وزارة الاتصالات وتكنولوجيا المعلومات

Ministry of Information and Communications Technology

National Cyber Security Strategy 2018-2023

الاستراتيجية الوطنية للأمن السيبراني 2018-2023

Policies and Strategies Directorate
E-Government Strategies

مديرية السياسات والاستراتيجيات
استراتيجيات الحكومة الالكترونية

1 Foreword

Jordan Government is committed to enhancee its cyber security and, with the publication of its National Information Assurance and Cyber Security Strategy (NIACSS) in 2012, to 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 cyber security 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.

Securing National information assets is vital to us making the best use of such 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 investors and business opportunities.

Since these increased opportunities present new and challenging threats to national cyber security. We must ensure that we tackle these threats effectively in a way that makes best use of our existing capabilities and resources, whilst delivering sustainable sovereign capabilities through the development of our resources.

The 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 Cyber Security Strategy 2018-2023 sets out how Government is going to achieve this vision.

1 تمهيد

تسعى حكومة المملكة الأردنية الهاشمية إلى تعزيز أمنها السيبراني، وقد عملت - من خلال نشر الاستراتيجية الوطنية لضمان أمن المعلومات والأمن السيبراني (NIACSS) للعام 2012- على بيان أولويات الأمن السيبراني سواء للحكومة أو لبيئات الأعمال أو للمواطنين، وقد حان الوقت لمراجعة ما تم إحرازه من تقدم في تحقيق الأهداف الاستراتيجية الخمسة الواردة في الاستراتيجية المذكورة، ومواصلة الجهود نحو تحقيق هذه الأهداف وتحديد الأولويات أولوياتها للسنوات الخمس القادمة على ضوء التهديدات السيبرانية التي تزداد تطوراً وعلى ضوء تطور السياسات الحكومية.

يوفر النمو المُطرّد للتكنولوجيا الرقمية والإنترنت فرصاً جوهرية للتطور في المملكة على الصعيدين المحلي والدولي، كما ويحفز من نمونا. حيث يدعم العالم الرقمي خطط التطور و الازدهار من خلال تعزيز الإدماج المجتمعي وإتاحة الوصول إلى الخدمات الأساسية والتعليم وتوفير فرص العمل والوفرة والنمو الاقتصادي والاستثمار.

ومع ذلك لا يمكن أن ينشأ مجتمع معلومات يتسم بتوفر الخدمات الإلكترونية دون وجود أمن سيبراني فعال، فالفضاء السيبراني الوطني يُعَدّ بيئة عصرية تتطلب حماية ممنهجة وشاملة على المستوى الدولي والمحلي والقطاعي وكذلك على مستوى المؤسسة والفرد.

وعليه؛ فإن حماية الأصول المعلوماتية في المملكة يعّد أمراً بالغ الأهمية لتحقيق الاستفادة القصوى من مثل هذه الفرص، ولضمان أن الفضاء السيبراني في المملكة آمن لكل من يعمل ويقيم فيها، و لجذب المستثمرين الجدد واستحداث فرص استثمارية جديدة.

ولأن هذه الفرص المتزايدة تنشئ تحديات جديدة للأمن السيبراني، فيجب علينا ضمان معالجة كل تحدٍ من هذه التحديات بفعالية وبشكل يحقق الاستغلال الأمثل لقدراتنا ومواردنا الحالية، مع توفير إمكانيات سيادية مستدامة من خلال تطوير مواردنا.

يعتمد نجاح الاستراتيجية الوطنية للأمن السيبراني على الالتزام الفعال من قبل الحكومة والقطاع الخاص والمواطنين بأسس السلامة السيبرانية على المدى البعيد في مواقع العمل وفي المنازل على حد سواء. وعليه، فإن نشر الوعي بهذا المفهوم يعتبر أمراً في غاية الأهمية كما يلعب القطاع الأكاديمي دوراً رئيسياً في التأهيل على أساليب الحماية في بيئة الإنترنت وضمان حصول الكوادر البشرية على الإمكانيات اللازمة لحماية الأمن الوطني والإنجازات الوطنية في مواجهة كل من يستهدف الإضرار بهما.

تحدد الاستراتيجية الوطنية للأمن السيبراني 2018 – 2023 الأدوار المنوطة بالحكومة لتحقيق هذه الرؤية.

2 Introduction

2 المقدمة

This National Cyber Security Strategy (NCSS) 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.

إن هذه الاستراتيجية الوطنية للأمن السيبراني ,والتي ستسري حتى عام 2023، ستستعرض ملخصاً عما تم إحرازه من تقدم في تحقيق الأهداف التي تم وضعها في العام 2012، ولتؤكد على أن اتجاهات التهديدات السيبرانية الحالية تتطلب توجهاً وطنياً أكثر حزماً بهدف ضمان حوكمة الأمن السيبراني.

The use of Cyberspace is transforming business, making it more efficient and effective. It is opening up new 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 the best choice.

يُمكِّن استغلال الفضاء السيبراني في تطوير الأعمال وزيادة فعاليتها وكفاءتها، فهو يؤدي إلى فتح أسواق جديدة ويتيح مزاولة الأعمال التجارية بتكاليف أقل، ودون الارتباط بمكان محدد. كما عزز الفضاء السيبراني إمكانيات خلق الأفكار الجديدة واعتماد نماذج أعمال ابتكارية، ووفر فرصاً جديدة للنمو ولمزاولة الأعمال التجارية سواء بالنسبة للمشاريع القائمة أو الجديدة، وهو أيضاً يسمح للشركات بتحسين تجربة التسوق التي تقدمها إلى زبائنها وتقليل كلفتها، كما ويساعد الافراد على الإحاطة بكافة العروض المتاحة ومقارنة الأسعار والتوصل إلى أفضل خيار ممكن من بين الخيارات المتاحة للشراء.

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.

