CITRA

الهيئة العامة للاتصالات وتقنية المعلومات

COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

دولة الكويت

STATE OF KUWAIT

NATIONAL CYBER SECURITY STRATEGY FOR THE STATE OF KUWAIT 2017 - 2020

First Edition

2017

His Highness

Shiekh Sabah Al-Ahmad Al-Jaber Al-Sabah

Amir of Kuwait

His Highness

Shiekh Nawaf Al-Ahmad Al-Jaber Al-Sabah

The Crown Prince

Prime Minister's Foreword

Communications, information technology and Internet culture have become the most vital characteristics of this era. These technologies have contributed in changing the concepts of space and time, making it possible to connect with the world and track international events within moments, promote cooperation and limit the barriers to business and innovation locally and internationally, thereby driving economic growth. These technologies now encompass all aspects of social life, and contribute inimproving and enriching our lives by providing opportunities for innovation, a variety of products and services, and diversity of communication channels.

At the time our dependence on the Internet and modern means of communication is increasing, these benefits accompanied by so many cyber risks. Such risks entail the practice of committing crimes and causing damages to individuals and institutions. Prominent examples of cybercrimes center around intrusions; hacking; information theft, privacy violations and illegal activity. In fact, the cybercrimes turn out to not only pose a threat to individuals and institutions, but beyond that to threaten the security of the country and safety of its facilities and economy. And this is what calls for building new security capabilities, devoting more efforts to enhancing the security of the State of Kuwait and its citizens, and confronting the real challenges and threats raised by cyber security breaches.

The National Cyber Security Strategy acknowledges the imminent challenges and threats facing the country. It is therefore important to identify principles and actions to be taken, adopt all essential technologies, build capabilities, and improve the ability to deal with cyber security issues. We aim to promote the security of our national critical infrastructure and information, reducing cyber risks that threaten the country's economy and national security, along with ensuring a reliable, trusted and secure cyber environment for the government, the private sector, and individuals.

His Highness the Prime Minister
Sheikh. Jaber Mubarak Al-Hamad Al-Sabah

CONTENTS

1. INTRODUCTION

Information and communication technology has become an essential engine for the movement in modern societies, in fact it turns out to be a key factor for economic growth, human progress and social development. As the variety of telecommunication networks have facilitated access to all information and data from different forms and locations, herein lies the risk of what these networks and information can come with.

The incremental dependence on information and communication technologies make us vulnerable to the risks, threats and attacks of cyber space. These risks emerge from technical weaknesses of operating systems and software, lack of legislation outlawing electronic crimes, and ineffective information sharing between the government, the private sector and individuals. Such inefficiency has enabled amateur and computer specialists to practice illegal activities, thereby threatening the basic services provided to individuals, government entities, companies and institutions.

Attacks and cybercrimes spread widely and in various forms such as malware, DDOS attacks,piracy of personal data and those protected by intellectual property rights, spam e-mails sent to carry out extortion, fraud, identity theft, unauthorized access to systems, and sabotage or manipulation of systems and data. Irrespective of the motives of hackers and criminals, all these activities pose an alarming threat to institutions and individuals, and can cause a negative impact on the economy.

Moreover, cybercrimes have now become more organized to cause defects not only to government entities, the private sector and individuals, but their impact extends to reach nations. Criminals are now able to exploit cyber space to perform their criminal activities and in a complement manner to ordinary crime. To highlight, they have now become able to organize themselves, exchange information or form criminal gangs, utilize infrastructure and cyber space to practice different crimes such as money laundering, extortion, drug dealing,arms smuggling, corruption,human trafficking, child abuse, and financial manipulation.

