations were mandated by the regulator to adopt cybersecurity standards prior to the Cybersecurity Law. Participants from the Finance sector reported the requirement to comply with the International Organization for Standardization (ISO) 27001 standard to obtain a banking licence, as well as others dependent on the nature of their operation, such as the Payment Card Industry Data Security Standard (PCI DSS) for card operations.[84]

In other sectors, there is some adherence to standards. This varies dependent on the maturity of the organisations, and also driven by their requirements to operate internationally. Participants from large telecommunications companies reported having adhered to ISO 27001 for over a decade. Participants from government agencies and public sector transportation organisations such reported seeking to be certified against ISO 27001. The Mongolian National Authority for Accreditation expanded its scope to include ISO 27001 certification in December 2024, and there are reportedly some local accreditation centres capable of providing ISO 27001 certification, improving accessibility to Mongolian organisations who previously were obliged to work with international organisations to obtain this accreditation.

According to the Cybersecurity Law (see further detail in D1.3.2), the CI organisations are obliged to adopt internationally recognised cybersecurity standards, as well as the “General Procedures on Cyber Security”, which were drafted by MDDIC to align with the ISO 27001 and NIST 8000 cybersecurity standards, to incorporate the minimum common ground. The requirements of the Law are not yet fully implemented; CI organisations will reportedly need to comply by the Law’s audit deadline (August 2025). The level of cybersecurity standards adoption currently varies across the CI. There was some debate about whether the standards that need to be adhered to by the CI should be mandated more specifically, rather than leaving the choice to the organisations (see D1.3 for further detail).

Government entities and technology providers are also obliged by the Cybersecurity Law to adopt internal procedures to ensure cybersecurity. MDDIC reported a view that most government agencies are trying to follow to General Procedures to create their own internal cybersecurity policies. MDDIC has run some activities to promote the General Procedures and train organisations on how to implement them. It was reported that the sessions run so far have reached over 600 government staff.

The view was expressed that while many larger CI organisations are likely to have the resources to adopt these cybersecurity standards, smaller organisations might face challenges. It may also be beneficial to consider how to develop standards or best-practice guidance that can be used by small and medium-sized organisations with resource limitations.

There is no evidence of measurement of the use of cybersecurity standards by organisations outside of the CI and government. However, it would be beneficial to consider how to

[84] https://www.mongolbank.mn/file/beb8a25d6bc7b7f718f2a9a71f0c2b39/files/2018_03_06_A57.pdf

promote the use of cybersecurity standards and the General Procedures to other private organisations, and implement schemes to measure uptake.

There is no guidance given by the government on the standards to be used by Mongolian organisations to guide procurement processes (including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services). While some more mature organisations are using standards to guide these processes, implementation is ad-hoc and uncoordinated. Participants expressed the view that there is a need for guidance on procurement standards that specify the metrics that need to be checked by organisations when procuring products.

For CI and government organisations, there is some progress towards testing the security of products. The NCS contains an Action to "*establish a laboratory for checking and certifying information, communication equipment and information systems used in organizations with state and critical information infrastructure*". Reportedly, this laboratory has been established and is tasked with validating the cybersecurity of hardware and software used by CI organisations. However, the laboratory currently lacks a formal mechanism for proactively identifying and assessing new hardware and software acquisitions by CI organisations. In practice, therefore, it is not yet consistently conducting cybersecurity assessments.

Participants noted that the procurement law for government organisations may be creating some issues for procuring secure and compatible products, since the main concept of the law is reportedly to procure the lowest-price products. It may be important to explore with stakeholders perceived issues relating to this law.

Similarly, while an increasing number of technology providers are following standards for software development (see D5.3), there is no evidence of government promotion or monitoring of the use of standards by technology and service providers. The Cybersecurity Law does place requirements on technology providers to adopt various processes to secure their organisation, but it is not clear from the Law that this includes following security standards in the development of their products. It would be valuable to explore how to promote and monitor the use of standards by technology and service providers in the software development processes, hardware quality assurance, and provision of managed services and cloud services.

D 5.2 SECURITY CONTROLS

This Factor reviews evidence regarding the deployment of security controls by users and public and private sectors, and whether the technological cybersecurity control set is based on established cybersecurity frameworks.

Stage: Start-up to Formative

Security controls are being deployed by some public and private organisations in Mongolia, but this is not consistent across sectors. The existing regulation of the adoption of cybersecurity standards for organisations in the Finance sector also means that these organisations are implementing technological and cryptographic security controls accordingly.

