وزارة الإتصالات و تكنولوجيا المعلومات

Ministry of Information and Communications Technology

National CyberSecurity Programme

National CyberSecurity Strategy

February 2018

Table of Contents

1 Foreword

Jordan Government is committed to enhancing its cyber security and, with the publication of its National Information Assurance and Cyber Security Strategy (NIACSS) in 2012, set out its priorities for cyber security for Government, business and citizens. Now is the time to review our progress against delivery of the five strategic objectives established in the NIACSS and to establish priorities for the next five years in the context of the evolving threat and the evolution of our strategy.

The rapid growth of the internet and digital technology present significant opportunities for Jordan, both nationally and internationally, and underpin our growth. The digital world supports the prosperity agenda through social mobility and inclusion, access to key services and education, job creation and wealth, economic growth and investment. However, an information society with critical e-services cannot exist without effective cyber security. National Cyberspace is a modern environment that needs systematic and comprehensive protection at international, national, sector, organisation and individual levels.

The security of our digital assets is vital to us making the best use of these opportunities and for ensuring that cyber space, as it relates to Jordan, is a safe place for those already living and working here and attracts new people and business.

This increased opportunity also presents new and challenging threats to our cyber security. We must ensure that we tackle these threats effectively in a way that makes best use of our existing capabilities and people, whilst delivering sustainable sovereign capabilities through the development of our people.

Our national cyber security strategy recognises that its success depends on effective and long-term commitment from the Government, the private sector and citizens with basic cyber hygiene being relevant to boardroom and home alike. Education is critical to this understanding and academia has an important role to play in equipping Jordanians to keep themselves safe online and to ensure that we have the right people with the right skills protecting our national security and prosperity from those who would seek to do us harm.

This National CyberSecurity Strategy 2018-2023 sets out how Government is going to achieve this.

2 Introduction

This National CyberSecurity Strategy (NCS) covering the period to 2023 provides a summary of the progress made against the delivery of the objectives set out in 2012 and considers how current trends in cyber threats indicate a more robust national approach to the governance of cyber security is required.

The use of Cyberspace is transforming business, making it more efficient and effective. It is opening up markets, allowing commerce to take place at lower cost and enabling people to do business on the move. It has promoted fresh thinking, innovative business models and new sources of growth and business opportunity for established enterprise and emerging entrepreneurs alike. It enables companies to provide a better, cheaper and more convenient shopping experience to customers. It also helps individuals to shop around, compare prices and find what they want.

The digital world is also transforming the quality and speed of the way that the Government seeks to engage with citizens, business and academia. It offers improved information flow and processes within Government, speed and quality of policy development and improves co-ordination and enforcement.

Governments around the world are mobilising to counter the growing cyber threat, which is becoming more sophisticated and complex. As the digital world grows, so does its attraction to those with malicious intent, including state and non-state actors.

These actors are not only working relentlessly to compromise digital assets, they are also looking for new and simple ways of damaging its integrity and disrupting its availability. Cyber criminals threaten people's trust in the security of our digital world such that good cyber security is essential for the success of the digital economy in Jordan.

In a modern society where people are informed mainly through the various forms of media, and form their opinions on it, these same people lose their confidence in the state when it is no longer clear what is false and what is correct. This mistrust can impact on law and order, business investment and international relations.

Secure cyber space is essential for Jordanian entities to prosper, to grow and to demonstrate to external organisations that Jordan is a safe place in which they can conduct business. For national security and prosperity, it is incumbent upon us all to play our part; this includes both the public and private sector organisations and staff, as well as our citizens.

To address the challenges of cyber security head on, and seize the opportunities that cyber space offers, requires leadership and governance of cyber at the highest levels.

3 Progress in Delivering the 2012 Strategy

The National Information Assurance and Cyber Security Strategy (NIACSS) sought to achieve comprehensive information security and the successful implementation of this strategy required collaboration among all involved parties: Government, Defence and Security, the private sector and international partners. It was understood that the efforts of involved parties should complement rather than conflict with each other and that strategies and policies developed by the private sector should augment, comply, and be consistent with this strategy.

When the NIACSS was published in 2012, it was apparent that the scale and pace and impact of technological change was shaping the future for nations and citizens and it provided a wealth of opportunity.

The NIACSS recognised that the greater uptake of internet-based technologies offered increasing opportunities for economic and social development. These developments were seen as offering significant advantages to connected societies.

It has become obvious over the period of the NIACSS that as the reliance on networks globally has grown, so have the opportunities for those who would seek to compromise systems and data.

