CYBERSECURITY CAPACITY REVIEW

Kyrgyz Republic

Summary of the Findings and Recommendations
of a Report submitted in September 2017

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

KWPF KOREA-WORLD BANK PARTNERSHIP FACILITY

KISA Korea Internet & Security Agency

GCCD Global Cybersecurity Center for Development

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP

LIST OF ABBREVIATIONS

CI	Critical Infrastructure
CIIP	Public Foundation “Civil Initiative on Internet Policy” (*Гражданская инициатива интернет политики*)
CMM	Cybersecurity Capacity Maturity Model
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service
DNS	Domain Name Server
GCSCC	Global Cyber Security Capacity Centre
ICT	Information and Communication Technologies
ISP	Internet Service Provider
MOI	Ministry of Internal Affairs (*Министерство внутренних дел КР*)
NSC	National Statistical Committee of the Kyrgyz Republic (*Национальный статистический комитет Кыргызской Республики*)
SCITC	State Committee on Information Technology and Communications of the Kyrgyz Republic (*Государственный комитет информационных технологий и связи КР*)
SME	Small and medium-sized enterprise
UNDP	United Nations Development Programme
UNICEF	United Nations International Children's Emergency Fund
WB	World Bank

INTRODUCTION

In collaboration with the World Bank, the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') was invited to undertake a review of the maturity of cybersecurity capacity in the Kyrgyz Republic. The review was hosted by the State Committee on Information Technology and Communications of the Kyrgyz Republic (SCITC, *Государственный комитет информационных технологий и связи КР*). The objective of the review was to enable the Kyrgyz Republic to gain an understanding of its cybersecurity capacity in order to develop an investment strategy for the development of the cybersecurity capacity of the country.

Between 4th and 6th April 2017, stakeholders from the following sectors participated in a three-day consultation to review cybersecurity capacity in the Kyrgyz Republic:

- Public sector entities:
    - State Committee on Information Technology and Communications of the Kyrgyz Republic (*Государственный комитет информационных технологий и связи КР*)
    - State Committee for National Security of the Kyrgyz Republic (*Государственный комитет национальной безопасности КР*)
    - State Committee for Defence Affairs of the Kyrgyz Republic (*Государственный комитет по делам обороны КР*)
    - National Statistical Committee of the Kyrgyz Republic (*Национальный статистический комитет КР*)
    - Ministry of Education and Science of the Kyrgyz Republic (*Министерство образования и науки КР*)
    - Ministry of Internal Affairs of the Kyrgyz Republic (*Министерство внутренних дел КР*)
    - Ministry of Finance of the Kyrgyz Republic (*Министерство финансов КР*)
    - Ministry of Foreign Affairs of the Kyrgyz Republic (*Министерство иностранных дел КР*)
    - Ministry of Justice of the Kyrgyz Republic (*Министерство юстиции КР*)
    - Ministry of Health of the Kyrgyz Republic (*Министерство здравоохранения КР*)
    - Ministry of Transport and Roads of the Kyrgyz Republic (*Министерство транспорта и дорог КР*)
    - Centre for Standardisation and Metrology under the Ministry of Economy of the Kyrgyz Republic (*Центр по стандартизации и метрологии при Министерстве экономики КР*)
    - State Service for Combating Economic Crimes under the Government of the Kyrgyz Republic (*Государственная служба по борьбе с экономическими преступлениями при ПКР*)
    - State Financial Intelligence Service under the Government of the Kyrgyz Republic (*Государственная Служба Финансовой Разведки при Правительстве Кыргызской Республики*)
    - State Registration Service under the Government of the Kyrgyz Republic (*Государственная регистрационная служба при Правительстве Кыргызской Республики*)
    - State Customs Service under the Government of the Kyrgyz Republic (*Государственная таможенная служба при Правительстве Кыргызской Республики*)

    - State Tax Service of the Kyrgyz Republic (*Государственная налоговая служба КР*)
    - Local government representatives
- Criminal justice sector
- Defence sector
- Private sector
- Telecommunications companies
- Finance sector
- Academia
- Civil society organisations
- International organisations and embassies

The consultations revolved around the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five dimensions of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cyber Culture and Society*
- *Cybersecurity Education, Training and Skills*
- *Legal and Regulatory Frameworks*
- *Standards, Organisations, and Technologies*

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors consist of aspects and for each aspect there are indicators, which describe steps and actions that once observed define which state of maturity this specific element of aspect is. 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. For more details on the definitions of these, please advise the CMM document (p.5)[1].