Currently, the deployment of technological and cryptographic security controls varies across organisations in Mongolia dependent on their resources and cybersecurity awareness, and their adherence to cybersecurity standards (see D5.1).

As described in Section 5.1, the audit deadlines (August 2025) of the Cybersecurity Law means that CI organisations will be obliged to adopt internal cybersecurity procedures and adhere to cybersecurity standards, and their consequent implementation of technological and cryptographic controls will be audited. It is therefore anticipated that the deployment of controls across CI organisations will become more consistent once the regulation comes into force.

It was reported that research by academic institutions and private cybersecurity companies has found that the application of security controls in certain sectors in lacking. The healthcare sector was cited as a particular example.

Representatives from government cited concerns about the prevalence of successful attacks, for example, including APT attacks, against government organisations. For government organisations, issues with budget were reported to be creating challenges for the implementation of cybersecurity controls. There is a need to explore how to ensure that government organisations are allocated sufficient budget by the Ministry of Finance to implement controls. Some participants suggested that creating a separate cybersecurity heading under which organisations can request budget might be beneficial.

Some organisations outside of government also reported concerns about their ability to obtain budget to implement controls. The view was expressed that the leadership of organisations are not consistently prioritising cybersecurity in their allocation of resources. It may be beneficial to explore running initiatives to raise the cybersecurity awareness of organisational leadership.

A number of government organisations host their systems at the National Data Centre (NDC), and are connected to the government information network run by the Information Security Department of the GIA, which is used to exchange information between connected government organisations. It was reported that the Information Security Department of the GIA implements network-level security controls on the government information network such as network intrusion-detection systems (NIDS), but does not implement host-level security controls on the systems of the government organisations. The implementation of these controls is the responsibility of the individual government organisations. There are cases, as is detailed in D1.2, where the NDC supports the response to cybersecurity incidents affecting the government systems that it hosts. The NDC is also hosting the websites and services of government organisations, but is not responsible for managing their security.

The NDC also hosts the government cloud and manages its security. This hosts the email systems of some government organisations, and is a computing resource available to government organisations. In terms of the implementation of security controls at the NDC, it reported implementing security controls in line with ISO 27001 and being certified against this standard, and running a physically separated data-recovery centre.

Ensuring consistent implementation of security controls in government is particularly important as government services are becoming increasingly digitised: the e-Mongolia website is making increasing numbers of government services available online to citizens and organisations.[85] While there are strong security features included, such as the ability for citizens to access these e-government systems using a unified digital identity (a single sign-on system run by NDC), weaknesses in the security of the host government institutions may be creating risk. The suggestion was made that a platform or conference for government representatives to share knowledge and best practices might be beneficial.

It was noted that in many public and private organisations, a shortage of employees with cybersecurity expertise is creating challenges for the implementation of controls. Many large organisations reported having only a single person responsible for IT, and no specific cybersecurity personnel. The Cybersecurity Law obliges CI organisations to have cybersecurity personnel or a cybersecurity unit in place once it comes into force. There are concerns about how this will be achieved, given a perceived shortage of skilled workforce in the nation and, for public-sector organisations, how skilled professionals can be attracted with relatively low public-sector salaries. Some organisations reported having already experienced challenges in trying to hire cybersecurity personnel to comply with the Law

Some participants from private organisations reported the use of cryptographic controls and data-handling processes to protect data at rest. This is not consistent across organisations; for example, some concerns were noted that sensitive files are sometimes transferred over social media by government employees, and that data at rest including personally identifiable information (PII) is not always properly protected with the right levels of privileged access. Some government ministries reported ongoing work with GIA to improve their data-transmission and storage policies.

A few approaches to improving this situation were suggested, including the development of a unified government policy prohibiting the use of social platforms to transfer information (noting that some individual organisations already have such policies in place), and the development of a secure, controlled chat platform for government staff. It was noted that there is currently no coordination of the cryptographic requirements for interactions between organisations, and that this can create challenges for interaction. It may be beneficial to

[85] https://e-mongolia.mn/home

explore how to guide or standardise the cryptographic requirements for the exchange of information between organisations in the private sector and government.

There is some provision of security services by Internet Service Providers (ISPs). Participants reported that the regulation from the Communications Regulatory Commission requires ISPs to provide DDoS protection to clients; however, it was noted that not all ISPs have the resources to comply with this requirement. Some ISPs reported offering a range of security services to clients, including firewalls and vulnerability scanning.