Equally, the geopolitical landscape has changed. Malicious cyber activity knows no international boundaries. State actors are experimenting with offensive cyber capabilities. Cyber criminals are broadening their efforts and expanding their strategic modus operandi to achieve higher value pay-outs from individuals, organisations and institutions. Terrorists, and their sympathisers, are conducting low-level attacks and aspire to carry out more significant acts.

3.1 National CyberSecurity Programme

The National CyberSecurity Programme (NCP) was established to focus on delivering the strategic objectives and national priorities set out in the NIACSS in 2012 and the programme has:

- Completed a critical network risk assessment programme based on internationally recognised standards and is actively using the outcome of this exercise to deliver protective security enhancements;
- Utilised the outcomes of the risk assessment programme to identify a set of information security standards and policies required to drive an enhanced and consistent approach to national information security;
- Created specific Computer Emergency Response Teams (CERTs) to deliver continuous network monitoring and threat intelligence and incident response capability;
- Planned for a Jordanian National CyberSecurity Centre to further advance our protective security abilities and provide an environment for Government, private sector and citizen engagement to flourish;

- Delivered a cyber training programme to enhance the skills of NCP stakeholders and CERT staff;
- Established a Public Key Infrastructure (PKI) to manage information encryption;
- Started establishing an international information security co-operation programme to aid information sharing, exchange lessons learned and enhance capability development; and
- Established the foundations for a National Cyber Academy to create a Security Awareness and Capacity Building Programme.

There have been some challenges in delivering the 2012 strategy, most notably in the area of developing an appropriate legal and regulatory framework due to the complexity of this area and the international dimension of the threat. Cyberspace is borderless and threat actors exploit this to the fullest extent to stay anonymous. Key relationships are being established with international partners to develop a consistent response whilst at the same time continuing to develop a national legal and regulatory response.

The successful delivery of the NCP over the past five years demonstrates commitment to improving cyber security and has provided a strong legacy on which to move to the next phase of cyber security excellence. The opportunity has been taken to develop this updated strategy with renewed objectives to deliver capability and capacity in the context of the current threat environment and to consolidate and strengthen those successes achieved over the first period of the national cyber security strategy.

This renewed strategy establishes the strategic aims of to deliver a safe information security environment in the national interest.

It is recognised that change in the online world continues to accelerate in a way that has overtaken previous visions of the digital future and the opportunities and dangers it presents. This accelerating pace of change has challenged our ability to adequately protect ourselves from the threats posed by new technologies and applications that have come to the fore. Our strategy needs to be reinvigorated to meet the evolving cyber security challenge.

4 The Evolving Threat Landscape

The environment that Jordan operates in subjects it, in common with other global and regional governments, to threats that are constantly evolving. Recent attacks on other global governments and organisations' infrastructure and personnel (such as acts of terrorism to public services) have highlighted the need for an integrated, co-ordinated, and consistent approach for managing information security threats.

Recent events that have also highlighted the diverse range of threats that governments face include but are not limited to:

- The Snowden leaks have shown the ease with which vast amounts of classified data can be removed from a 'highly secure' network and released to the media, the public and used by foreign intelligence services and other organisations;
- Threats to sensitive and often classified intellectual property have been highlighted by the recent WikiLeaks disclosures exposing, amongst others, National Security Agency (NSA) and Central Intelligence Agency (CIA) activities;
- The recent cyberattack on the UK's National Health Service (NHS) displayed the ease with which ransomware can be used to cripple and hold essential services to ransom.
- Cyberattacks in the Middle East have typically been carried out by hackers targeting the oil and gas sectors, defence and security and other critical industries. The impacts of cyberattacks on Qatar's state news agency have potentially undermined the stability in the Middle East.

Governments, regulators, and societies as a whole are increasingly holding public and private organisations to account for practices across the globe. The previous convention of adopting a defensive and reactive stance as being sufficient to protect an organisation has led to economic loss, reputational damage and increasing legal challenges.

The threat context discussed in this strategy seeks to highlight the sources of threat and levels of persistence to relevant information assets and people.

4.1 Threat Agents

The Global Cyber threat landscape is driven by socio-political context as threat actors discover and attack gaps in information network security. The most likely threats to Jordan are:

Foreign Intelligence Services

Foreign Intelligence Services (FIS) continue to represent the greatest threat to global government information assets through direct external attacks on their systems and through its personnel.

Hacktivists

Hacktivists are activists that use technical tools and means to gain unauthorised access to computer files or networks in order to further or showcase political, social, ideological, or religious messages through illegal or legally-ambiguous methods.

Insider

Humans are biggest cyber security vulnerability where information security breaches can be intentional or unintentional. They can be the result of a single employee's carelessness or a disgruntled employee seeking to deliberately undermine an organisation or another employee.