كما ويساعد العالم الرقمي على الارتقاء بجودة وسرعة النهج الذي تتبعه الحكومة بهدف إشراك المواطنين وقطاعات الأعمال والقطاعات الأكاديمية إذ من شأنه أن يزيد من انسياب المعلومات وأن يطور العمليات الحكومية وأن يحسن من سرعة وجودة تطور السياسات العامة فضلاً عن تطوير أساليب التنسيق والتنفيذ.

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.

تعمل الحكومات حول العالم على توظيف مواردها من أجل التصدي للتهديدات السيبرانية المتنامية التي تزداد تطوراً وتعقيداً. ، فمع تنامي العالم الرقمي تنامت دوافع ذوي النوايا السيئة سواء كانوا من الأطراف الفاعلة الحكومية أو غير الحكومية.

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

ويعمل ذوو الدوافع السيئة بلا كلل أو ملل لتقويض الأصول الرقمية، كما ويسعون إلى إيجاد أساليب جديدة وبسيطة للإخلال بسرية وأمن هذه الأصول والتأثير سلباً على توافرها، ولأن المجرمون السيبرانيون يسعون الى زعزعة ثقة الناس في أمن العالم الرقمي، فإن الأمن السيبراني الفعال عامل أساسي للازدهار الاقتصادي في الأردن.

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. Therefore, for this strategy, the scope of cyber security is taken to include measures against the deployment of 'fake news' by adversaries and other elements of information operations.

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 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.

يستمد الناس في المجتمعات المعاصرة المعلومات بشكل أساسي من وسائل الإعلام بمختلف صورها، ويشكلون آراءهم بناء عليها، ومن شأن التباس الصواب بالخطأ أن يزعزع الثقة بالدولة، كما أن من شأن غياب الثقة على هذا النحو أن يؤثر سلباً على تطبيق القوانين وعلى النظام العام، وعلى الاستثمارات بل وعلى العلاقات الدولية كذلك، وعليه يشمل نطاق الأمن السيبراني لغايات هذه الاستراتيجية التدابير التي تتخذ لغايات مجابهة انتشار الأخبار الزائفة وغير ذلك مما يستهدف المعلومات.

يُعتبر الفضاء السيبراني الآمن عنصراً أساسياً لنجاح ونمو المؤسسات الأردنية ولتعزيز صورة الأردن أمام المنظمات الخارجية كبيئة آمنة لمزاولة الأعمال، وهنالك دور ملقى على كل منا - سواء المؤسسات أو موظفو القطاعين العام أو الخاص فضلاً عن المواطنين- لحفظ الأمن الوطني ودعم التنمية.

وعليه فمن الواجب مجابهة التحديات التي تواجه الأمن السيبراني واستغلال الفرص التي يوفرها، وهو ما يتطلب أعلى درجات القيادة والحوكمة في الفضاء السيبراني.

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.

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 global reliance on networks and emerging technologies and applications 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 التقدم المحرز في تحقيق أهداف استراتيجية عام 2012

سعت الاستراتيجية الوطنية لضمان أمن المعلومات والأمن السيبراني (2012) إلى تحقيق أمن شامل للمعلومات، وقد تطلب تنفيذ الاستراتيجية التعاون بين كافة الجهات المعنية بما في ذلك الحكومة والجهات الأمنية والقطاع الخاص والشركاء الدوليين، وقد أدركت كل هذه الجهات أن المطلوب هو تكامل جهود الجهات المذكورة لا تضاربها، وأنه يتوجب أن تعزز السياسات والاستراتيجيات التي يعتمدها القطاع الخاص الاستراتيجية المذكورة وأن تتوافق وتتناسق معها.

وعليه فقد أكدت الاستراتيجية المذكورة على أن ازدياد الإقبال على التكنولوجيا المبنية على استخدام الإنترنت يعزز فرص التطور الاجتماعي والاقتصادي، ومن شأن ذلك التطور أن يساهم في توفير مزايا هامة للمجتمعات المتصلة بها.

كما قد اتضح على مدى الفترة التي غطتها الاستراتيجية المذكورة بأن تطور اعتماد الدول على الشبكات والتكنولوجيا الناشئة والتطبيقات قد قابلته زيادة في فرص الإضرار في الأنظمة والبيانات.

وقد أصبحت الأنشطة السيبرانية الخبيثة تتخطى الحدود الدولية كنتيجة لتغير المشهد الجيوسياسي حول العالم، فقد أصبح بمقدور مجموعات القرصنة التابعة للدول استغلال فرص الإضرار بالفضاء السيبراني، حيث تعمل هذه المجموعات على توسيع جهودها وتطوير أساليبها الاستراتيجية لتعظيم المكاسب المالية التي تستولي عليها من الأفراد والمؤسسات والمنظمات.

ويقوم الإرهابيون والمتعاطفون معهم بتنفيذ هجمات سيبرانية بدائية في مستواها كما ويسعون كذلك إلى تنفيذ هجمات أكثر تعقيداً في المستقبل.

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;

3.1 البرنامج الوطني للأمن السيبراني

تم وضع البرنامج الوطني للأمن السيبراني للتركيز على تحقيق الأهداف الاستراتيجية والأولويات الوطنية المنصوص عليها في الاستراتيجية الوطنية لضمان أمن المعلومات والأمن السيبراني (2012) وقد أدى تطبيق البرنامج المذكور إلى تحقيق الإنجازات التالية:

- الانتهاء من برنامج تقييم مخاطر الشبكات الحرجة بناءً على المعايير المعتمدة دولياً، ويتم الآن استخدام مخرجات هذا التقييم من أجل تحسين الإجراءات الأمنية الوقائية.
- استغلال مخرجات برنامج تقييم المخاطر لوضع مجموعة من معايير أمن المعلومات والسياسات اللازمة لاعتماد توجه متطور ومتناسق تجاه أمن المعلومات الوطني.