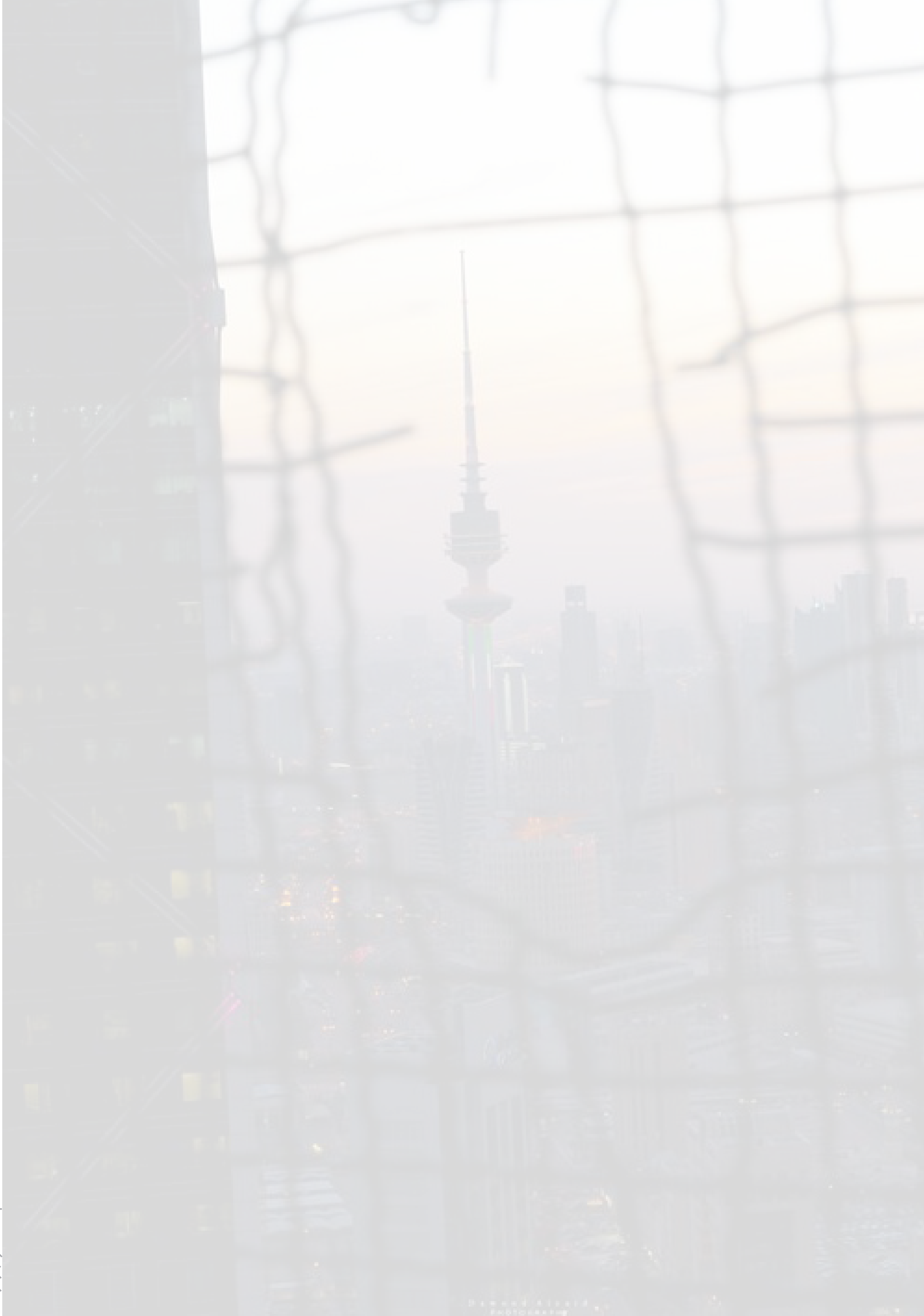
There are criminals who follow organized groups or governments of states, endangering national security to new challenges related to information technology, and alarming a rise of an informational war that can have serious effects on the economy of the state, its security and stability. Activities such as electronic intelligence, espionage and gathering of sensitive information, or spread rumors and misinformation aimed at undermining security may be practiced. This extends to take on a terrorist dimension if targeting systems of vital infrastructure and public utilities such as energy, electricity, water, transportation, communication systems, financial sector, and medical services.

And so, we realize the necessity to safeguard our critical national infrastructure, assets and resources of the State of Kuwait, alongside the necessity to regulate communication and the exchange of information between networks, while providing continuous monitoring of the flow of information to ensure that they do not carry any threats, and are not used to damage the interests of the State, institutes or individuals.

In this respect, many institutions within the State of Kuwait have applied initiatives to safeguard their critical national infrastructure, data and assets, as well as formulate policies and rules of cyber security to provide a means of protection against any potential risks of cyberspace. Moreover, the enactment of laws and legislations related to cybercrime have covered a lot of activities of cyberspace criminals.

Yet, there is still a high demand to govern these initiatives, manage cyber security activities, and to ensure that there is an integrated, comprehensive and resilient mechanism to manage national cyber security. In addition to the need for a national strategy that integrates between the efforts and initiatives of each institute, and ensures all cyber security risks are addressed, whether within the institutions or from the Internet gateways that connect these institutions with the external world.

The “National Cyber Security Strategy of the State of Kuwait” is a response from the Kuwaiti government due to the extent of threats and challenges of cyber risks against institutions and individuals. The Strategy serves as a road map towards strengthening information security in all different forms, and to ensure we harness all possibilities and take all effective precautions needed.