Figure 1 below provides an overall representation of the cybersecurity capacity in the Kyrgyz Republic 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] Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

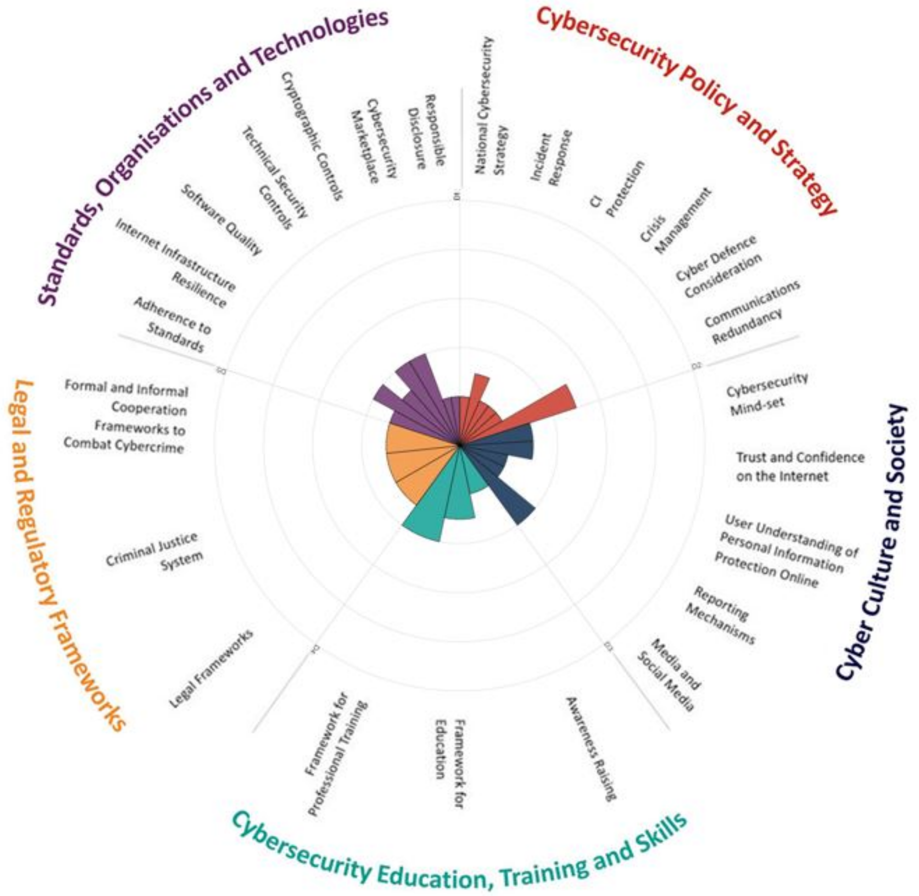

Figure 1: Overall representation of the cybersecurity capacity in the Kyrgyz Republic

CYBERSECURITY POLICY AND STRATEGY

The *Cybersecurity Policy and Strategy* dimension was assessed to range from *start-up* to *formative* stages of maturity. This is because there is no official national cybersecurity strategy document in the Kyrgyz Republic detailing how to establish coordination between key cybersecurity governmental and non-governmental actors. While some departments have altered their structure to establish cybersecurity units, cybersecurity policies are uncoordinated. Similarly, there is no national computer-related incident response organisation that would serve as the coordinating body for the reporting and management of cybersecurity incidents in the country. The State Committee for National Security of the Kyrgyz Republic, however, has a computer incident response unit, set up at the request of the President of the Kyrgyz Republic, A. Atambaev. The unit conducts active practical interaction with CERTs from other countries. Furthermore, private sector organisations are providing ad-hoc incident response internally, in particular in the energy, telecommunications and banking sectors.

The concept of cybersecurity in critical infrastructure (CI) is still in its infancy in the Kyrgyz Republic. While procedures are in place to identify which infrastructures should be prioritised in crisis situations, the notion of critical infrastructure protection does not yet encompass cybersecurity practices. However, risk assessments and business-continuity plans that address general risks, such as blackouts, natural catastrophes, etc., could serve as a first step towards integrating cybersecurity practices into CI business processes.