- Created specific national Computer Emergency Response Teams (CERTs) to deliver continuous network monitoring and threat intelligence and incident response capability;
- Delivered a cyber-training programme to enhance the skills of NCP stakeholders and CERT staff;
- to Establish a Public Key Infrastructure (PKI) to manage secure information communication, identity authentication and digital signatures;
- Started establishing an international information security co-operation programme to aid information sharing, exchange lessons learned and enhance capability development.

There have been some challenges in delivering the 2012 strategy, most notably in 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 fully 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 presented in (5.2) 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 challenges.

- إنشاء فرق وطنية للاستجابة لحوادث الأمن السيبراني لتتولى إجراء رقابة دائمة للشبكات ولتقنيات التهديد وإمكانيات الاستجابة للحوادث.
- تنفيذ برنامج تدريبي للأمن السيبراني لتعزيز مهارات الجهات المعنية بالبرنامج وأعضاء الفرق الوطنية للاستجابة لحوادث الأمن السيبراني.
- إنشاء البنية التحتية للمفتاح العام لإدارة تراسل المعلومات والتحقق من الهوية والتوقيع الرقمي بشكل آمن.
- البدء بإنشاء برنامج للتعاون الدولي في مجال أمن المعلومات لدعم تبادل المعلومات والخبرات وتطوير القدرات.

وقد واجه تنفيذ استراتيجية العام 2012 بعض التحديات والتي كان من أبرزها الحاجة إلى إعداد إطار قانوني وتنظيمي ملائم وذلك بسبب التعقيدات في هذا المجال والبعد الدولي للتهديدات المحتملة، فالفضاء السيبراني لا حدود له ومن يسعون إلى تهديده يستغلون هذه الخاصية لإخفاء هوياتهم الحقيقية، ولذلك يتم بناء علاقات متينة مع شركاء دوليين من اجل تطوير عمليات استجابة منسقة بين كافة الشركاء مع الاستمرار بالعمل على المستوى الوطني لتطوير آلية وطنية للاستجابة القانونية والتنظيمية.

برهن نجاح تطبيق البرنامج المذكور على مدار السنوات الخمس الماضية على مدى الالتزام بتحسين الأمن السيبراني بما يوفر أساساً متيناً للانتقال إلى المرحلة التالية من التميز فيه. وقد تم استغلال ذلك فعلاً في تطوير هذه الاستراتيجية بأهداف متجددة وبما يضمن توفير الكفاءات والقدرات بشكل يتناسب مع التهديدات الحالية، وكذلك في تعزيز الإنجازات التي تحققت خلال المرحلة الأولى من الاستراتيجية الوطنية للأمن السيبراني.

تتضمن هذه الاستراتيجية الجديدة الأهداف الاستراتيجية المبينة في البند (5.2) التي تضمن بدورها توفير بيئة معلومات آمنة تسهم في تحقيق المصلحة الوطنية.

تدرك الحكومة بأن التطورات في عالم الإنترنت تستمر بالتسارع بشكل يتجاوز الرؤى السابقة للمستقبل الرقمي والفرص والمخاطر التي تترتب عليه، وقد فرض هذا التسارع في وتيرة التغيير تحدياً في قدرتنا على حماية أنفسنا بالشكل الكافي من التهديدات التي تفرضها التقنيات والتطبيقات الحديثة، وعليه كان لا بد من تحديث الاستراتيجية لمواجهة التحديات المتنامية للأمن السيبراني.

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 organisation's infrastructure and personnel have highlighted the need for an integrated, coordinated, and consistent approach for managing national information security threats.
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 by an insider 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 WikiLeaks disclosures exposing, amongst others, National Security Agency (NSA) and Central Intelligence Agency (CIA) activities and tools;
- The recent 'WannaCry' ransomware attack that seriously affected the UK's National Health Service (NHS) displayed the ease with which cyber-attacks can cripple essential services;
- 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.

Governments, regulators, and societies are increasingly holding public and private organisations to account for practices across the globe. The previous approach of governments and organisations has been to adopt a defensive and reactive stance, hoping that the provision of standards combined with market pressures will improve the security of products and systems. However, experience has shown that this has not provided sufficient cyber protection and 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 واقع التهديدات المتنامية

يواجه الأردن – كحال الحكومات الأخرى على مستوى المنطقة والعالم- تهديدات متنامية، وقد نبّهت الهجمات التي استهدفت مؤخراً حكومات وبنى تحية وموظفين في منظمات عدة إلى الحاجة إلى اعتماد توجه متكامل ومنسق ومتناسق لغايات إدارة تحديات أمن المعلومات الوطني.
تشمل الأحداث التي أبرزت التهديدات المتباينة التي تواجهها الحكومات ما يلي على سبيل المثال لا الحصر:

- تسريبات سنودن (Snowden) التي أظهرت مدى سهولة حذف كميات هائلة من البيانات المصنفة من "شبكة آمنة جداً" من قبل شخص مطلع عليها، وتسريبها للإعلام وللعموم وتيسير استخدامها من قبل وكالات الاستخبارات الأجنبية وغيرها من المنظمات.
- تهديد حقوق الملكية الفكرية الحرجة، والتي قد تشكل كذلك معلومات سرية مصنفة، وقد أدت تسريبات ويكيليكس وغيرها إلى الكشف عن أعمال وأدوات وكالة الاستخبارات المركزية الأمريكية ووكالة الأمن القومي الأمريكي.
- برمجيات الفدية التي ألحقت أضراراً كبيرة، منها على سبيل المثال ما لحق) بهيئة الخدمات الصحية الوطنية البريطانية، وهو ما كشف عن قدرة الهجمات السيبرانية على إعاقة تقديم الخدمات الأساسية للمواطنين بسهولة.
- الهجمات السيبرانية في الشرق الأوسط التي كان يقوم بها القراصنة ويستهدفون قطاعات النفط والغاز والدفاع والأمن وغير ذلك من القطاعات الحساسة.