2. KUWAIT'S APPROACH TO CYBER SECURITY

This strategy articulates the overall vision and objectives of Kuwait's National Cyber Security Strategy, and sets out the strategic priorities to achieve its objectives. Furthermore, the strategy describes the initiatives and activities that will take effect through a comprehensive program to direct the efforts of the government agencies and the private sector toward the National Cyber Security Strategy driven by the government of Kuwait.

Vision

Assure a secure and resilient cyber space to safeguard the national interests of Kuwait.

Our vision in the state of Kuwait is to attain the greatest social and economic potential of cyberspace usage, and make the most of the possibilities and advantages it provides. This can be achieved by averting cyber-risks, threats and vulnerabilities through the adoption of all security precautions, to promote and protect the competence governing cyber security administration and the response to any emergency.

Mission

Establish and promote a national cyber security structure including technical, legal regulatory and administrative dimensions, for all government agencies and the private sector. This will maintain the cyber environment and promote security and prosperity to all those who live and work in Kuwait.

Objectives

The Cyber Security Strategy is based on three main objectives that enable the government of the state of Kuwait to achieve its vision:

Objective 1

Promote a culture of cyber security that supports safe and proper usage of cyberspace.

Objective 2

Safeguard and continuously maintain the security of national assets including critical infrastructure; national data, communication technologies and the Internet in the State of Kuwait.

Objective 3

Promote the cooperation, coordination and information exchange among local and international bodies in the field of cyber security.

Objective 1: Promote a culture of cyber security that supports safe and proper usage of cyberspace

The Kuwaiti government acknowledges the importance of building and maintaining a secure cyberspace to promote confidence of the Kuwaiti community in the cyber environment, and ensure the security and confidentiality of their electronic transactions and personal information. The Kuwaiti government also recognizes that cybercrimes have become an increasing concern to many people, and as information and communication technologies continue to be integrated into many aspects of daily life, such crimes have proven to be a cause of concern.

Kuwaiti government, therefore, to provide high attention in empowering the knowledge and education for all segments of society, providing them with all the information of cyber risks they are exposed to, and the required protection tools and techniques for cyberspace-connected personal and financial information.

Moreover, the assurance of a secure cyber environment which is essential for an effective digital economy, requires government and private sector collaboration to limit cyber security risks, protect critical national interests, and deliver a trusted cyber operating environment for Kuwait society. This can be achieved by strengthening the means of protection of national information, Internet infrastructures and critical government systems, utilizing the best international practices of cyber security, and encouraging government agencies and the private sector to exchange information securely to ensure the protection of important data.

Under this objective, the following activities must be undertaken:

- Develop a culture of cyber security that provides Kuwait society with the awareness of the risks, threats and vulnerabilities associated with cyberspace usage.
- Encourage people to utilize cyber security tools and techniques to protect themselves online.
- Develop cyber security curriculum for schools and universities.
- Collaboration of Kuwait government and the private sector to improve cyber security and ensure the protection of data transactions, by promoting awareness of cyber risks, as well as following the best practices in the field of cyber security and applying the best protection systems.

Objective 2:Safeguard and continuously maintain the security of national assets, including critical infrastructure, national data, communication technologies and internet in the State of Kuwait

Information and communication technologies are critical to Kuwait's national interests, therefore Kuwait government needs specific attention towards ensuring secure and resilient communication and information technologies for all government agencies, companies and institutions, as well as the whole community.

Kuwaiti Government recognizes that it must be proactive in identifying and analyzing cyber threats and risks, and accordingly, developing the appropriate means of proactive defenses, mitigation strategies, and continuous monitoring of incident responses.

In addition, the government acknowledges the importance of having a national cyber security framework comprised of standards, policies and procedures, to be implemented by all critical national institutions, and ensure that they do not rely on security technologies alone. Building at the same time, national capabilities that can deal with cyber security issues with the assistance of international expertise.