Cyber defence is not yet a priority in the national cybersecurity posture, with no cyber defence strategy or dedicated unit established in the Kyrgyz Republic. As the cyber defence capacity matures, it will need to be integrated into the country’s current defence posture. In contrast, communications redundancy as a broad concept has been considered in the Kyrgyz Republic, resulting in sectoral efforts to backup data and establish redundant networks in cases of communication breakdown.

CYBER CULTURE AND SOCIETY

National capacity in the *Cyber Culture and Society* dimension was judged to range between *start-up* and *formative* stages. When discussing the cybersecurity mind-set within the Kyrgyz Republic, participants had diverging opinions on how aware government officials, private sector staff and other users are of cyber risks and cybersecurity good practice. Generally, respondents found that cybersecurity has not yet become a priority across the public and private sectors, or among end-users. This lack of awareness or prioritisation was attributed among other things to the comparatively low-security incident rate in the Kyrgyz Republic.

Since the early 2000s, the Kyrgyz government has prioritised investments into the development of e-government services across different departments. As a result, various e-government services have been established. While these services have enabled citizens to access governmental services and information more easily and quickly, the uptake of e-government services is still relatively low and many citizens prefer to access services through the traditional channels. In contrast to the development of e-government services, the national e-commerce sector is still at initial stages in the Kyrgyz Republic.

Despite the adoption of the Law of the Kyrgyz Republic on Personal Data in 2008 (*Закон Кыргызской Республики об информации персонального характера*), respondents considered the understanding of personal information protection online to be at the initial stage of development. Most users are not familiar with protection measures that may be in place to prevent data breaches and no central dedicated mechanism exists to enable citizens to report computer-related or online incidents and crimes in the Kyrgyz Republic.

The role of mass media and social media in cybersecurity reporting and raising awareness in the Kyrgyz Republic is ad-hoc. Media reports appear when major incidents occur, but journalists and bloggers rarely provide information on preventive actions that users can take to protect themselves. On social media platforms, cybersecurity is emerging as an increasingly important issue of discussion. However, information is mostly provided by individuals who are invested in the issues, rather through targeted or large-scale dissemination of information for Internet users.

CYBERSECURITY EDUCATION, TRAINING AND SKILLS

Consultations indicated that the *Cybersecurity Education, Training and Skills* capacity ranged from the *start-up* to *formative* stage. The general lack of cybersecurity awareness in the Kyrgyz Republic was acknowledged across the various stakeholder discussions during the review. Respondents from different stakeholder groups agreed that the government would be best placed to coordinate a national cybersecurity awareness-raising programme, but should do so in conjunction with other stakeholders, in particular from among private sector, civil society, academia and IT experts.

Among executive managers, both in public and private sectors, cybersecurity awareness is very limited, which is one reason why cybersecurity awareness raising is not yet perceived as a priority. Generally, participants raised concerns regarding the fragmented nature of current awareness raising efforts and called for a centralised approach, which builds on existing initiatives and expertise.

The development of cybersecurity educational offerings is at the formative stage in the Kyrgyz Republic, representing one of the most advanced areas of capacity in the country. There are numerous ICT-related Bachelor and Master Degree programmes and specific security-related programmes.

Similarly, to the education sector, training courses are provided in a largely uncoordinated manner by different organisations and vary in depth and coverage. Training programmes are mostly developed in isolation by individual universities or companies, rather than coordinated across organisation and sectors. This leads to a gap between the supply and demand of cybersecurity training programmes.

LEGAL AND REGULATORY FRAMEWORKS

Legal and Regulatory capacities ranged between the *start-up* and the *formative* stages of maturity. The development of a legal framework to regulate the full scope of cybersecurity and cybercrime is still at initial stages in the Kyrgyz Republic. While several laws address some aspects of cybersecurity, such as the protection of personal data or access to governmental information, other key aspects, such as the protection of children online, have not yet been addressed. Moreover, existing legislation is not yet sufficiently enforced due to a lack of commencement orders (i.e., statutory instruments that bring into force all or part of an Act of Parliament[2]) and dedicated enforcement authorities.