Crime and Corruption

Threat actors are known to use all feasible attack vectors and increasingly criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

4.2 Cyber Security Challenges

There is a clear shift away from purely money-based motivation and a raft of political and ideological ideas are now coming into play with cyberattacks. Recent cyberattacks indicate that there is going to be an increasingly prevalent role played by Government in cyber security over the period of this strategy, both through its own activity and through relationships with business, international partners and citizens.

Internet of Things

The increasing number of connected devices offers huge opportunity for economic growth, social inclusion and mobility, job creation and communication. There has been a fragmented approach to the security of these 'things' which has provided an opportunity which hostile actors have been keen to exploit.

Ransomware

The popularity of malware as an attack vector has grown steadily as the tactic of encrypting files and charging for their decryption proved successful and its use will be a feature of cyberattacks for some time to come.

Artificial Intelligence (AI) Bots

Cyber criminals are using AI bots to place more targeted phishing adverts and emails, analysing large amounts of social media information to profile their targets. Online chat bots are also being seen more and more in use for customer service – positioning them as a system that people trust. Attackers will look to use this trust and build chatbots to try and obtain bank details from people.

Serverless Apps

Information is particularly at risk when users access an application off-server, locally on their device. When stored on server the owner is more able to control what security precautions are taken to ensure the user's data remains private from identity thieves and other cybercriminals. With serverless applications, however, security precautions are, by and large, the responsibility of the user.

Critical Infrastructure

Critical infrastructure organisations rely hugely on interconnected industrial control systems to manage all aspects of their operation and these provide opportunities for determined attackers to interfere with these systems for political or economic gain.

Sophisticated Phishing Campaigns

Phishing emails, often used to deliver malware or to induce victims to divulge personal information, are becoming more sophisticated with the addition of specific company information regarding billing, logistics, and more. The use of AI Bots by threat agents is adding to this challenge.

Strategic Use of Information Operations

Cyberattacks, cyberespionage and the dissemination of false information (Fake News) are growing tools used by nation-states and other actors to achieve political and economic disruption.

Cyber Awareness

The visibility and public awareness of cyber security remains limited and significantly undermines efforts to protect critical information.

Hacker-for-Hire Services

Easy-to-use and affordable tools have made it easier than ever for attackers to offer hacker-for-hire services.

Skills Shortages

The critical skills shortage of cybersecurity professionals is a global problem that continues to be a major concern for government, businesses and the public.

5 Strategic Context

The revised objectives set out in this strategy recognise the progress made by the NCP in delivering the NIACSS and affirm our ambition to protect Jordan's cyber space to allow Government, Business and Citizens to engage securely in developing a diverse, prosperous and inclusive society:

5.1 Cyber Security Vision

The vision for cyber security for the Kingdom is to be:

Vision	**Confident and secure in an online world.**

This will be achieved through the development, growth and establishment of national cyber security capabilities and an appropriate security response to allow excellence in national security, international business and co-operation and support for e-Government transformation to increase individual and national prosperity.

5.2 Strategic Objectives

Our four strategic objectives set out our aims for achieving a cyber secure Jordan and describe how we will go about achieving them.

5.2.1 **Protect:**

Enhances trust in and resilience of the Government, Critical National Infrastructure, businesses and the general public against cyber threats

- Publishing policies, and procedures to ensure a unified approach to security is established;
- Establishing an appropriate governance structure and entities to ensure effective cyber security;
- Building the necessary organisational structures to develop and operate the nation's cyber security and provide a unified source of advice in Government for threat intelligence and information assurance.

5.2.2 **Detect**:

Supports understanding and disruption of hostile action taken against the Kingdom and its information assets

- Evolving existing cyber threat intelligence capability;
- Understanding the nations cyber space adversaries and their methods;
- Ensuring security defences are effective and detect cyber security events;

- Defining what is ‘normal’ for the context and then detect anomalous events using a broad range of skills and capabilities;
- Ensuring security defences remain current, effective and continue to detect cyber security events.

5.2.3 **Respond**:

Develops and deploys the appropriate capabilities to respond to cyberattacks in the same way as we respond to any other attack on our National Security

- Having well-defined and tested incident management processes, capabilities and mitigation activities;
- Minimising and containing the impacts of cyber security incidents;
- Restoring essential services;
- Using root cause analysis and forensic tools post-incident to drive improvements.

5.2.4 **Evolve**:

Develops the knowledge, skills and sustainable sovereign capability required to maintain robust cyber security, through academia, private sector, research and development and international partnerships

- Partnering with the right organisations and partners to collaborate and share learning;
- Defining and establishing the key academic partners to build suitably qualified and experienced personnel, including a National Cyber Academy;
- Enacting the legislation and regulation needed to establish and operate National CyberSecurity as defined in the strategy;
- Establishing the means to develop sustainable sovereign capabilities and corporate entities that can deliver effective cyber security initiatives;
- Establishing appropriate and robust national and international communication channels.