Under this objective, the following activities must be undertaken:

- Develop and maintain a risk assessment and threats analysis for critical national infrastructures.
- Develop and promote the means of defenses of the State of Kuwait's civil and military networks to limit the possibilities of electronic attacks.
- Establish and maintain National Cyber Security Center- NCSC including Security Operation Center (SOC) and Computer Emergency Response Team (CERT) functions to serve all government agencies, private sector and individuals, in order to promote the country's ability to protect national interests from possible cyberattacks.
- Establish and maintain Security Operation Center (SOC) in the vital sectors of the state of Kuwait to provide a continuous monitoring of cyber security events, and develop the proper means of response.
- Provide continuous monitoring mechanisms for the critical national infrastructures and information.
- Develop and maintain national incident response and business continuity plans to manage crises of cyber security for the State of Kuwait.
- Develop and maintain national cyber security policies and controls for the national critical networks, electronic services, and critical ICT systems.
- Develop legislation for laws of cybercrime and cyber security to keep pace with technological evolution
- Monitor the compliance with cyber security regulations and national policies.
- Cooperate with the private sector to identify and implement cyber security controls that ensures protection from attacks and various cybercrimes.
- Develop national capabilities in different cyber security domains such as the fight against cybercrime, implementation and monitoring of policies and regulations, and emergency response.
- Develop national standards and criteria to classify information security technology.

Objective 3: Promote the cooperation, coordination and information exchange among local and international bodies in the field of cyber security

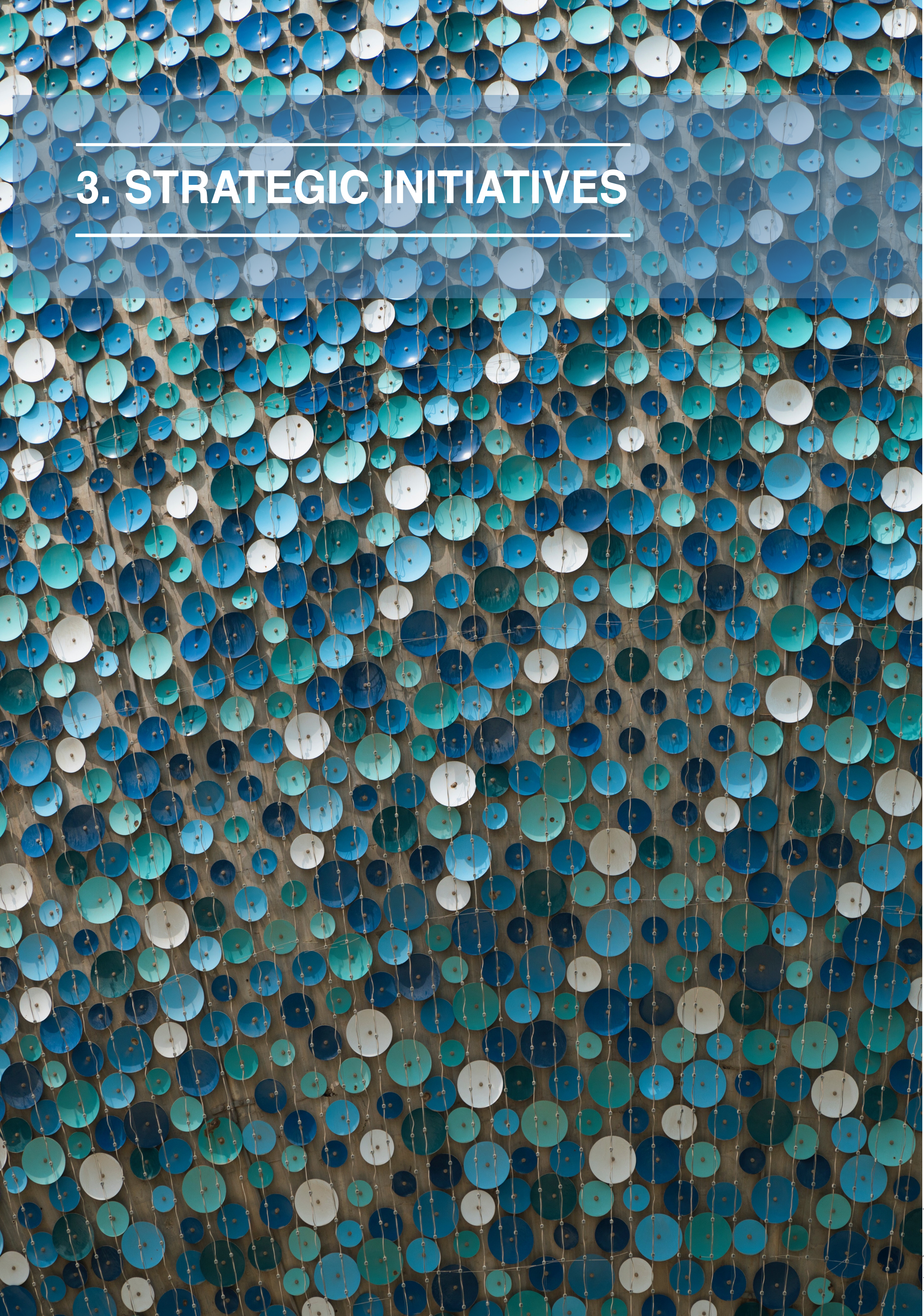
Cyber threat intelligence within the state of Kuwait is considered as one of the essential practices of prevention, and is important to coordinate efforts of addressing potential cyber risks. The prior knowledge of any cyber threat, including its nature and target, can promote prevention practices and the mitigation of any negative impacts. Furthermore, by enhancing knowledge transfer among all organizations to express cyber threats,accordingly can adopt the proper means of defenses.