There is a public-key infrastructure (PKI) in Mongolia: the root Certification Authority (CA) is owned by MDDIC and hosted and maintained by NDC, and there three CAs in total in the country. The digital certificates that these CAs provide to Mongolian organisations are owned by foreign root CAs (they are not created locally). The NCS includes an Activity to create conditions for the international use of national digital signatures, by updating the current infrastructure and having it included in the internationally accredited list.

The NDC reported that digital certificates are requested by some more mature clients to implement digital signatures and encryption of website data via the Transport Layer Security (TLS) protocol, but that not all client organisations are requesting digital certificates. The Law on Digital Signature (2021) establishes the legal conditions for the use of digital signatures in the country.

In relation to implementing security features in their websites and services, some organisations noted the challenge of low levels of public cybersecurity awareness leading to pushback against security features implemented which are perceived to be inconvenient to use. This is creating a trade-off for organisations between keeping customers happy with the business, and security. Cybersecurity service providers reported that this is leading to some client organisations refraining from implementing certain security features in their customer-facing services.

D 5.3 SOFTWARE QUALITY

This Factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this Factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the critical nature of services.

Stage: Start-up to Formative

Software quality requirements are recognised by some organisations. Some participants from private CI organisations described the security reviews and testing processes conducted for software procured, and having mature processes in place for software updates and maintenance.

This level of maturity in ensuring the use of high-quality and secure software is not consistent across organisations. Concerns were that some organisations lack the resources or awareness to purchase licenses for software and cybersecurity technologies, leading to the use of unlicensed or pirated software. MDDIC supported this observation, noting that a recent audit conducted of seven different government agencies highlighted that one of the key problems was with the use of unlicensed software. It was stated the use of unlicensed software is contrary to the new General Procedures to be followed by CI organisations and other government organisations, but that these have not yet been fully implemented or audited.

Participants reported that, until recently, there was little use of security standards in the development of software by local companies, but that recently progress is being made in the adoption of secure-design processes and security reviews. This change was attributed in part to the increase cybersecurity-service providers, and the increasing profitability of local software companies, meaning that cybersecurity services can be procured to ensure software security.

The view was expressed that software purchased from abroad tends to be better standardised and more reliable. Participants from private organisations noted that in using domestic software, there is a greater need to conduct their own security reviews and testing to rely on it, since it is usually not standardised, and its security depends on the quality of the company developing it. No catalogue for assured software platforms exists to guide organisations in their procurement.

Processes to ensure the procurement of secure software by government organisations may be lacking. It was noted that, when there is government tender for software development, the initial specifications do not currently specify cybersecurity requirements, with cybersecurity requirements sometimes being added by MDDIC later in the project, creating additional workload. Greater coordination between ministries on the specification of cybersecurity requirements in government tenders might be beneficial.

D 5.4 COMMUNICATIONS AND INTERNET INFRASTRUCTURE RESILIENCE

This Factor addresses the existence of reliable Internet services and infrastructure in the country, as well as rigorous security processes across private and public sectors. Also, this Factor reviews the control that the government might have on its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Formative to Established

Reliable Internet services were reported to be widely available and used in Mongolia. In 2024 there were an estimated 2.9 million Internet users in Mongolia, a significant proportion of which uses mobile broadband technologies.[86] The infrastructure is composed of terrestrial fibre-optic cables which are connected to the global Internet through Russia (and onward to European countries) and China (and onward to the United States). There is also a large domestic backbone of fibre-optic cables spanning all 21 provinces of the nation.[87] For remote parts of the country, this Internet provision is supplemented by satellite connections, and improvements to connectivity and lower latency have reportedly been made recently, including through Starlink satellite connections. It was noted that there may remain some connectivity issues in remote areas.

The Internet infrastructure is formally managed by the Communications Regulatory Commission, which issues licenses to Internet Service Providers (ISPs) and regulates ISPs, for example requiring a specified minimum percentage of ISPs' traffic to be routed through alternative paths to improve redundancy. There is also a requirement for ISPs to provide DDoS protection to clients; however, it was noted that not all ISPs have the resources to comply with this requirement, and it was not clear that the requirement is being enforced consistently.

In relation to redundancy, there is also a Mongolian Internet Exchange Point (IXP) hosted by the NDC, which facilitates traffic exchange amongst ISPs, and which participants stated provides good redundancy in the case of failure at an ISP. It was also reported that discussions are ongoing between ISPs and the Communications Regulatory Commission to create further IXPs.