5.3 Guiding Principles

This Strategy is based on the following principles:

- Cyber security will be managed at the highest levels of Government as a top priority National Security Threat;
- Government will establish the appropriate levels of national governance, co-ordination and control to ensure a collaborative approach to cyber capability development, protection, crisis response and recovery;

- The application of cyber security measures to organisations and systems will be prioritised by risk and impact as it is not possible or affordable to prevent all cyber incidents;
- Cyber security is a shared responsibility at Government, business, academia and individual levels;
- Government has leadership responsibility to ensure that critical infrastructure, whether public or privately owned, is protected against cyber threats;
- Sufficient effort will be expended on ensuring also that individuals understand what they need to do to protect themselves online;
- Linkage with key strategic e-Government strategies is vital to the success of the cyber strategy and the delivery of vital services;
- A positive cyber security culture is essential for effective cyber security and developing citizens and businesses is fundamental to the success of cyber security capability;
- The management of digital risks and the appropriate application of cyber security will be mandated to be a Board level responsibility in all companies ;
- Cyber security is explicitly included in all people, physical and technology decisions;
- Defence in depth and secure by design will be core network and infrastructure design principles.

To achieve the National Strategic Objectives discussed above, the Jordan Government has identified six major national priorities, each priority demanding collaboration across Government, the private sector and citizens supported by international partners. These priorities form the action lines of this National CyberSecurity Strategy.

6 National CyberSecurity Priorities

To achieve the National Strategic Objectives, and building on the success of the National Information Assurance and Cyber Security Strategy, there will be a set of investment priorities which are part of the strategy to bring a new, unified approach to how Government and business deals with cyber security. These priorities dictate the activity that Government of Jordan will engage in over the life of the strategy:

6.1 National CyberSecurity Standards and Policies

A national unified approach to cyber security will be realised through the publication of National CyberSecurity Standards and Policies in the form of a Security Policy Framework and managed through a National CyberSecurity Centre;

6.2 International Information Security Cooperation Program

The ability to safeguard and exchange information securely with foreign Governments and organisations will continue to advance through the International Information Security Cooperation Program;

6.3 Security Awareness and Capacity Building Program

Through close consultation with academia and international partners, a greater degree security awareness will be achieved, along with establishing our own home-grown and organic expertise will be achieved through a defined Capability Building Program;

6.4 Critical National Infrastructure Protection (CNIP) Program

Protection of the most critical elements of Jordan's infrastructure will continue to evolve and grow through the Critical National Infrastructure Protection (CNIP) Program;

6.5 National Computer Emergency Response Teams

The coordinated analysis, dissemination of cyber threat warning information and response to cyber incidents will be achieved through a series of National Computer Emergency Response Teams that will be established across Government, Defence and Security, Finance, Critical National Infrastructure, and to support elements of the Private Sector;

6.6 Legal and Regulatory Reform

Where required, legislative reform will take place to ensure that a balance is maintained between security and privacy, as technology outpaces historical legal and regulatory processes.

7 Strategy Implementation

7.1 Implementation Plan

Having a plan for implementing the strategy is as important as the National CyberSecurity Strategy itself as it sets out the actions necessary to deliver the strategic priorities. The national cyber strategy implementation plan will establish necessary governance to ensure the translation of priorities and objectives into specific well-defined initiatives/projects through:

7.1.1 Ownership

The Government will own the endorsed National CyberSecurity Strategy, assuring that it is afforded the highest precedence across the country.

7.1.2 Co-ordination

Chaired by a Senior Government Official, the Higher CyberSecurity Council will have representatives from Government, Defence and Security, Financial Critical Network Infrastructure and the Private sector and will coordinate Jordan's approach to meeting the National Strategic Objectives though empowered Security Operating Centres and Computer Emergency Response Teams. National Security Operating Centres and Computer Emergency Response Teams will be established to support national sectors of interest. Academic collaboration and international cooperation will play a vital role and underpin the Higher CyberSecurity Council's decision making process.

7.1.3 Implementation Planning

Implementation of the National CyberSecurity Strategy is complex as the activities will impact a number of different organisations and will create a number of new entities. Consequently it will be necessary to manage the implementation as a programme with multiple projects running in different organisations.

A national implementation and action plan will determine short term actions and deliver the strategy to enhance cybersecurity awareness and encourage everyone to take better control of digital security, improve information security, protect privacy, maintain national security and public safety and safeguard economic well being.

The action plan fosters the conditions required for long-term improvements in our approach to cybersecurity across Government, the private sector and our personal lives. Key milestones will be established to monitor and measure progress in delivering the strategy and particularly the effectiveness of our information security measures.