Moreover, through international cooperation we utilize global standards and best practices in the field of cyber security, and develop an international legal partnership to combat cybercrime and promote best practices in cyber security awareness, strategic prevention and crisis response.

Under this objective, the following activities must be undertaken:

- Develop a national information sharing partnership including government agencies, the private sector and leading cyber security companies.
- Develop a regional and international coordination mechanism for the exchange of cyber security information.
- Develop an international police partnership for joint investigation and disruption of e-crimes.
- Participate in international cyber security programs.
- Take advantage of leading companies' experience in the field of cyber security.

3. STRATEGIC INITIATIVES



Objective 1: Promote a culture of cyber security that supports safe and proper usage in cyberspace

The Initiative
Promote national awareness in cyber security to all segments of society by identifying expected risks from cyberspace usage, while encouraging the usage of security and risk deterrence solutions. Government lead: CITRA (NCSC-KW)
Cooperate with the Ministry of Education and Ministry of Higher Education and affiliates to develop an educational curriculum for cyber security. Government lead: CITRA (NCSC-KW) and MOE
Cooperate with the private sector, telecommunication and mobile operators, and Internet Service Providers to improve cyber security and ensure the protection of data transactions, by promoting awareness of cyber risks. Government lead: CITRA (NCSC-KW)

Objective 2: Safeguard and continuously maintain the security of national assets, including critical infrastructure, national data, communication technologies and the Internet within the State of Kuwait

The Initiative
Establish and maintain a National Cyber Security Center (NCSC) including Security Operation Center (SOC) and Computer Emergency Response Team (CERT) functions, to work as a focal point for CNIs SOCs. Government lead: CITRA(NCSC-KW)
Establish and maintain Security Operation Center SOC in vital sectors within the state of Kuwait to provide a continuous monitoring of cyber security events, and develop proper means of response. Government lead: MOD, OIL COMPANIES, AND OTHER CNIs
Develop national capabilities in different cyber security domains such as the fight against cybercrime, secure software development, network security, application and monitoring of laws and policies, and information security emergency response. Government lead: CITRA(NCSC-KW)
Develop national standards and criteria to classify information security technology. Government lead: CITRA(NCSC-KW)
Develop national capabilities in the fight against cybercrime according to international standards. Government lead: MOI
Develop and maintain national incident response and business continuity plans to manage crises of cyber security in the State of Kuwait. Government lead: CITRA(NCSC-KW)
Develop and promote the means of defence of the State of Kuwait’s civil and military networks to limit possibilities of electronic attacks. Government lead: CITRA (NCSC-KW), MOD AND CNIs
Develop legislation and laws of cybercrime and cyber security to keep pace with technological evolution. Government lead: MOI, MOD, MOInformation, CAIT and CITRA(NCSC-KW)
Develop and maintain national cyber security policies and controls for the national critical networks, electronic services, and critical ICT systems. Government lead: CITRA(NCSC-KW)
Monitor the compliance with cyber security regulations and national policies. Government lead: CITRA(NCSC-KW)

Objective 3: Promote the cooperation, coordination and information exchange among local and international bodies in the field of cyber security

The Initiative
Develop a national information sharing partnership including government agencies, the private sector and leading cyber security companies. Government lead: CITRA(NCSC-KW)
Develop a coordinating mechanism for the exchange of information among regional and international institutions and participate in cyber security programs to deal with cyber threats, and facilitate access to reliable information and ensuring an effective response to all threats. Government lead: CITRA(NCSC-KW)
Develop a national reporting mechanism for cyber threats, attacks and cybercrimes. Government lead: CITRA(NCSC-KW), MOI
Develop international police partnerships for joint investigation and disruption of E-crimes. Government lead: MOI

4. IMPLEMENTATION APPROACH

Successful implementation of the National Cyber Security Strategy requires leadership, commitment, proper governance and continuous measurement of cyber security performance in terms of improved cyber maturity and reduced exposure to cyber risks. Accordingly, the National Cyber Security Strategy is based on the following guiding principles:

National Leadership:

The challenge in implementing the strategy mainly resides in the strong national leadership, therefore, Kuwait government is to form a National Cyber Security Committee which will report to the Council of Ministries. The committee works as a focal point for all cyber security activities and efforts across Kuwait.