Participants expressed the view that Internet services are generally trusted in Mongolia for conducting e-commerce and electronic business transactions. There is no evidence of metrics having been collected on this; measuring the status would facilitate the identification of any issues.

Telecommunications organisations have been identified as CII according to the Cybersecurity Law ("*Operators in communications, and information technology that are natural monopolies and exercise a dominant position*). This creates several requirements, including the obligation to conduct risk assessments and audits, implement internal cybersecurity procedures and standards, and develop incident-response plans. Prior to the Law, the sector was unregulated

[86] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf

[87]https://www.apt.int/sites/default/files/2019/09/ADF-16_INP-17_Mongolia_Development_of_National_Broadband_infrastructure_in_Mongolia_and_its_usage.pdf

regarding the implementation of mechanisms for protecting against, detecting and responding to cybersecurity incidents, and the requirements of the Law have not yet been fully implemented since the audit deadline has not yet passed. Their implementation therefore varies across telecommunications organisations.

D 5.5 CYBERSECURITY MARKETPLACE

This Factor addresses the availability and development of competitive cybersecurity technologies, cyber-insurance products, cybersecurity services and expertise, and the security implications of outsourcing.

Stage: Start-up to Formative

Participants reported that there are no cybersecurity products produced by Mongolian companies. Cybersecurity products used in Mongolia are supplied by foreign vendors, with some resellers operating in Mongolia. There is an intention to increase the production of local products, noting the potential implications of reliance on foreign technologies: the NCS contains an Action "*to support the national production, innovation, research and analysis of information and communication equipment, software, and electronics, and to reduce technological dependence*". Some participants noted the potential dangers of procuring technologies from certain countries, given the state-sponsored APT attacks that have been suffered by some Mongolian organisations, and it may be important to discuss this issue further.

Participants stated that the Mongolian cybersecurity-services industry has expanded rapidly in the past three years. Companies are offering services including cybersecurity standards-compliance audits, penetration testing, implementation of Information Security Management Systems (ISMS). Some organisations from the CI reported experience in using local cybersecurity consultancy services. A limited number of service providers possess international professional certifications.

Some participants from government expressed the view that, while it is growing, the supply of cybersecurity-service providers is still not sufficient to meet demand, particularly to fulfil requirements of the Cybersecurity Law. The accompanying procedures to the Cybersecurity Law state that service providers auditing the CI must have a full-time employee certified by a professional association or standards organisation. According to MDDIC, who conducted an evaluation of the eligible service providers, only a small number currently meet this requirement.

There are legal constraints specifying the service providers that can provide audit and risk assessment to the CI organisations (that they must be authorised by MDDIC according to the Cybersecurity Law, and that any risk assessments conducted by foreign entities must be approved by the GIA). There was no evidence of guidance available to assist other organisations with the selection of service providers. Some participants reported that not all organisations currently possess the cybersecurity expertise to fully understand their own requirements, and may therefore risk procuring low-quality services.

There is no national body to accredit service providers. Establishing an accreditation body could encourage accreditation and assist organisations in selecting service providers.

Some organisations are outsourcing their IT. For some government organisations, it is mandated that their systems are hosted in the government cloud or directly by the National Data Centre. Other organisations, including some government agencies, may choose to host at the NDC, and some choose to outsource to other third-party cloud services, including international services.

The capability of organisations to conduct risk assessments to determine how to mitigate the risks of outsourcing varies according to their maturity. There is some legislation aimed at addressing the risks: a requirement in the Data Protection Law that personally identifiable information of Mongolian citizens must be physically hosted within the nation's borders. The NDC reported a further plan to develop a policy jointly with MDDIC to clearly outline the different information-classification levels and where they can be hosted.

Some organisations have developed business-continuity processes to help address the risks of failure in outsourced services. This again varies depending on the cybersecurity maturity of organisations. In the case of CI organisations, these processes will need to develop soon, since the Cybersecurity Law requires CI organisations to "*have an action plan in place for ensuring the normal, uninterrupted operation of the information system and infrastructure, and for restoration thereof in case of damages and interruptions*". The increase in the number of organisations that have established business-continuity processes is a metric that will be used to assess the progress of the NCS (see D1.1 for details on the progress monitoring of the NCS).