7.2 National CyberSecurity Capabilities

In order to evolve and establish a mature, digitally safe and secure Jordan, there are key high-level capabilities required to establish and manage effective cyber security. These capabilities can be established and grown incrementally and concurrently, in line with the strategic priorities, in order to ensure the delivery of the strategic objectives. Each

capability has a number of supporting functions that will also be built and matured over time, this will include the National CyberSecurity Centre, in order to fully realise and manage the National CyberSecurity Strategy. The National CyberSecurity Centre will be at the heart of the national unified approach to cybersecurity including development of the key cyber security capabilities:

- Strategy Development, Policy Creation and Enforcement;
- Enterprise Preparation and National Cyber Awareness;
- Academia, National Skills, and Investment;
- Cyber Incident Response and Management;
- Critical Network Infrastructure Cyber Risk and Compliance;
- Operational and Threat Intelligence Research;
- Situational Awareness Monitoring and Reporting;
- International Relationships and Partnerships.

7.2.1 National CyberSecurity Centre

The National Cyber Security Centre is the centre of excellence for cyber security and provides active cyber defence to detect and respond to cyber incidents and acts as a link between Government, business, academia and citizens in the delivery of the National CyberSecurity Strategy. Key responsibilities include:

- Collating and analysing information from diverse sources to inform the cyber threat assessment and identity anomalous behaviour for investigation and action;
- Establishing the appropriate legal capability to support the management and discharge of all the cyber related legal and regulatory requirements needed to execute the National CyberSecurity Strategy.
- Strategic planning to determine future requirements that could influence strategic cyber direction, as well as testing current capabilities to provide assurance that expected levels of cyber security are in place, or to identify areas for improvement.
- Assessing cyber tools, products and services for their suitability for use and developing new tools and approaches for use by cyber professionals across the country;
- Developing good guidance and standards to set out expectations for all elements of cyber security;
- Identifying critical national assets that could be threatened by cyber incidents causing significant impact and conducting and maintaining risk assessments of

these assets to identify and implement prioritised measures to manage identified risks;

- Developing a clear understanding of the cyber environment in which national and private sector organisations are operating to support threat awareness and cyber security measures;
- Providing mechanisms to collate and disseminate cyber related alerts to end user organisations, so that national assets and organisations have as much opportunity as possible to manage the impact of cyber incidents;
- Defining and implementing a consistent and effective approach to the management of cyber related incidents to ensure that organisations are able to contain them. Taking a leadership role where appropriate;
- Developing the national and organisational capabilities to respond quickly to cyber incidents through improving the tools, people and processes that need to act whilst events are still happening;
- Providing technical and forensic investigative techniques for cyber related incidents that can be legally admissible where necessary;
- Identifying and mitigating the people related risks to information assets, including those given authorised access to those assets;
- Verification of an organisation's compliance with its own and external cyber security requirements through assessment against relevant policies, standards and guidelines and the provision of constructive feedback aimed at enabling improvement;
- Defining physical security measures necessary to protect cyber assets from accidental or deliberate acts.

The establishment and operation of a properly and appropriately resourced National CyberSecurity Centre enables Government and the private sector to work more effectively together to enhance information security capability and capacity.

Delivering the National CyberSecurity Strategy objectives will require definition of the cyber capabilities required at both national and organisational levels and an assessment of the capability and capacity growth needed.

This requires detailed leadership planning to build and develop the people, processes, information technology and facilities necessary to deliver and maintain a specified capability at the right scale and within the right time frame. Immediate priorities for the newly established National CyberSecurity Centre are:

7.2.1.1 **Leadership and Governance** to:

- Define and maintain the National CyberSecurity Strategy to direct the development of national cyber security capabilities.
- Lead national collaboration and promote information sharing across all national entities to further cyber security and provide authoritative governance.
- Establish the right authoritative leadership and governance and clearly define the membership, lines of communication, roles and responsibilities and empower the Higher CyberSecurity Council to prioritise and coordinate Jordan's approach towards cyber security.
- Ensure that the National CyberSecurity Centre has the authority and skills to influence entities to comply with policies and direction and to intervene where necessary in order to bring entities in line with national priorities, policies and direction.
- Embed the right accountable authorities within entities to take local responsibility for the development and operation of cyber security.

Action Plan	
	1. Identification and appointment of the right people into key leadership roles within the new organisational structures; 2. Development of the terms of reference for each key leader; 3. Establishment of the appropriate authorities for each leader to operate; 4. Establishing appropriate responsible and accountable owners for cyber security at executive leadership and operational levels within entities.