National Governance:

Kuwait government is to form a National Governance Committee who will report to the National Cyber Security Committee. The responsibility of this committee is to ensure proper governance is practiced through the implementation of the strategy, as well to the following responsibilities:

- Mandate to manage the National Cyber Security Programme.
- Develop and maintain national cyber security priorities.
- Working in close relation with government agencies, companies and institutions concerned with the National Cyber Security Strategy.
- Provide the National Cyber Security Committee with the strategic approach for the NCS.
- Run national risk management activities.
- Manage national cyber maturity measurement activities.

National Cyber Security Programme:

To achieve the Strategy of national cyber security, a three-year programme will be developed which consists of all the initiatives and activities associated with the funding plan.

Cyber Risk Management:

As all ICT systems are vulnerable to cyber risks, a risk-based approach must be conducted continuously while applying the cyber security strategy to assess, prioritize, monitor and invest in appropriate cyber security activities.

National Cyber Maturity Measurement:

Is the tool to measure and report NCS improvement and maturity against an international cyber security maturity standard.

Shared responsibilities:

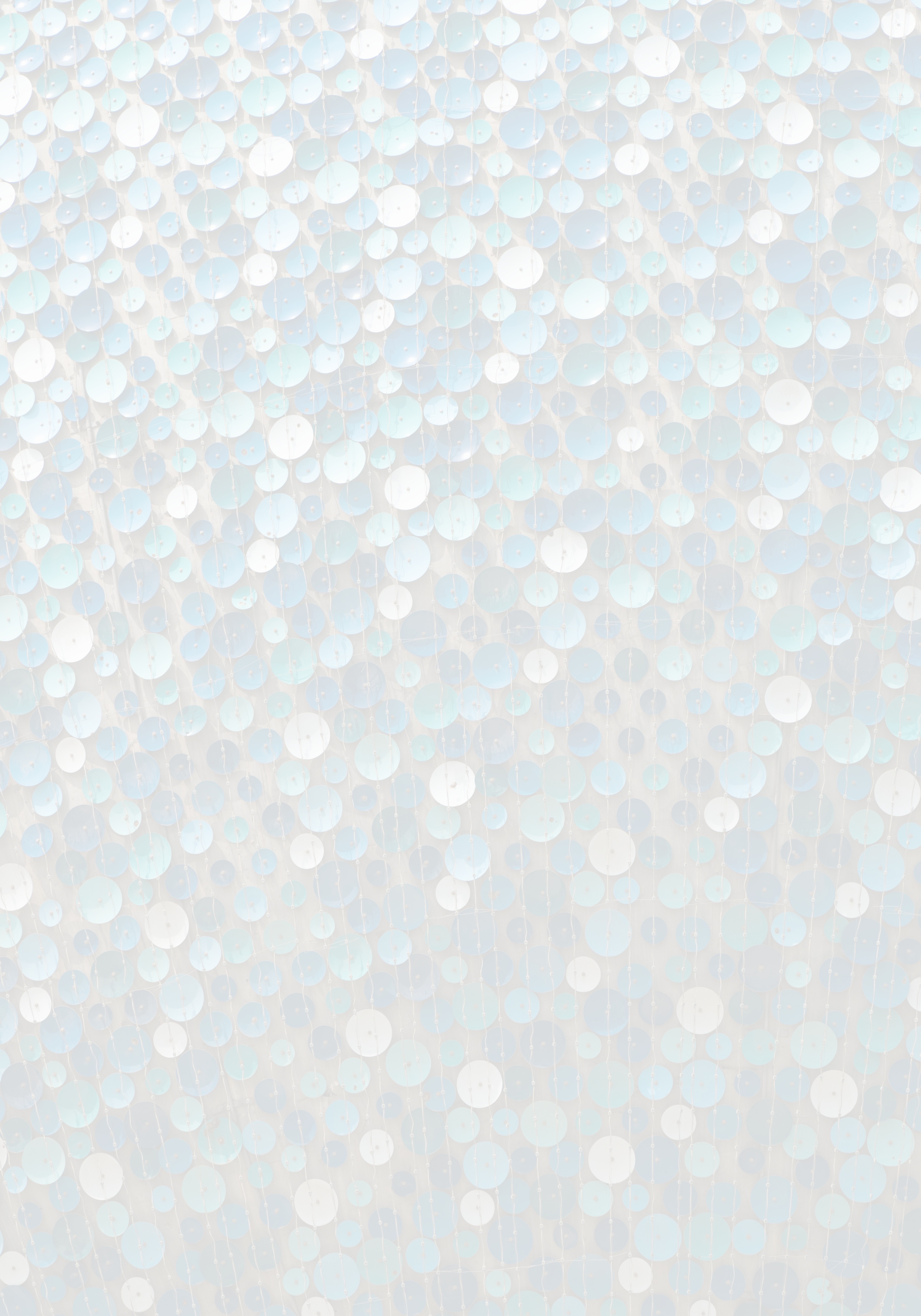
Cyber security is the responsibility of all government entities, the private sector, institutions and individuals. All must take actions to secure their own ICT systems, protect the means of communication, and securely store critical information and respect the privacy of other systems and users.