Cyber-insurance offerings are emerging in Mongolia. The National CSIRT website contains an introduction to cyber-insurance, and guidance on choosing the right cyber-insurance product.[88] Participants were not aware of any local companies offering cyber-insurance products, but stated that such products are made available to Mongolian companies by some international providers. Uptake of cyber-insurance products is in the early stages, and the participants consulted during the CMM did not have any experience in using cyber-insurance products.

[88] https://ncsirt.gov.mn/a/26

D 5.6 RESPONSIBLE DISCLOSURE

This Factor explores the establishment of a responsible disclosure framework for the receipt and dissemination of vulnerability information across sectors, and whether there is sufficient capacity to continuously review and update this framework.

Stage: Start-up to Formative

Within some sectors, mechanisms exist for operators to share threat and vulnerability information with each other. It was reported that there is a banking Information Sharing and Analysis Centre (ISAC), through which financial institutions share threat and vulnerability information. Some organisations in the financial sector also reported subscribing to international cyber-threat intelligence (CTI) feeds. Members of MNCERT/CC, primarily composed of large private-sector organisations, also share information between themselves.

The view was expressed that it would be beneficial to have information-sharing mechanisms that can be used by a wider range of organisations in Mongolia, to facilitate the exchange of threat and vulnerability information. This aligns with Objective 5 of the NCS, which includes an Action "*to develop basic infrastructure for exchanging information about cyber-attacks and violations*". The approach taken might be sector-based sharing mechanisms, or mechanisms for use more broadly. Some participants expressed that view that there may be a culture of reluctance to share cybersecurity information with other organisations, and it is important to consider whether initiatives to increase awareness of the benefits of information exchange would be beneficial alongside any mechanisms developed.

There is some culture of ethical hacking and vulnerability disclosure in Mongolia. There have been some successful bug-bounty programmes conducted. MNCERT/CC has run events with the Mongolian Banking Association to raise awareness amongst financial organisations of how to conduct bug-bounty programmes. The Haruul Zangi Cyber Drill, organised annually by MNCERT/CC, was also highlighted as an event that includes an ethical hacking tournament.

This has reportedly led to instances of companies openly inviting researchers to search for vulnerabilities in their systems. Some organisations have a responsible-disclosure policy in place, detailing the processes to be followed in the case that a vulnerability in their software or website is discovered, including disclosure deadlines and scheduled resolutions. It was noted that this is dependent on the culture and maturity of the organisation, however, and is primarily seen in private financial institutions. The current lack of consistently implemented responsible-disclosure mechanisms may hinder the effective reporting and remediation of security vulnerabilities by organisations, including government institutions.

There is no legislation in place to protect researchers disclosing vulnerabilities responsibly. Some participants who participate in ethical hacking communities in Mongolia reported a reluctance to approach companies due to fear of repercussions. The view was expressed that it would be beneficial to develop the mechanisms to protect researchers, noting that these mechanisms need to be suited to the Mongolian context. Participants reported instances of hackers taking down websites then asking for payment to fix it, and noted that there needs to be a clear distinction between this type of criminal activity, and any legislation brought in to protect those disclosing vulnerabilities responsibly.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity Standards and Technologies, the following set of recommendations are provided to Mongolia. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1.1 Expand the nationally agreed baseline of standards to include:

- cybersecurity standards and best practices guiding procurement processes (including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services);
- cybersecurity standards for the provision of products and services (including software development, hardware-quality assurance, provision of managed services and cloud security).

R5.1.2 Explore whether there is a need to update the current nationally approved set of localised cybersecurity standards in line with more recent developments in international standards.

R5.1.3 Consider issuing guidance to smaller-and-medium sized organisations on how to deploy a more basic level of cybersecurity controls that is achievable with more limited financial and personnel resources. The UK's Cyber Essentials scheme may be a useful example.

R5.1.4 Assign an entity responsibility for measuring the use of cybersecurity standards across the public and private sectors, in particular for organisations outside of the CI and government that will not be covered by the new regulations. Collaboration with academic institutions or research organisations might be beneficial for tracking and analysis.

R5.1.5 Establish government programmes for promoting the adoption of the identified cybersecurity standards, standards in procurement, and standards for the provision of products and services, across organisations in Mongolia. Use insights into adoption (generated through R5.1.4) to promote awareness within groups of organisations with lower levels of adoption.

R5.1.6 Consider whether the current government procurement laws conflict with the procurement of secure products and associated standards in procurement, and resolve any issues identified.