7.2.1.2 **International Collaboration** to:

- Establish appropriate regional and international relations to collaborate effectively with like-minded governments and organisations on cyber-related issues to derive national benefit;
- Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

Action Plan	
	1. Broker international and regional agreements at the most senior levels of Government to collaborate on the appropriate sharing of cyber intelligence; 2. Broker international agreements that enable Jordan to benefit from and contribute to cutting edge cyber research and development; 3. Broker international legal agreements that enable collaboration in bringing cyber criminals to justice; 4. Influence and shape international and regional policies related to cyber security; 5. Broker international and regional agreements on the cyber controls that each country has in place.

7.2.1.3 **Sector Engagement** to:

- Work within and across sectors to develop focused sector understanding of cyber security issues. Communicate and develop sector focused capabilities that enable those issues to be better addressed.
- Understand the different sectors and their unique threat profiles as a product of how they use information, the value of that information to threat actors and the operational systems and services in place.
- Focus cyber security support from the very basic guidance, to intelligence sharing, to the central deployment of active security tools through Security Operating Centres.
- Build trust through engagement across the different sectors and enable appropriate sharing of information and support in line with strategic cyber security priorities.
- Provide certified cyber security-related advice and guidance to support national and organisational entities in achieving the objectives set out in the National CyberSecurity Strategy.

Action Plan	
	1. Create and maintain sector cyber security interest groups for the discussion and exchange of information and intelligence within and between sectors; 2. Identify sector specific cyber security skills gaps and develop a strategy to grow and apply the relevant expertise where it is most strategically important; 3. Develop and implement arrangements for formal downwards sharing of central intelligence and information based on strategic cyber security priorities including threat alerts; **4.** Draw on sector expertise to inform Government strategy and capability.

7.2.1.4 **Education and Training** to:

- Establish an early years curriculum to ensure that we attract, develop and nurture future talent to address the shortage of young people entering the cyber security profession;
- Develop the underpinning education, training and development and career paths for cyber professionals as well as identifying capabilities from commercial sources and partners that can provide capability.

Action Plan	
	1. Establish mechanisms for measuring National Cyber capabilities; 2. Assess the Nation's current Cyber Security capabilities and capacities; 3. Develop national and organisational cyber security capability targets for qualifications, skills, structure and capacity; 4. Prioritise and sequence the development of capabilities in support of the National CyberSecurity Strategy; 5. Assess the most critical gaps that needs addressing as a priority; 6. Learn from international allies about what works and what does not in growing national cyber capability and capacity; 7. Develop a short term plan to buy in the right capabilities where they are needed before they can be developed internally; 8. Procure and deliver international education courses and qualifications to fix near to medium term skills gaps; 9. Develop career paths and benefits that encourage capability direction in support of the National CyberSecurity Strategy; 10. Develop internal education, training and development to grow skills and capacity; 11. Invest in the right technologies and facilities needed to enable the development, establishment and operation of cyber capabilities; 12. Develop national and organisational policies and standards that enable capabilities to be realised 13. Establish appropriate National legal frameworks where appropriate to support the successful development and working of Cyber capabilities.

8 Strategy Milestones for 2023

8.1 Key Milestones

Following on from the success of the 2012 National Information Assurance Cyber Security Strategy, the next key milestones for 2023 are to:

- Clearly define the membership, lines of communication, roles and responsibility, and empower the Higher CyberSecurity Council to prioritise and coordinate Jordan's approach towards cyber security.
- Clearly define the capabilities and establish the Jordanian National CyberSecurity Centre to lead on the implementation of cyber security and development of a national implementation and action plan. Through the establishment of the Jordanian National CyberSecurity Centre, the cyber security capabilities will be established and managed through dedicated cyber Security Operating Centres, across Government, Defence and Security, Finance and Private sectors of business.
- Increase investment in cyber security as a necessity to protect the nation including technology modernisation across government.
- Realise the benefits and continue to grow and share the protection afforded by the existing Governmental and the Defence and Security Computer Emergency Response Teams (JoCERT and JAFCERT).
- Create a robust set of key performance indicators and metrics and establish regular and routine reviews of progress in delivering the strategy.
- Publish a roadmap that shows how the National CyberSecurity Capabilities will be grown in accordance with other e-Government incentives, National Skills and international relationships.

8.2 Measuring Success in Delivering the CyberSecurity Strategy

The disparate definitions of "security incidents," numbers of "vulnerabilities," "threats" or even what's included under "cybersecurity," make the metrics for measuring success in delivering the cyber security strategy very hard.

This strategy will be founded upon a rigorous and comprehensive set of metrics and key performance indicators against which progress towards the outcomes we need to achieve will be measured. As well as being a major deliverable under the Strategy in its own right, the National CyberSecurity Centre will play a crucial role in enabling Government, industry and society to deliver all of these strategic outcomes within this strategy and the monitoring and measurement of success.