Across the criminal justice system, capacities are at initial stages of development. The capacity to investigate cybercrime among law enforcement officers was limited, as there are no regular training courses for law enforcement officers within the country, financial and human resources are insufficient, and specialised knowledge has not yet been built. The capacity of prosecutors and judges to handle and preside over cybercrime cases and cases involving digital evidence was even more limited than within law enforcement. No specialised regular

[2] http://www.parliament.uk/site-information/glossary/commencement-order/

training is available to prosecutors or judges and there are neither specialised prosecutors or judges, nor dedicated structures within the criminal justice system to handle cybercrime cases or cases involving electronic evidence. Insufficient financial and human resources were mentioned by respondents as aggravating factors.

The need to establish informal and formal cooperation mechanisms, both domestically and across borders, has not yet been widely recognised in the Kyrgyz Republic, as cybercrime has only recently emerged as an issue of concern and there have not been many major cases that were brought before the courts. Among the different available cooperation channels, law enforcement cooperation was identified by participants as most advanced, in particular through INTERPOL. Occasionally, cooperation also occurred between Kyrgyz law enforcement and Russian, Kazak or Armenian ISPs

STANDARDS, ORGANISATIONS, AND TECHNOLOGIES

The Kyrgyz capacity in *Standards, Organisations and Technologies* was assessed to range from the *start-up* to the *formative* stages. The Kyrgyz Republic has established a Centre for Standardization and Metrology under the Ministry of Economic Regulation (*Центр по Стандартизации и Метрологии при Министерстве экономики*). Experts from different sectors are invited to advise on standards in general. However, standards regarding cybersecurity or information security are in their infancy. The implementation of standards and the auditing process were deemed by respondents to be problematic due to the lack of a centralised institution responsible for the execution of these tasks.

Respondents raised further concerns regarding the resilience of the Internet infrastructure of the Kyrgyz Republic. Although the country's Internet infrastructure is established and is continuously expanding, Internet penetration is fairly limited, especially in rural areas. Internet downtime and interruptions, often caused by power outages, are frequent.

An inventory of software used in public and private sectors, as well as a catalogue of secure software is absent in the Kyrgyz Republic. The quality and performance of deployed software is an issue of concern and effective monitoring and quality assessment is conducted in an ad-hoc manner in few private institutions. Similarly, the adoption of technical security controls in the country varies across sectors and organisations. Generally, the level of understanding and deployment of security controls in the private sector is reasonable, however, there are no mechanisms in place to assess the effectiveness of these controls. Raising awareness of security controls, promoting their use and assessing their effectiveness among all sectors of the country are important steps in enhancing the capacity within this dimension.

Cryptographic controls is a factor that was deemed to be the most advanced in the Kyrgyz Republic in this dimension. Cryptographic controls are applied to data at rest and, in a small number of cases, to data in transit. Focusing on cyber insurance, no market for cybersecurity technologies and cybercrime insurance products has yet been developed.

Finally, no responsible disclosure policy or framework has been established in the public or private sectors. However, respondents suggested that the private sector is more advanced in this area than the public sector. Focusing on the financial sector, although vulnerabilities are an increasing concern, they are perceived to be confidential, commercially valuable information. Consequently, organisations conceal any detected issues and no information is shared formally with other institutions, either within or across sectors.

ADDITIONAL REFLECTIONS

This was the 16th country review supported directly by the Global Cyber Security Capacity Centre at Oxford. This review is intended to assist the Government of the Kyrgyz Republic to gain insights into the breadth and depth of the country's cybersecurity capacity. While still in the initial stages, the country has begun the process of developing different aspects of cybersecurity capacity across all dimensions. If existing efforts in different organisations and sectors are linked and coordinated, and if a comprehensive legal, strategic and operational framework for national cybersecurity can be established, these can form the foundation for more advanced capacity in the future. The review suggests a number of specific steps by which the Kyrgyz Republic's cybersecurity capacity might achieve greater levels of maturity and might contribute to the development, among other things, of a comprehensive legal and regulatory framework, a national cybersecurity strategy and a national CSIRT.

SUMMARY OF THE RECOMMENDATIONS

CAPACITY FACTORS	STAGE OF MATURITY	RECOMMENDATIONS
D1.1 National Cybersecurity Strategy	**Start-up**	**R1.1** Embark upon developing a national cybersecurity strategy. This document should set out the objectives, roles and responsibilities necessary for achieving a comprehensive and integrated national cybersecurity posture. The strategy should be aligned with national goals and risk priorities to be effective and provide actionable directives. **R1.2** Allocate budget and assign a government agency to oversee the implementation of the national cybersecurity strategy, taking into account existing roles and responsibilities. **R1.3** Identify and involve key stakeholder groups in the development of the national cybersecurity strategy, including international partners. Involve, at minimum, the organisations which participated in the CMM review. **R1.4** Design and disseminate coordinated cybersecurity programmes. Strengthen and promote inter-departmental cooperation in cybersecurity to ensure full implementation of the cybersecurity programmes.
D1.2 Incident Response	**Start-up to Formative**	**R1.5** Identify government bodies and organisations in the private sector that are key to national cybersecurity.