R5.1.7 Ensure that the new laboratory for testing the cybersecurity of hardware and software acquisitions by CI organisations has sufficient capabilities and mechanisms to enable it to conduct timely security assessments consistently for acquisitions of technology by CI.

SECURITY CONTROLS

R5.2.1 Promote the use of cybersecurity standards across public and private organisations in Mongolia, so that the technological and cryptographic cybersecurity control sets used by organisations consistently reflect established cybersecurity frameworks, standards and good practices.

R5.2.2 Explore how to ensure that government organisations are allocated sufficient budget to implement security controls by the Ministry of Finance. It was suggested that creating a separate cybersecurity classification within which organisations can request budget might be beneficial.

R5.2.3 Consider conducting a study to identify successful examples of effective security-control deployments by organisations in Mongolia. These examples could be used to demonstrate the impact and importance of effective security-control adoption.

R5.2.4 Conduct initiatives to raise the cybersecurity awareness of leaders in organisations, to promote the prioritisation of cybersecurity in their allocation of resources.

R5.2.5 Explore how to improve the security with which information is exchanged by government employees, and prevent the exchange of sensitive information via social media. Some approaches were suggested, which it may be beneficial to explore:

- developing a unified government policy prohibiting the use of social platforms to transfer information (noting that some individual government organisations already have such policies in place);
- developing a secure, controlled chat platform for government staff;
- standardising the cryptographic requirements for the exchange of information between organisations in government, and for the exchange of this information to and from organisations in the private sector.

R5.2.6 Consider running platforms or conferences for government employees to share cybersecurity knowledge and best practices.

R5.2.7 Consider how to increase the use of digital certificates by organisations in Mongolia. This might involve running awareness campaigns.

SOFTWARE QUALITY

R5.3.1 Assign a body responsible for gathering evidence of software security and deficiencies, and characterising software applications as to their reliability, usability, performance and security in adherence to international standards and good practices. Consider international engagement to identify suitable best practices and benchmark current capability in this area.

R5.3.2 Use the information gathered in R5.3.4 to issue guidance for all organisations on how to identify secure and reliable software platforms and applications. This may take the form of a catalogue of assured software, or of guidance on how to assess software quality, functional and security requirements.

R5.3.3 Issue guidance for all organisations on software updates and maintenance (including patch-management).

R5.3.4 Develop a framework for measuring the security of software and application of software-maintenance policies across organisations (for example, collecting and analysing statistics).

R5.3.5 Consider conducting a study or consultation to determine the causes of software-procurement issues in government (including the use of unlicensed software) and identify how these issues can be addressed.

R5.3.6 Consider conducting a study or consultation to explore the security of domestic software and how to bridge the reported gap in quality between domestic software and software purchased from abroad. Consider how government support or incentives might foster improvements in local software development practices.

COMMUNICATIONS AND INTERNET INFRASTRUCTURE RESILIENCE

R5.4.1 Monitor the implementation of the requirements of the Cybersecurity Law by ISPs identified as CI, to ensure that these organisations are capable of implementing sufficient controls to mitigate against and respond to cybersecurity incidents.

R5.4.2 Consider how support might be given to smaller ISPs to improve cybersecurity practices, for example through sharing of best practices.

R5.4.2 Establish mechanisms (e.g., surveys) to measure trust in Mongolian Internet services for conducting e-commerce and electronic business transactions. Use the data gathered to identify and resolve any issues. Consider regularly publishing the metrics to promote transparency and accountability.

CYBERSECURITY MARKETPLACES

R5.5.1 Convene stakeholders to consider the security implications of relying on foreign cybersecurity technologies, and consider whether any actions are needed to mitigate potential risks.

R5.5.2 Issue and promote guidance for organisations in Mongolia on how to identify and manage the security implications of reliance on foreign technologies.

R5.5.3 In promoting the growth of the domestic cybersecurity-technology marketplace, ensure that secure development processes are promoted, according to internationally accepted standards. Consider how secure development practices could be incentivised.

R5.5.4 Review the supply and demand for cybersecurity-service providers Mongolian organisations, to ensure that the offering meets the continuously growing demand.

R5.5.5 Assign a body responsible for accrediting cybersecurity service providers.

R5.5.6 Issue guidance to organisations on how to select cybersecurity service providers. This is particularly important for organisations outside of the CI, for whom the choice of service providers for risk assessment and audit is not regulated.