Protected Fundamental Rights and Values:

By the implementation of the National Cyber Security Strategy, Kuwait aims to pursue effective cyber security policies, initiatives, precautions and tools, to combat e-crime, promote cyber security and privacy, and ensure the consistency with laws and regulations of the State of Kuwait. At the same time, the strategy preserves the fundamental rights, freedom and privacy of individuals and institutions.

As an example, the absence of personal security in cyberspace greatly increases the possibility of personal data breach, therefore breaching the privacy of the individual. This requires presupposing actions and initiatives to promote the cyber security such as utilizing ICT systems, and apply policies to reserve privacy rights while using communication systems and safeguarding personal data and information security.

Accordingly, the national cyber security strategy endeavours to balance between these two concepts, by considering both national and international legal requirements while protecting data, secure information, threat intelligence, privacy protection, monitoring and others while establishing cyber security policies and controls for information security and communication technologies.



5 ACKNOWLEDGMENTS

We would like to thank all who effectively participated during the development of the “National Cyber Security Strategy of the State of Kuwait”. Firstly, we would we would like to thank the members of the National Cyber Security Committee, chaired by Communications and Information Technology Regulatory Authority, and membership from vital Government agencies for their active participation and contribution to enrich the Strategy from the fact of their experience in Cyber Security field.

- Ministry of Defense
- Kuwait National Security Bureau
- Central Agency for Information Technology
- Ministry of Interior
- Ministry of Electricity and Water
- Kuwait Petroleum Corporation

We would also like to thank the Government agencies, telecommunications and Internet Service Provider companies that participated in reviewing the National Cyber Security Strategy, and provided us with valuable recommendations.

- Central Bank of Kuwait
- The Public Authority for Civil Information
- VIVA
- Ooredoo
- Zajil Telecom
- Wireless Mobile Data Co. WiMD
- Kuwait Oil Company
- Zain
- Qualitynet
- Fast Telecommunications
- Mada Communication
- Gulfnet

6 APPENDIX (A)

Cyber Security Definitions and Terminology

Cyber security: is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise Availability, Integrity, which may include authenticity and non-repudiation, and Confidentiality.

Cyberspace or cyberspace environment: is figuratively the virtual space for computer systems and electronic networks, where information stored electronically and directly connect to the network, it is an intangible space including data such as personal information, electronic transactions, intellectual property and other related topics.

Vital sectors for the State of Kuwait: is the service or productive sectors of the state from Government, companies or institutions. Any crashes, destruction or damaging in those sectors can harm the security of the State, the business of institutions or the economic situation, and include all the following:

- Oil sector.
- Military sector.
- Energy sector and electricity and water.
- Financial sector.
- Communications, telecommunication and information technology sector.
- Transport sector.
- Health sector.
- Other government entities.

The infrastructure: is the physical assets, systems, machinery or equipment used to connect computers, it is vital to the State of Kuwait, and in any event, it had been damaged or destroyed, then a serious impact may occur on business of institutions, economy or security of the State.

Risk management: it is a continuous process of identifying potential risks, analysis and evaluation of their impact and maintained the risk at an acceptable level. Risk management enables organizations to define policies and controls which are the most likely to protect the assets.

Hackers and criminals of information technology: they are professionals earn their living from their work, or amateur admirers in presenting their technical skills, these criminals and hackers take several forms of cyberattacks like the APT attack, DDoS attack, destruction or theft of sensitive data, intrusion of networks, breach of software security, electronic eavesdropping (which includes sabotage and stealing telephone calls, and the cost often paid by the victims, whether individuals or institutions).