يزداد توجه الحكومات والجهات التنظيمية والمجتمعات حول العالم نحو مساءلة مؤسسات القطاع العام والخاص عن أفعالها، ففي السابق كانت الحكومات والمؤسسات تتخذ موقفاً دفاعياً يعتمد على الاستجابة بعد وقوع الحدث، وذلك أملاً بالتوصل إلى تحسين أمن المنتجات والأنظمة من خلال اعتماد المواصفات وضغط آليات السوق، إلا أن التجربة قد برهنت إخفاق هذا التوجه في تأمين حماية كافية للفضاء السيبراني وهو ما أدى إلى خسائر اقتصادية وإضرار في سمعة هذه المؤسسات، فضلاً عن التحديات القانونية المتزايدة.

يهدف نطاق التهديدات الذي تتناوله هذه الاستراتيجية إلى تسليط الضوء على مصادر هذه التهديدات ومدى جسامة آثارها على أصول المعلومات وعلى الناس.

4.1 Threat Agents

The Global Cyber threat landscape is driven by the 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 globally to the information assets of governments through direct external attacks on their systems and the subversion of their personnel.

Terrorism and geo-political disruption

The risk of terrorism is a global threat to information, personnel and physical assets through direct physical attacks on facilities, people or assets and increasingly sophisticated cyber-based attacks. Some Nation states seek to undermine regional and national stability by cyber-attacks on critical infrastructure, including energy, transportation, utilities and food and construction and accusations of interference in democratic processes.

Hacktivists

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

Insiders

Humans are the biggest cyber security vulnerability leading to information security breaches either intentionally or unintentionally. 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 Cyber 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.

4.1 جهات التهديد

يؤثر السياق الاجتماعي والسياسي على المشهد العالمي للتهديدات السيبرانية، حيث تعمل جهات التهديد على اكتشاف الثغرات في أمن شبكات المعلومات ومهاجمتها، وفيما يلي أبرز التهديدات التي يمكن أن تؤثر على الأردن:

خدمات الاستخبارات الأجنبية

لا تزال خدمات الاستخبارات الأجنبية (FIS) تمثل أكبر تهديد عالمي لأصول المعلومات الخاصة بالحكومات من خلال الهجمات الخارجية المباشرة على أنظمتها واستهداف موظفي الحكومات بهجماتها.

الإرهاب والاضطرابات الجيوسياسية

يعتبر خطر الإرهاب تهديداً دولياً للمعلومات وللموظفين وللأصول المادية، وذلك من خلال الهجمات المباشرة أو الهجمات السيبرانية المتطورة على المنشآت أو الأصول أو الأشخاص، وتسعى بعض الدول كذلك إلى زعزعة الاستقرار الوطني والإقليمي من خلال الهجمات السيبرانية على البنى التحتية الأساسية، بما فيها مرافق الطاقة والنقل والخدمات العامة والغذاء والإنشاءات، هذا فضلاً عن الاتهامات بالتدخل في العملية الديموقراطية.

القراصنة الناشطون (Hacktivists)

القراصنة الناشطون هم ناشطون يستخدمون الأدوات والوسائل التقنية للوصول غير المصرح به إلى ملفات أو شبكات الحاسوب من أجل دعم أو إيصال رسائل سياسة أو اجتماعية أو أيديولوجية أو دينية من خلال وسائل غير قانونية او قانونيًا.

المطلعون الداخليون (Insider)

يمثل العنصر البشري في مجال الأمن السيبراني أكبر عامل ضعف يؤدي إلى انتهاك أمن المعلومات سواء بقصد أو بغير قصد، حيث يمكن أن تنتج هذه الانتهاكات عن إهمال موظف واحد على الأقل أو عن رغبة موظف ناقم في الإضرار بالمؤسسة أو بموظف آخر بشكل متعمد.

الجريمة والفساد

من المعروف أن جهات التهديد تستخدم جميع وسائل الهجوم الممكنة، إذ يستغل مجرمو الإنترنت على نحو متزايد خصائص السرعة والسهولة والقدرة على إخفاء الهوية على الإنترنت لارتكاب أنشطة إجرامية متنوعة لا تعرف الحدود سواء المادية أو الافتراضية، وهو ما يؤدي إلى أضرار بالغة ويعرض الضحايا لتهديدات حقيقية في جميع أنحاء العالم.

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 have been fragmented approaches to the security of these "things" which has provided an opportunity which hostile actors have been keen to exploit.

Governments and business are increasingly reliant on the Industrial Internet of Things (IIoT) where devices utilise communications technologies to monitor, collect, exchange and analyse large amounts of data to drive better informed and faster decision making.

Ransomware

The popularity of malware capable of encrypting or destroying files as an attack vector has grown steadily as the tactic has proved successful and its use is expected to be a feature of cyberattacks for some time to come.

Artificial Intelligence (AI)

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 financial 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.

4.2 تحديات الأمن السيبراني

من الملاحظ أن الدافع المالي البحت لم يعد الدافع الأوحد للهجمات السيبرانية، حيث نشهد مؤخراً تعاظم الدوافع السياسية الايدولوجية من وراء الهجمات السيبرانية، فيما تُظهِر الهجمات السيبرانية التي حصلت مؤخراً أن دور الحكومة سيزداد أهمية خلال الفترة التي تغطيها هذه السياسة سواء من خلال الأنشطة الخاصة أو من خلال العلاقات مع المواطنين والشركات التجارية الاستثمارية والشركاء الدوليين.

إنترنت الأشياء

يوفر العدد المتزايد من الأجهزة المتصلة بالإنترنت فرصاً متزايدة للنمو الاقتصادي والادماج والحراك المجتمعي والتواصل وإيجاد فرص عمل جديدة، ولا تزال المنهجيات الهادفة إلى تحقيق أمن هذه الأشياء متجزأة، وهو ما يتيح المجال أمام المجرمين السيبرانيين لاستغلال ذلك.