		R1.6 Establish a national CSIRT with clear processes, defined roles and responsibilities. Draft legislation that will allocate mandates to the national CSIRT. **R1.7** Create a mandate for a national cyber incident response detailing when and how organisations should report incidents. Identify and document key incident response processes. **R1.8** Categorise and record national-level cyber incidents in a central registry, possibly hosted by a national CSIRT. **R1.9** Develop coordination and information/cybersecurity threat sharing mechanisms between the private and the public sector, as well as within the cybersecurity community at national, regional and international levels.
D1.3 Critical Infrastructure (CI) Protection	**Start-up**	**R1.10** Develop and disseminate a list of Critical Infrastructure (CI) assets with identified risk-based priorities. **R1.11** Establish a mechanism for regular vulnerability disclosure and information sharing between CI asset owners and the government. Establish regular dialogue between tactical and executive strategic levels regarding cyber risk practices and encourage communication among CI operators. **R1.12** Identify internal and external CI communication strategies with clear points of contact. **R1.13** Establish information protection and risk management procedures and processes within CI, supported by adequate technical security solutions, which inform the development of an incident response plan for cyber incidents. **R1.14** Establish common processes to measure and assess the capability of CI asset owners to detect, identify, respond to and recover from cyber threats.
D1.4 Crisis Management	**Start-up**	**R1.15** Allocate cybersecurity exercise planning to a relevant authority, such as the Ministry of Emergency Situations of the Kyrgyz Republic (*Министерство чрезвычайных ситуаций Кыргызской Республики*). **R1.16** Design a cybersecurity needs assessment of measures and techniques for crisis management. Involvement of key stakeholders and other experts, such as think tanks, academics and civil leaders should be sought. Conduct and test a needs assessment of measures with consideration of a simple exercise scenario. Since several emergency exercises exist, it might be more feasible to integrate cyber elements in one of these scenarios. **R1.17** Identify metrics to evaluate the success of the exercise. Evaluate the exercises and feed the findings back into the decision-making process.
D1.5 Cyber Defence Consideration	**Start-up**	**R1.18** Ensure the development of a cyber defence component in the national security strategy. This component should consider the identified threats to national security that might emerge from cyberspace. **R1.19** Designate an organisation within the army that will be responsible for central command and control of cyber capabilities. Establish cyber operation units in different branches of government and armed forces as appropriate. **R1.20** Develop a communication and coordination framework for cyber defence in response to malicious cyber-attacks on military information systems and critical infrastructure. **R1.21** Assess and determine cyber defence capability requirements, involving public and private sector stakeholders. Conduct continuous reviews of the evolving threat

		landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives.
D1.6 Communications Redundancy	**Formative to Established**	**R1.22** Allocate appropriate resources, not solely to activities such as hardware integration, technology stress testing, personnel training and crisis simulation drills, but also to ensure that redundancy efforts are appropriately communicated to relevant stakeholders. **R1.23** Establish a process, involving all relevant stakeholders, to identify gaps and overlaps in emergency response asset communications and authority links. **R1.24** Link all emergency response assets into a national emergency communication network with isolated but accessible backup systems. **R1.25** Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. Create outreach and education activities of redundant communications protocols tailored to the roles and responsibilities of each organisation in the emergency response plan.
D2.1 Cybersecurity Mind-set	**Start-up to Formative**	**R2.1** Enhance efforts at all levels of government to promote understanding of risks and threats, but also to design systems that enable users across society to more easily embed secure practices into their everyday use of the Internet and online services. **R2.2** Promote the sharing of information on incidents and best practices among public sector entities to promote a proactive cybersecurity mind-set. **R2.3** Promote cross-sectoral cooperation and information sharing among private sector organisations on cybersecurity risks and best practice. **R2.4** Identify vulnerable groups and high-risk behaviour across the public, in particular young people, to inform targeted awareness campaigns, as recommended in R3.1.
D2.2 Trust and Confidence on the Internet	**Start-up to Formative**	**R2.5** Develop campaigns that promote the safe use of online services across the general public, enabling users to critically assess online content. **R2.6** Alongside the promotion of e-government services, raise awareness of applied security measures and safeguards to enhance trust in the use of these services. **R2.7** Encourage the development of local e-commerce services, while emphasising the need for security. **R2.8** Improve the affordability and availability of online payment services to encourage users to use new e-commerce services.
D2.3 User Understanding of Personal Information Protection Online	**Start-up**	**R2.9** Establish programmes to raise user awareness of online risks and available measures to protect personal information online. **R2.10** Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making.
D2.4 Reporting Mechanisms	**Start-up**	**R2.11** Establish a central mechanism that allows citizens to report all types of cybercrime to law enforcement. **R2.12** Raise awareness about available reporting channels among the wider public.