9 Conclusion

The Jordan Government appreciates the huge benefits offered by information technology and the online world. This National CyberSecurity Strategy 2018-2023 is presented as a result of the Government's review of the current threats and challenges for information security. Considerable strides have been made since 2012 to mature approaches and implement systematic policy and procedures consistent with international standards that deal effectively with the threats emanating from cyberspace. Risk-understanding is being addressed at the national level to protect Government and Critical Infrastructure.

The National CyberSecurity Strategy for 2023 presents the National Strategic Objectives, the National CyberSecurity Priorities. An implementation road map is now required to ensure and maintain a resilient and trusted cyber space environment that supports National Security, enhances the economy, and builds awareness and trust of citizens towards achieving national prosperity. The six major National Information Security Priorities collectively contribute to achieving the National Strategic Objectives and help to prevent, deter, and protect National Infrastructures against damage or attacks whilst minimizing damage and recovery time from attacks that do occur.

For implementation purposes, the National CyberSecurity Strategy reiterates the need to establish a well-defined national organisation that oversees the efforts required to implement the National CyberSecurity Strategy and its related projects.

It cannot be underestimated how important the National CyberSecurity Strategy is to the future of Jordan and how it under-pins and safeguards the activities of Government and non-governmental organisations, their approach to information assurance and all cyber security related issues.

Annex A – Glossary of Terms and Acronyms

Term	Meaning / Definition
Active Cyber Defence (ACD)	The principle of implementing security measures to strengthen the security of a network or system to make it more robust against attack.
Anonymisation	The use of cryptographic anonymity tools to hide or mask one's identity on the Internet
AI (Artificial Intelligence) Bots	Gamers understand bots as AI characters in a game, while botnets are groups of hijacked computers which cyber criminals use for various tasks such as sending out millions of spam emails or even to attack and attempt to take down websites.
Authentication	The process of verifying the identity, or other attributes of a user, process or device.
Automated system verification	Measures to ensure that software and hardware are working as expected, and without errors.
Autonomous System	A collection of IP networks for which the routing is under the control of a specific entity or domain.
Big data	Data sets which are too big to process and manage with commodity software tools in a timely way, and require bespoke processing capabilities to manage their volumes, speed of delivery and multiplicity of sources.
Bitcoin	A digital currency and payment system.
Commodity malware	Malware that is widely available for purchase, or free download, which is not customised and is used by a wide range of different threat actors.
Computer Network Exploitation (CNE)	Cyber espionage; the use of a computer network to infiltrate a target computer network and gather intelligence.
Controls	Controls are the method by which organisations evaluate potential losses and then take action to implement measures designed to either reduce or eliminate such threats.
Critical Assets	Critical assets are those assets with a high consequence of failure. They are often found as part of a network in which, for example, their failure would compromise the performance of the entire network.
Cryptography	The science or study of analysing and deciphering codes and ciphers; cryptanalysis.

Cyber attack	Deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm.
Cyber crime	Cyber-dependent crime (crimes that can only be committed through the use of ICT devices, where the devices are both the tool for committing the crime and the target of the crime); or cyber–enabled crime (crimes that may be committed without ICT devices, like financial fraud, but are changed significantly by use of ICT in terms of scale and reach).
Cyber Crime marketplace	The totality of products and services that support the cyber crime ecosystem.
Cyber ecosystem	The totality of interconnected infrastructure, persons, processes, data, information and communications technologies, along with the environment and conditions that influence those interactions.
Cyber incident	An occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may require a response action to mitigate the consequences.
Cyber resilience	The overall ability of systems and organisations to withstand cyber events and, where harm is caused, recover from them.
Cyber security	The protection of internetconnected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.
Cyber Security Challenge	Competitions encouraging people to test their skills and to consider a career in cyber.
Cyber threat	Anything capable of compromising the security of, or causing harm to, information systems and internetconnected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means.
Cyber – physical system	Systems with integrated computational and physical components; ‘smart’ systems.
Cyberspace	The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internetconnected devices and embedded processors and controllers. It may also refer to the virtual world or