R5.5.7 Develop guidance or training for organisations on how to manage cybersecurity risks when outsourcing services to third-party providers.

R5.5.8 Identify the cyber-insurance needs of organisations in Mongolia through consultations to assess the financial risks for the public and private sectors. Further, consider a study to identify any barriers to the development of insurance solutions. Use these insights to inform and support the development of the cyber-insurance market.

RESPONSIBLE DISCLOSURE

R5.6.1 Conduct initiatives to raise the awareness of public and private organisations of the benefits of responsible disclosure of vulnerabilities (and how it differs from genuine attacks and extortion).

R5.6.2 Promote the development of responsible-disclosure policies, channels and resolution approaches, and bug-bounty programmes amongst a wider range of Mongolian organisations. This should be supported by improved awareness as recommended in **R5.6.1**.

R5.6.3 Consider developing legislation that protects parties disclosing vulnerabilities responsibly and clarifies the conditions under which discovering and reporting vulnerabilities could or should be considered a criminal offence. The Global Forum on Cyber Expertise (GFCE) Global Good Practices on Coordinated Vulnerability Disclosure may be a useful resource for the development of legislation.[89] It may be beneficial to pilot this legislation with ethical-hacker communities to ensure practicality.

R5.6.4 Develop information-sharing mechanisms that can be used by a wider range of organisations in Mongolia to exchange information on threats and vulnerabilities.

R5.6.5 Consider whether initiatives to increase organisations' awareness of the benefits of information exchange would be valuable to encourage the use of any mechanisms developed. Awareness campaigns may need to be supported by a study of the barriers to information sharing perceived by organisations. It may be beneficial to tailor the awareness campaigns to different sectors, to increase participation in sectoral information-sharing mechanisms.

[89] https://thegfce.org/wp-content/uploads/CoordinatedVulnerabilityDisclosure-1-1.pdf

ADDITIONAL REFLECTIONS

The level of stakeholder engagement in the review was good, and the representation and composition of stakeholder groups was, overall, balanced and broad. This enabled the review team to collect comprehensive evidence to support this CMM review.

APPENDICES

METHODOLOGY - MEASURING MATURITY

Deploying the CMM involves data-gathering both through in-country stakeholder consultation (typically over the course of three days) and remotely through desk research. It is designed to produce an evidence-based report which is submitted to the government representatives for the country being studied and will include recommendations to:

- benchmark the maturity of a country's cybersecurity capacity;
- provide a detailed a set of pragmatic actions to contribute towards the advancement of cybersecurity capacity
- identify maturity gaps; and
- identify priorities for investment and future capacity-building.

During the review of a country, specific dimensions are discussed with relevant groups of stakeholders. Each group of stakeholders is asked to respond to one or two dimensions of the CMM, depending on their expertise. For example, Academia, Civil Society and Internet Governance groups would all be invited to discuss both Dimension 2 'Cybersecurity Culture and Society' and Dimension 3 'Building Cybersecurity Knowledge and Capabilities' of the CMM.

Data collection

The Review Team gathers the evidence necessary to identify the stages of maturity across the CMM through desk research, in-depth interviews, and modified-focus group discussions, utilising the CMM Structured Field Coding (SFC) Tool to capture the results. The functions of the Review Team include that of a facilitator to lead the group sessions, and a note-taker.

The CMM uses a **modified focus-group discussion methodology** that elicits data that complements and helps validate in-depth interviews and desk research.[90] As with interviews, focus-group discussions are an interactive methodology with the advantage that during the process of collecting data, diverse viewpoints and conceptions can emerge as participants follow the discussion. Rather than posing questions to specific participants, the researcher(s) facilitate a discussion among the participants, encouraging them to adopt, defend or explain different perspectives.[91] It is this interaction that offers advantages over other methodologies,

[90] Williams, M. (2003). Questionnaire design. In *Making sense of social research* (pp. 104-123). SAGE Publications, Ltd, https://www.doi.org/10.4135/9781849209434; Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. (Ed.), *Successful focus groups: Advancing the state of the art* (pp. 35-50). SAGE Publications, Inc., https://www.doi.org/10.4135/9781483349008; Richard A. Krueger, R. A., & Mary Anne Casey, M. A., (2009) Focus-groups: A Practical Guide for Applied Research. SAGE Publications, London.