يزداد اعتماد الحكومات والشركات على إنترنت الأشياء الصناعية (IIoT)؛ حيث يُمْكِن للأجهزة استغلال تكنولوجيا الاتصالات لمراقبة وجمع وتبادل وتحليل كميات ضخمة من البيانات من أجل توجيه عملية صنع القرار بشكل أسرع وأفضل.

برمجيات الفدية

نمت شهرة البرمجيات الخبيثة كأحد أدوات الهجوم القادرة على تشفير أو تدمير الملفات بشكل مضطرد بعد أن أُثبِت نجاحها. ومن المتوقع أن يكون استخدامها أحد اهم أشكال الهجمات السيبرانية في المستقبل.

الذكاء الاصطناعي

يستغل المجرمون الذكاء الاصطناعي في نشر إعلانات وإرسال رسائل بريد إلكتروني متصيدة أكثر استقطاباً لفئات محددة في الفضاء السيبراني، وذلك من خلال تحليل كم كبير من المعلومات المتأتية من وسائل التواصل الاجتماعي لتحديد الفئات المستهدفة، من الملاحظ كذلك تزايد استخدام نظام الدردشة على الإنترنت لغايات خدمة الزبائن، وهو ما يكسب هذا النظام ثقة الجمهور، وعليه سيسعى المهاجمون إلى استغلال هذه الثقة وإنشاء منصات دردشة للحصول على بيانات مالية من الناس.

التطبيقات التي لا تعتمد على خوادم

تتعرض المعلومات لخطر كبير نتيجة استخدام تطبيقات لا تعتمد على الخوادم على الأجهزة الشخصية، فعند التخزين على الخوادم يكون مالك المعلومات أكثر قدرة على اختيار الاحتياطات الأمنية الضرورية لضمان الحفاظ على خصوصية بيانات المستخدم لحماية البيانات من سارقي الهوية وغيرهم من المجرمين السيبرانيين، أما مع استخدام التطبيقات التي لا تعتمد على خوادم فتكون تلك الاحتياطات من مسؤولية المستخدم إلى حد كبير.

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 and devices for political or economic gain.

البنية التحتية الحساسة

تعتمد مؤسسات البنية التحتية الحساسة بشكل كبير على أنظمة التحكم الصناعية المتصلة مع بعضها البعض لإدارة مختلف جوانب أعمالها، الأمر الذي يزيد من فرص المهاجمين لاعتراض تلك الأنظمة والأجهزة بهدف الحصول على مكاسب سياسية أو اقتصادية.

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

حملات التصيّد المتطوّرة

يتزايد تطور رسائل التصيّد الإلكترونية التي تُستخدم عادةً لنشر برامج خبيثة أو لتحفيز الضحايا للإفصاح عن بياناتهم الشخصية، خاصةً بعد إضافة معلومات معينة عن الشركة مثل معلومات الفواتير والشؤون اللوجستية وغيرها.

Strategic Use of Information Operations

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

الاستخدام الاستراتيجي لعمليات المعلومات

تعتبر الهجمات وعمليات التجسس السيبرانية ونشر المعلومات المغلوطة (الأخبار الزائفة) من الأدوات المستخدمة بشكل متزايد من قبل بعض الدول والأشخاص لخلق الاضطرابات السياسية والاقتصادية.

Cloud Computing

Organisations increasingly favour cloud technologies that allow them to respond to changing business needs quickly and flexibly. The main challenge is how security and privacy concerns are managed by cloud providers.

الحوسبة السحابية

يزداد تفضيل المؤسسات للتقنيات السحابية التي تسمح بالاستجابة لاحتياجات الأعمال المتزايدة بشكل أكثر سرعة ومرونة، ويكمن التحدي الرئيسي هنا في إدارة مخاوف الأمن والخصوصية من قبل مقدمي الخدمات السحابية.

Cyber Security Awareness

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

الوعي بالأمن السيبراني

لا يزال الوعي العام بالأمن السيبراني محدودا نوعاً ما، مما يُضعف بشكل كبير الجهود المبذولة لحماية المعلومات الحساسة.

Hacker-for-Hire Services

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

خدمات القرصنة مقابل أجر

بسبب توافر الأدوات وسهولة استخدامها وانخفاض تكاليفها، أصبح بإمكان مجموعات القرصنة تقديم خدمات القرصنة مقابل أجر بشكل أسهل من أي وقت مضى.

Skills Shortages

The critical skills shortage of cybersecurity professionals is a global problem that continues to be a major concern for public and private sectors.

نقص المهارات

يعتبر نقص مهارات المهنيين المعنيين بشؤون الأمن السيبراني مشكلة عالمية لا تزال مقلقة للقطاعين العام والخاص.

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 السياق الاستراتيجي

تقر الأهداف الواردة في هذه الاستراتيجية والتي تمت مراجعتها بالتقدم الذي أحرزه البرنامج الوطني للأمن السيبراني في تحقيق أهداف الاستراتيجية الوطنية لضمان أمن المعلومات والأمن السيبراني لعام 2012، وتؤكد على الطموح الوطني في حماية الفضاء السيبراني الأردني من أجل إتاحة الفرصة للحكومة والشركات والمواطنين للمساهمة بشكل أمن بتطوير مجتمع متعدد ومزدهر ويتسم بالشمولية.

5.1 Cyber Security Vision

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

5.1 رؤية الأمن السيبراني

تنص رؤية الأمن السيبراني للمملكة الاردنية الهاشمية على ما يلي:

Vision		الرؤية
	Jordan is confident and secure in the digital world and resilient to cyber threat	**أردن واثق وآمن ضمن العالم الرقمي ومقاوم للتهديد السيبراني**

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

يمكن تحقيق ذلك من خلال تأسيس وتنمية وتطوير الكفاءات الوطنية في مجال الأمن السيبراني والاستجابة الأمنية الملائمة لتحقيق التميز في الأمن الوطني والتجارة والتعاون الدوليين ودعم التحول الحكومي الرقمي لزيادة الرفاه على المستويين الفردي والوطني.