	domain as an experienced phenomenon, or abstract concept.
Data breach	The unauthorised movement or disclosure of information on a network to a party who is not authorised to have access to, or see, the information.
Domain	A domain name locates an organisation or other entity on the Internet and corresponds to an Internet Protocol (IP) address.
Domain Name System (DNS)	A naming system for computers and network services based on a hierarchy of domains.
Doxing	The practice of researching, or hacking, an individual's personally identifiable information on the Internet, then publishing it.
e-commerce or electronic commerce	Trade conducted, or facilitated by the Internet.
Encryption	Cryptographic transformation of data (called 'plaintext') into a form (called 'cipher text') that conceals the data's original meaning, to prevent it from being known or used.
Horizon scanning	A systematic examination of information to identify potential threats, risks, emerging issues and opportunities allowing for better preparedness and the incorporation of mitigation and exploitation into the policy-making process.
Incident management	The management and coordination of activities to investigate, and remediate, an actual or potential occurrence of an adverse cyber event that may compromise or cause harm to a system or network.
Incident response	The activities that address the short-term, direct effects of an incident, and may also support short-term recovery.
Industrial Control System (ICS)	An information system used to control industrial processes, such as manufacturing, product handling, production and distribution, or to control infrastructure assets.
Industrial Internet of Things (IIoT)	The use of Internet of Things technologies in manufacturing and industry.
Information Security	Information Security (InfoSec) is the practice of defending information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction. Information Security is a general term that can be used regardless of the form that the data may take (e.g. electronic, physical, etc.)

Insider	Someone who has trusted access to the data and information systems of an organisation and poses an intentional, accidental or unconscious cyber threat.
Integrity	The property that information has not been changed accidentally, or deliberately, and is accurate and complete.
Internet	A global computer network, providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.
Internet of Things	The totality of devices, vehicles, buildings and other items embedded with electronics, software and sensors that communicate and exchange data over the Internet.
Malware	Malicious software or code. Malware includes viruses, worms, Trojans and spyware.
Network (computer)	A collection of host computers, together with the sub-network or inter-network, through which they can exchange data.
Offensive cyber	The uses of cyber capabilities to disrupt, deny, degrade or destroy computers networks and internetconnected devices.
Patching	Patching is the process of updating software to fix bugs and vulnerabilities
Penetration testing	Activities designed to test the resilience of a network or facility against hacking, which are authorised or sponsored by the organisation being tested.
Phishing	The use of emails that appear to originate from a trusted source, to deceive recipients into clicking on malicious links or attachments that are weaponised with malware, or share sensitive information, with an unknown third party.
Ransomware	Malicious software that denies the user access to their files, computer or device until a ransom is paid.
Reconnaissance	The phase of an attack where an attacker gathers information on and maps networks, as well as probing them for exploitable vulnerabilities in order to hack them.
Risk	The potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm.
Router	Devices that interconnect logical networks by forwarding information to other networks based upon IP addresses.

Script kiddie	A less skilled individual who uses ready-made scripts, or programs, that can be found on the Internet to conduct cyberattacks, such as web defacements.
Secure by default	The unlocking of the secure use of commodity technologies whereby security comes by default for users.
Secure by design	Software, hardware, systems and networks that have been designed from the ground up to be secure.
SMS spoofing	A technique which masks the origin of an SMS text message by replacing the originating mobile number (Sender ID) with alphanumeric text. It may be used legitimately by a sender to replace their mobile number with their own name, or company name, for instance. Or it may be used illegitimately, for example, to fraudulently impersonate another person.
Social engineering	The methods attackers use to deceive and manipulate victims into performing an action or divulging confidential information. Typically, such actions include opening a malicious webpage, or running an unwanted file attachment.
Spear phishing	Spear phishing is a cyber attack that spoofs emails to gain unauthorised access to sensitive information by targeting specific individuals or organisations. This practice is often referenced alongside other attack vectors as social engineering.
Threat Agent	A Threat Agent is a group or named organisation that is judged to be hostile to Jordanian Government interests. Threat agents are quantified and profiled by intent, capability and perseverance.
Threat Vector	A Threat Vector is a method that may be used by threat agents to attack the organisation. A threat vector may exploit multiple vulnerabilities, both physical and logical, in order to leverage an attack.
Trusted Platform Module (TPM)	An international standard for a secure cryptoprocessor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.
User	A person, organisation entity, or automated process, that accesses a system, whether authorised to, or not.
Virus	Viruses are malicious computer programs that can spread to other files.
Vulnerability	Vulnerability is the state of being vulnerable, exposed, or susceptible to attack.
Water holing	Water holing attacks are attacks in which attackers

	seek to compromise specific groups of users by infecting websites that members of the groups are known to visit with the goal is to infecting the targeted users computers to gain access to the network
Whaling	A whaling attack is a targeted attempt to steal sensitive information from a company such as financial information or personal details about employees, typically for malicious reasons. A whaling attack specifically targets senior management that hold power in companies, such as the CEO, CFO, or other executives who have complete access to sensitive data. Called “whaling” because of the size of the targets relative to those of typical phishing attacks, “whales” are carefully chosen because of their authority and access within the company. The goal of a whaling attack is to trick an executive into revealing personal or corporate data, often through email and website spoofing.