Electronic crime: illegal, unethical or unauthorized conduct, and is an extension of the normal criminal activity that conducted via cyberspace using non-traditional methods to complement the ordinary crime. Cybercrime has several types including:

- Cybercrime that targets individuals, aimed to obtain illegally on the electronic identity of individuals, such as email and password, or impersonation electronically, or drag photos and important files from victim's device to threaten him and request orders.

- Cybercrime that targets government and private agencies, destroying important files, data or proprietary software, by sending malware to the user's computer and in a variety of ways like electronic mails.

- Cybercrime that targets Governments, the pirate attacks government official websites and network systems aiming to damage the website, the infrastructure of the site, the network system or destroy all aforementioned. Or it may target military sites for some States to steal data relating to State security.

- Other crimes such as fraud, theft, extortion, theft of electronic information and use them illegally, cursing and swearing, slander, and cyber terrorism.

National governance: is a framework that determines the roles and responsibilities of all parties involved in the implementation of the national cyber security strategy, and provides a clear mechanism for communication and coordination among all parties and during the cycle of the strategy.

Security Audit: a systematic analysis of all security components including people, policies, solutions and tools that used by any institution to secure its environment. Furthermore, security audit aims to monitor compliance with security policies, assess the level of risk and the balance between resources including organizational, technical and human resources.

Cyber security policies: it is the cyber security framework, and the reference that reflects the national strategy, activities and implementation tools.

National Cyber Security Center of Kuwait (NCSC-KW): is a government center within Communication and Information Technology Regulatory Authority-CITRA that is responsible of all national cyber security activities in the State of Kuwait.The center works with government agencies and private sector to monitor Kuwait's networks for cyber security threats, collect and disseminate threat intelligence, and support the national cyber security response.

NCSC-KW other functions include standardization of the national cyber security, evaluation and classification of cyber security industry, ICT systems and services.

7 APPENDIX (B)

References

1- “Definition of cybersecurity”. International Telecommunication Union (ITU), ITU-T X.1205, **http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.asp**

2- “National Cyber Security Strategies Practical Guide on Development and Execution”. European Network and Information Security Agency (ENISA), **https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-.implementation-guide**

National Cyber Security Strategy for the State of Kuwait 2017 - 2020

Objective 1

Promote a culture of cyber security that supports safe and proper usage for the cyberspace

- Promote national awareness in cyber security to all segments of society by identifying expected risks from cyberspace usage, while encouraging the usage of security and risk deterrence solutions.
- Cooperate with the Ministry of Education and Ministry of Higher Education and affiliates to develop an educational curriculum for cyber security.
- Cooperate with the private sector, telecommunication and mobile operators, and Internet Service Providers to improve cyber security and ensure the protection of data transactions, by promoting awareness of cyber risks.

Objective 3

Promote the cooperation, coordination and information exchange among local and international bodies in the field of cyber security

- Develop a national information sharing partnership including government agencies, the private sector and leading cyber security companies.
- Develop a coordinating mechanism for the exchange of information among regional and international institutions and participate in cyber security programs to deal with cyber-threats, and facilitate access to reliable information and ensuring an effective response to all threats.
- Develop a national reporting mechanism for cyber threats, attacks and cybercrimes.
- Develop international police partnerships for joint investigation and disruption of E-crimes.

Objective 2

Safeguard and continuously maintain the security of national assets including critical infrastructure, national data, communication technologies and Internet in the State of Kuwait

- Establish and maintain a National Cyber Security Center (NCSC) including Security Operation Center (SOC) and Computer Emergency Response Team (CER)T functions, to work as a focal point for CNIs CERTs.

- Establish and maintain Security Operation Center SOC in vital sectors within the state of Kuwait to provide a continuous monitoring of cyber security events, and develop proper means of response.

- Develop national capabilities in different cyber security domains such as the fight against cybercrime, secure software development, network security, application and monitoring of laws and policies, and information security emergency response.

- Develop national standards and criteria to classify information security technology.

- Develop national capabilities in the fight against cybercrime according to international standards.

- Develop and maintain national incident response and business continuity plans to manage crises of cyber security in the State of Kuwait.

- Develop and promote the means of defence of the State of Kuwait’s civil and military networks to limit possibilities of electronic attacks.

- Develop legislation and laws of cybercrime and cyber security to keep pace with technological evolution.

- Develop and maintain national cyber security policies and controls for the national critical networks, electronic services, and critical ICT systems.

- Monitor the compliance with cyber security regulations and national policies.

CONFIDENTIALITY STATEMENT
No information regarding this document can be shared, discussed or
disclosed to people without written approval from the document owner.