[91] Kitzinger, J. (1994). The methodology of focus groups: the importance of interaction between research participants. Sociology of health & illness, 16(1), 103-121. https://doi.org/10.1111/1467-9566.ep11347023;

making it possible for the participants to reach a mutual understanding and to raise everyone's awareness of cybersecurity practices and capacities.[92] During CMM reviews, the Review Team leads the discussion to get onto all the aspects within the relevant dimensions.

To determine the level of cybersecurity capacity maturity, each *Aspect* has a set of indicators corresponding to all five stages of maturity. A consensus method is used to drive the discussions within sessions, for the stakeholders to provide evidence on how many indicators have been implemented by the country and to determine the maturity level of every aspect of the model. During focus-group discussions, researchers use semi-structured questions to keep discussions around relevant indicators. The discussion among stakeholders provides evidence regarding the implementation of indicators. In gauging the maturity level, if there is no evidence for all the indicators being met at a particular stage, then that country has not yet reached that stage of maturity.

Inconsistencies between stakeholders will inevitably occur. Equally, information known to a stakeholder in one sector might not be familiar in other sectors. Accordingly, it will fall to the Review Team to perceive these information gaps and then investigate them.

Desk research and modified focus groups inevitably raise some additional questions and possible inconsistencies. For this reason, and to a gain more in-depth understanding of key and sometimes unique policies and practices, a set of in-depth interviews are also conducted during and on some occasions following the field research.

Data analysis

With the prior consent of participants, all sessions are recorded. Individual responses are treated as confidential with the Chatham House Rule applied in reporting our results.[93] After conducting a country review, the **data collected during consultations** with stakeholders and the notes taken during the sessions are used to find evidence and **define the stages of maturity** for each *Aspect* of the CMM. The CMM report aggregates this information and determines the maturity for each Factor of the CMM.

In the course of the review further desk research is undertaken to bridge any gaps that emerge during the in-country data-collection process and to validate the evidence provided. While drafting the **CMM report**, further desk research and interviews are often necessary to address any missing information, and to validate and verify the results. For example, stakeholders might not always be aware of recent developments in their country, or if the country has signed a particular convention on personal data protection policy. Therefore, official government or ministry websites, annual reports of international organisations, university websites, in-depth interviews, etc. can be used as supplementary sources for information. This type of additional research helps to ensure that the report accurately reflects the Host

Kitzinger, J. (1995). Qualitative research: introducing focus groups. Bmj, 311(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299; Fern, E. F. (1982). The use of Focus Groups for Idea Generation: The Effects of Group Size, Acquaintanceship, and Moderator on Response Quantity and Quality. Journal of Marketing Research, 19(1), 1–13. https://doi.org/10.1177/002224378201900101

[92] Kitzinger, J. (1995). Qualitative research: introducing focus groups. *Bmj*, *311*(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299

[93] https://www.chathamhouse.org/about/chatham-house-rule

Country’s cybersecurity capacity. In each case, the team does not privilege any particular source of information but seeks to reach a consensus on the most valid status of each indicator of the model.

Developing recommendations

For each *Dimension*, **recommendations** are provided for the next steps to be taken for the country to enhance its cybersecurity capacity. If a country’s capacity for a certain *Aspect* is, for example, at a formative stage of maturity then by looking at the CMM the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders. The recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the CMM. The recommendations are provided specifically for each *Factor.*

After a review by the GCSCC Technical Board, the draft report is submitted to the Local Host to secure feedback. If new evidence arises, the draft report is revised and the maturity stages of each *Aspect* and *Factor* in the CMM are updated correspondingly. Once all parties approve the draft report, the Local Host will take the lead in the publication process. Publication approval rests with the Host Country and if this is agreed the Local Host is encouraged to publish it via an official government portal or other outlet.

Data management and ethical considerations

Focus-group discussions are conducted online on Microsoft Teams™ and Zoom™ platforms. *(depending on platforms preferred by each nation)* The discussions are recorded using external recorders to guarantee confidentiality of the data and information collected, and for future transcription for the purpose of writing the CMM report. The recordings remain anonymised. The findings from the desktop study, in-depth interviews, and focus group discussions are consolidated during the analysis.

Global Cyber Security Capacity Centre

Department of Computer Science, University of Oxford

Wolfson Building, Oxford OX1 3QD,

United Kingdom

Tel: +44 (0)1865 287434

Email: cybercapacity@cs.ox.ac.uk

Websites: https://gcscc.ox.ac.uk/home-page#/ www.oxfordmartin.ox.ac.uk/cyber-security