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 الأهداف الاستراتيجية

تبين الأهداف الاستراتيجية الأربعة الغايات الوطنية لتحقيق الأمن السيبراني في الأردن كما وتبين كذلك آلية تحقيقها.

Protect:	**الحماية:**
Enhances trust in and resilience of the Government, Critical National Infrastructure, businesses and the public against cyber threats	**تعزيز الثقة والمرونة لدى الحكومة والبنية التحتية الوطنية الحساسة وقطاعات الأعمال والجمهور لمواجهة التهديدات السيبرانية والتصدي لها، ويتأتى ذلك من خلال:**
● Publishing policies, and procedures to ensure a unified national approach to cybersecurity 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. ● Establish cyber-security awareness and capacity building programs.	● نشر السياسات والإجراءات اللازمة لوضع منهجية وطنية موحدة للأمن السيبراني. ● إنشاء نموذج حوكمة ملائم ومؤسسات تضمن تحقيق الأمن السيبراني الفعال. ● بناء الهيكل المؤسسي اللازم لتطوير وتشغيل الأمن السيبراني الوطني وتوفير مصدر موحد للمشورة على مستوى الحكومة من أجل معالجة التهديدات الاستخباراتية والتثبت من المعلومات. ● إعداد برامج خاصة بنشر الوعي وبناء القدرات في مجال الأمن السيبراني.

Detect:	الكشف والتحري:
Supports understanding and disruption of hostile action taken against the Kingdom and its information assets	**تعزيز فهم واعتراض الأعمال العدوانية التي تستهدف المملكة وأصولها المعلوماتية، وهو ما يتم باعتماد التدابير التالية:**
• Evolving existing cyber threat intelligence capability • Understanding the nations cyber space adversaries and their methods; • Ensuring security defences remain current, effective and continue to detect cyber security events. • Defining what is "normal" for the context and then detect anomalous events using a broad range of skills and capabilities.	• تطوير القدرات الحالية لكشف التهديدات السيبرانية. • فهم طبيعة أعداء الفضاء السيبراني الوطني وأساليبهم. • التأكد من جاهزية الدفاعات الأمنية وفعاليتها واستمرارها في كشف الحوادث الأمنية السيبرانية. • تعريف المستوى الطبيعي في هذا السياق ومن ثم ضبط الحوادث غير الاعتيادية من خلال نطاق واسع من المهارات والقدرات.
Respond:	**الاستجابة:**
Develops and deploys the appropriate capabilities to respond to cyberattacks in the same way as we respond to any other attack on National Security	**تطوير وتوظيف القدرات الملائمة للاستجابة للهجمات السيبرانية بنفس طريقة الاستجابة لأي هجوم آخر ضد الأمن الوطني، وذلك باتخاذ التدابير التالية:**
• 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.	• وضع عمليات وكفاءات ونشاطات لإدارة الحوادث بقصد الحد من الأخطار، بحيث تكون محددةً بعنايةٍ وفعالة. • تقليل واحتواء آثار حوادث الأمن السيبراني. • استعادة الخدمات الأساسية • استخدام التحليل للأسباب الجذرية والأدوات الجنائية بعد وقوع الحوادث من أجل تحسين عمليات الاستجابة.
Evolve:	**التطوّر:**
Develops the knowledge, skills and sustainable sovereign capability required to maintain robust cyber security, through academia, private sector, research and development and international partnerships	**تطوير المعرفة والمهارات والقدرات السيادية المستدامة والملائمة من أجل المحافظة على أمن سيبراني متين من خلال الوسط الأكاديمي والقطاع الخاص والبحث والتطوير بالإضافة إلى الشراكات الدولية، وذلك من خلال:**
• 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 the creation of a National Cyber Academy; • Enacting the legislation and regulation needed to establish and operate National CyberSecurity • 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.	• الشراكة مع المنظمات والشركاء المختصين بهدف التعاون وتبادل المعرفة. • تحديد الشركاء الأكاديميين من أجل تشكيل فريق عمل مؤهل ومتمرس بالإضافة إلى إنشاء أكاديمية وطنية للأمن السيبراني. • تفعيل التشريعات والأنظمة اللازمة لإنشاء وإدارة الأمن السيبراني الوطني. • توفير الأدوات اللازمة لتطوير القدرات السيادية المستدامة والشركات التي يمكنها إطلاق مبادرات فعالة في مجال الأمن السيبراني. • إنشاء قنوات التواصل الوطنية والدولية الملائمة والمتينة.

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 of National Security Threats;
- 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 Government policy in ICT and Postal sectors and key strategic e-Government strategies is vital to the success of the cyber strategy
- 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.

5.3 المبادئ التوجيهية

تستند هذه الاستراتيجية على المبادئ التالية:

- إدارة الحكومة للأمن السيبراني على أعلى المستويات باعتباره أولوية وطنية ملحّة في ظل التهديدات التي يواجهها الأمن الوطني.
- قيام الحكومة بتحديد المستويات الملائمة من نماذج الحوكمة الوطنية والتنسيق والسيطرة لضمان تطبيق نهج تعاوني لتطوير القدرات السيبرانية وتوفير الحماية والاستجابة للأزمات والتعافي منها.
- تحديد أولويات تطبيق تدابير الأمن السيبراني على المؤسسات والأنظمة بناءً على عاملي مقدار المخاطرة وحجم الأثر إذ من غير الممكن أو غير المجدي منع كافة الحوادث السيبرانية.
- اعتبار الأمن السيبراني مسؤولية مشتركة لكافة المؤسسات الحكومية والأكاديمية والشركات التجارية والأفراد.
- المسؤولية القيادية للحكومة في ضمان حماية البنية التحتية الحساسة، سواء أكانت عامة أو مملوكة للقطاع الخاص، من التهديدات السيبرانية.
- بذل جهود كافية لضمان فهم الأفراد لأساليب حماية أنفسهم على الإنترنت.
- اعتبار الربط مع السياسة العامة لقطاعات الاتصالات وتكنولوجيا المعلومات والبريد واستراتيجيات الحكومة الإلكترونية أمراً في غاية الأهمية لإنجاح هذه الاستراتيجية.
- اعتبار ثقافة الأمن السيبراني الإيجابية وتمكين المواطنين والشركات عاملاً مهماً في إنجاح إمكانيات الأمن السيبراني.
- اعتبار إدارة المخاطر الرقمية والتطبيق الملائم للأمن السيبراني من مسؤوليات مجالس إدارة الشركات.
- تضمين الأمن السيبراني بشكل واضح وصريح في جميع القرارات ذات الصلة بالأفراد والقرارات المعنية بالشؤون المادية والتقنية.
- اعتماد الدفاع في العمق وتحقيق الأمان من خلال التصميم كمبادئ جوهرية في تصميم الشبكات والبنى التحتية.

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.

من أجل تحقيق أهداف هذه الاستراتيجية الوطنية المبينة أعلاه، حددت الحكومة الأردنية ست أولويات وطنية أساسية تتطلب كل منها التعاون بين الحكومة والقطاع الخاص والمواطنين فضلاً عن دعم الشركاء الدوليين، وتمثل تلك الأولويات الخطوات الإجرائية لهذه الاستراتيجية.

6 National CyberSecurity Priorities

6 أولويات الأمن السيبراني الوطني

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

تحقيقاً للأهداف الاستراتيجية واستكمالاً لإنجازات الاستراتيجية الوطنية لضمان أمن المعلومات والأمن السيبراني 2012؛ سيتم تطبيق الأولويات التالية بهدف وضع منهجية جديدة وموحدة لآليات تعامل الحكومة وقطاع الأعمال مع الأمن السيبراني، حيث ستنبثق عن هذه الأولويات الأنشطة التي ستباشرها الحكومة خلال مدة تنفيذ هذه الاستراتيجية:

6.1 National CyberSecurity Standards and Policies

6.1 معايير وسياسات الأمن السيبراني الوطني

A national unified approach to cyber security will be supported by the publication of National CyberSecurity Standards and Policies in the form of a Security Policy Framework and managed through a National CyberSecurity Commission.

سيتم العمل على دعم تنفيذ منهجية وطنية موحدة للأمن السيبراني من خلال إصدار معايير وسياسات خاصة بالأمن السيبراني الوطني على شكل إطار للسياسات الأمنية التي ستتولى الهيئة الوطنية للأمن السيبراني إدارتها.

6.2 International Information Security Cooperation Program

6.2 برنامج التعاون الدولي لأمن المعلومات

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

ستستمر حماية وتبادل المعلومات بشكل آمن مع الحكومات الأجنبية والمنظمات الدولية بالتطور من خلال برنامج التعاون الدولي لأمن المعلومات.

6.3 Security Awareness and Capacity Building Program

6.3 برنامج التوعية بالأمن وبناء القدرات

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

سيتم تعزيز الوعي في النواحي الأمنية من خلال التشاور مع الشركاء الأكاديميين والدوليين، هذا فضلاً عن إعداد خبرات محلية مميزة من خلال برامج لبناء القدرات.

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.

6.4 برنامج حماية البنية التحتية الوطنية الحساسة

ستستمر حماية العناصر الأكثر حساسية في البنية التحتية في الأردن بالتطور والنمو من خلال برنامج حماية البنية التحتية الوطنية الحساسة.

6.5 National Computer Emergency Response Teams (CERTs)

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.

6.5 الفرق الوطنية للاستجابة لحوادث الأمن السيبراني

ستتولى فرق الاستجابة لحوادث الأمن السيبراني الوطنية التي سيتم تشكيلها على مختلف مستويات الحكومة والجهات الأمنية والدفاعية والقطاع المالي والبنية التحتية الوطنية الحساسة وعناصر الدعم من القطاع الخاص، مهام إجراء التحليل المنسق وإصدار التحذير من التهديدات السيبرانية والاستجابة للحوادث السيبرانية.

6.6 Legal and Regulatory Reform

As technology outpaces historical legal and regulatory processes, legislative reform will take place to ensure that an effective balance is maintained between security and privacy.

6.6 الإصلاح التنظيمي والقانوني

لأن تطور التقنية أسرع من التطور التاريخي والتشريعي والتنظيمي، سيتم العمل على إصلاح الإطار التشريعي لضمان التوازن الفعال بين الأمن والخصوصية.

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, and to establish the necessary governance to ensure the translation of priorities and objectives into specific well-defined initiatives/projects through:

Ownership

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

Co-ordination

Chaired by the Prime Minister; the Cyber Security Council will have representatives from Government, Defence, Security, Financial Academic and the Private sector. and will coordinate Jordan's approach to meeting the National Strategic Objectives.

Implementation Planning

Implementation of the National CyberSecurity Strategy is complex as the activities will impact several 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 wellbeing.

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 تنفيذ الاستراتيجية

7.1 خطة التنفيذ

يُعتبر إعداد خطة تنفيذية للاستراتيجية أمراً هاماً بقدر أهمية الاستراتيجية الوطنية للأمن السيبراني ذاتها، ذلك أنها تبين الإجراءات اللازمة لتحقيق الأولويات الاستراتيجية وتضع نموذج الحوكمة اللازم لضمان ترجمة الأولويات والأهداف إلى مبادرات ومشاريع مصممة بعناية ومحددة من خلال ما يلي:

المسؤولية

تتولى حكومة المملكة الأردنية الهاشمية إقرار الاستراتيجية الوطنية للأمن السيبراني، مع تأكيد الحكومة على إعطاء هذه الاستراتيجية أقصى درجات الأولوية في تنفيذها على المستوى الوطني.