D2.5 Media and Social Media	**Formative**	**R2.13** Encourage media content providers, including traditional media outlets, to disseminate information on good cybersecurity practice. **R2.14** Make full use of social media platforms to raise awareness on cybersecurity, including by engaging with national thought leaders that are already active in this field. **R2.15** Develop programmes to raise awareness among media and social media providers and actors on cybersecurity issues, for instance through a dedicated cybersecurity awareness month or dedicated sites on this topic.
D3.1 Awareness Raising	**Start-up**	**R3.1** Develop a national cybersecurity awareness raising programme as part of ICT literacy awareness-raising efforts for specified target groups, focusing on the most vulnerable users, in particular youth. Designate a government department to lead the implementation and monitoring of the cybersecurity awareness raising programme. **R3.2** Coordinate the development and implementation of the awareness raising programme with relevant stakeholders from private sector, academia and civil society in the development. **R3.3** Develop a dedicated awareness raising programme for executive managers within the public and private sectors.
D3.2 Framework for Education	**Start-up to Formative**	**R3.4** Develop specific degree programmes in cybersecurity and expand the availability of cybersecurity courses to students of non-technical study programmes, such as law or management studies. **R3.5** Create cybersecurity education programmes for educators to ensure that skilled staff is available to teach newly formed cybersecurity courses. **R3.6** Coordinate consultations across government, private sector, academia and civil society stakeholders to inform cybersecurity education priorities. Develop cooperation initiatives to enhance the interaction between universities and the national economy. **R3.7** Integrate cybersecurity modules into the curricula of primary and secondary schools, across all ages.
D3.3 Framework for Professional Training	**Formative**	**R3.8** Identify cybersecurity training needs and develop training courses, seminars and online resources for targeted demographics, including non-IT professionals. Ensure that the needs across the society are well understood and a list of training requirements is documented. **R3.9** Create a knowledge exchange programme to enhance cooperation and coordination between training providers from private sector and academia. **R3.10** Establish job creation initiatives for cybersecurity within organisations and encourage employers to train staff to become cybersecurity professionals. **R3.11** Institutionalise knowledge transfer between trained and untrained staff within organisations to maximise training outputs. R3.12 Endeavor to make national offerings of cyber training meet the training needs of the country and provide financial support for expensive local courses
D4.1 Legal Frameworks	**Start-up to Formative**	**R4.1** Supplement the existing legislative framework on cybersecurity, cybercrime and data protection. Develop legislative provisions by amending established legislation or adopting new legislation to address on the full scope of cybercrime, human rights online, child online protection, consumer protection and intellectual property online. **R4.2** Enact commencement orders to bring existing legislation in action and assign bodies to monitor the enforcement of cybersecurity and data protection laws.

		R4.3 Develop and adopt legal provisions on procedural powers for investigations of cybercrime and crimes involving electronic evidence. **R4.4** Consider joining regional cybercrime instruments to enhance international cooperation to combat cybercrime.
D4.2 Criminal Justice System	**Start-up to Formative**	**R4.5** Assess and strengthen the capacity of law enforcement to investigate computer-related crimes, including human, procedural and technological resources, digital forensic capabilities and digital chain of custody. **R4.6** Develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence. **R4.7** Build a cadre of specialised prosecutors and judges to handle cybercrime cases and cases involving electronic evidence.
D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime	**Start-up to Formative**	**R4.8** Establish formal international cooperation mechanisms, including mutual legal assistance and extradition, to combat cybercrime. **R4.9** Strengthen informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders. Consider experiences made in other areas, such as anti-corruption cooperation.
D5.1 Adherence to Standards	**Start-up to Formative**	**R5.1** Establish a programme to strengthen the government's capacity to adapt or adopt international standards in order to acquire a baseline in the context of organisational cybersecurity. **R5.2** Establish or assign an institution responsible for the implementation, auditing and measurement of the success of cybersecuritystandards across public and private sectors. **R5.3** Promote the adoption of international IT standards, in particular during procurement and software development. **R5.4** Promote the awareness and implementation of standards among SMEs. **R5.5** Establish a framework to assess the effectiveness of standards for procurement and software development.
D5.2 Internet Infrastructure Resilience	**Formative**	**R5.6** Increase reliability of Internet infrastructure and expand the national programme for infrastructure development. **R5.7** Establish or assign an institution responsible to enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors. **R5.8** Establish or assign an institution responsible to identify, implement and perform auditing on technology and processes deployed for Internet infrastructure. **R5.9** Establish a system to formally manage national infrastructure, with documented processes, roles and responsibilities, and redundancy.
D5.3 Software Quality	**Start-up to Formative**	**R5.10** Develop a catalogue of secure software platforms and applications within the public and private sectors. **R5.11** Develop an inventory of software and applications used in public sector and Critical Infrastructure.

		R5.12 Develop policies and processes on software updates and maintenance. **R5.13** Gather and assess evidence of software quality deficiencies regarding their impact on usability and performance. **R5.14** Establish or assign an institution to elicit in a strategic manner common requirements for software quality and functionality across all public and private sectors.
D5.4 Technical Security Controls	**Formative**	**R5.15** Promote user understanding of the importance of anti-malware software. **R5.16** Encourage ISPs and banks to offer anti-malware and anti-virus services. **R5.17** Establish metrics for measuring the effectiveness of technical controls across the public domain. **R5.18** Develop processes for reasoning about the adoption of more technical controls based on risk assessment methodologies across the public domain. **R5.19** Establish or assign an institution responsible for identifying the need for and adherence to cybersecurity technical controls such as SANS 20, CESG 10 steps and PAS 55 across the public domain.
D5.5 Cryptographic Controls	**Formative**	**R5.20** Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to international standards and guidelines. **R5.21** Raise public awareness of secure communication services, such as encrypted/signed emails. **R5.22** Use SSL/TLS connections to secure communications between schools and the registry office for the collection of students' data. **R5.23** Ensure that data are stored in an encrypted format in the schools' equipment. **R5.24** Establish or assign an institution responsible for designing a policy, aiming to assess the deployment of cryptographic controls according to their objectives and priorities within the public and private sector.
D5.6 Cybersecurity Marketplace	**Start-up**	**R5.25** Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological development. **R5.26** Promote sharing of information and best practices among organisations, to explore potential cybercrime insurance coverage.
D5.7 Responsible Disclosure	**Start-up**	**R5.27** Develop a responsible vulnerability disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledge report. **R5.28** Establish or assign an institution responsible for supervising the process of responsible disclosure and ensure that organisations do not conceal this information. **R5.29** Develop a system to facilitate threat-intelligence sharing within the critical infrastructure partners and ISPs. **R5.30** Encourage sharing of technical details of vulnerabilities among critical infrastructure and ISPs.

The review was conducted in cooperation with the World Bank and the dissemination of this report was carried out in cooperation with Global Cybersecurity Center for Development (GCCD) under Korea Internet Security Agency (KISA) of Republic of Korea. The financing came from Korea's Ministry of Strategy and Finance (MoSF) through the Korea-World Bank Group Partnership Facility (KWPF), which is administered by the World Bank.

World Bank Office in Bishkek

214 Moskovskaya Street, Bishkek, 720010

Kyrgyz Republic

Tel: +996 312 625262

Web: www.worldbank.org/en/country/kyrgyzrepublic

Global Cyber Security Capacity Centre

Oxford Martin School, University of Oxford

Old Indian Institute, 34 Broad Street, Oxford OX1 3BD,

United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435

Email: cybercapacity@oxfordmartin.ox.ac.uk

Web: www.oxfordmartin.ox.ac.uk

Cybersecurity Capacity Portal: www.sbs.ox.ac.uk/cybersecurity-capacity