التنسيق

تشكل الحكومة مجلساً للأمن السيبراني في المملكة يرأسه رئيس الوزراء ويضم ممثلين عن الحكومة وعن المؤسسات الدفاعية والأمنية والقطاع المالي والأكاديمي والقطاع الخاص، وسيقوم المجلس بالعمل على تنسيق المنهجيات الوطنية لتحقيق الأهداف الاستراتيجية الوطنية.

التخطيط للتنفيذ

يعد تنفيذ الاستراتيجية الوطنية للأمن السيبراني عملية مركبة، إذ أن الأنشطة التي سيتم تنفيذها ستؤثر على العديد من المؤسسات، وستتطلب إنشاء عدد من المؤسسات، وعليه سيكون من اللازم إدارة تنفيذ الاستراتيجية من حيث كونها برنامجاً يحتوي عدداً من المشاريع التي تنفذ في عدة مؤسسات.

تحدد خطة العمل الوطنية لتنفيذ هذه الاستراتيجية الإجراءات الواجب اتخاذها على المدى القصير لتعزيز الوعي بالأمن السيبراني وتشجيع كافة الجهات على تبني أفضل إجراءات السيطرة على الأمن الرقمي وتحسين أمن المعلومات وحماية الخصوصية والمحافظة على الأمن والاقتصاد الوطنيين والسلامة العامة.

وعلى المدى الطويل تعزز خطة العمل الاشتراطات المطلوبة لإجراء التحسينات اللازمة على توجهات الأمن السيبراني على مستوى الحكومة والقطاع الخاص وحياة الأفراد كذلك، وسيتم تحديد مراحل مراقبة وقياس التقدم المحرز في تنفيذ الاستراتيجية وتحديداً بخصوص فعالية تدابير أمن المعلومات.

7.2 National CyberSecurity Capabilities

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, 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 Commission, in order to fully realise and manage the National CyberSecurity Strategy. The National CyberSecurity Commission 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 إمكانيات الأمن السيبراني الوطني

يستلزم الوصول بالمملكة إلى حالة النضوج والأمن الرقمي وجود إمكانيات وطنية عالية المستوى من اجل تأسيس وإدارة الأمن السيبراني بفعالية، ويمكن إيجاد تلك الإمكانيات وتنميتها بشكل تدريجي ومتزامن يتوافق مع الأولويات الاستراتيجية لتحقيق الأهداف الاستراتيجية.

تتطلب الإمكانيات الوطنية للأمن السيبراني إيجاد عدد من المؤسسات والوظائف الداعمة والتي ستتطور تدريجياً مع الوقت، والتي من بينها إنشاء هيئة وطنية للأمن السيبراني لتعمل على تطبيق وإدارة الاستراتيجية، وسيكون للهيئة دور مركزي في تنفيذ التوجه الوطني الموحد تجاه الأمن السيبراني، بما في ذلك تطوير الإمكانيات الأساسية التالية في مجال الأمن السيبراني:

- تطوير الاستراتيجية وإعداد السياسات وإنفاذها.
- الاستعداد المؤسسي والتوعية الوطنية السيبرانية.
- المهارات الوطنية والأكاديمية والاستثمار.
- إدارة الحوادث السيبرانية والاستجابة لها.
- المخاطر السيبرانية المتعلقة بالشبكات الحساسة والاستجابة لها.
- إجراء الأبحاث في مجال عمليات كشف وإدارة التهديدات.
- مراقبة الوعي بالوقائع والإبلاغ عنها.
- العلاقات والشراكات الدولية.

7.3 National CyberSecurity Commission

The National Cyber Security Commission 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

7.3 الهيئة الوطنية للأمن السيبراني

تعتبر الهيئة الوطنية للأمن السيبراني مركزاً للتميز في مجال الأمن السيبراني، وتوفير الدفاع السيبراني الفعال لغايات التحري والاستجابة لحوادث الأمن السيبراني، وستعمل كحلقة وصل بين الحكومة وقطاعات الأعمال والقطاعات الأكاديمية والمواطنين لغايات تحقيق أهداف الاستراتيجية.

تتمثل **المسؤوليات الرئيسية للهيئة** بما يلي:

- جمع وتحليل المعلومات والبيانات من مصادر متنوعة للإبلاغ عن تقديرات التهديدات السيبرانية والإعلام عن سلوكيات مجهولي الهوية لغايات التحقيق واتخاذ الإجراءات المناسبة.
- إيجاد الإمكانيات القانونية اللازمة لدعم إدارة جميع المتطلبات القانونية والتنظيمية المتعلقة

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 is 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 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 and 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;

بالأمور الأمنية السيبرانية اللازمة لتنفيذ الاستراتيجية.

- التخطيط الاستراتيجي لتحديد المتطلبات المستقبلية التي قد تؤثر على اتجاهات الأمن السيبراني الاستراتيجي بالإضافة إلى التحقق من الإمكانيات الحالية لضمان تفعيل المستويات المتوقعة من الأمن السيبراني أو لتحديد مجالات التطوير فيها.
- تقييم الأدوات والمنتجات والخدمات السيبرانية من حيث ملاءمتها للاستخدام وتطوير أدوات ومنهجيات جديدة لاستخدامها من قبل المهنيين المختصين في المجال السيبراني في المملكة.
- تطوير المعايير والإرشادات الصحيحة لتحديد التوقعات لجميع عناصر الأمن السيبراني.
- تحديد الأصول الوطنية الحساسة المُهددَّة بالحوادث السيبرانية ذات الأثر الجوهري وإدامة إجراء تقييم للمخاطر التي تتعرض لها تلك الأصول من أجل تحديد وتنفيذ التدابير ذات الأولوية لإدارة المخاطر المُحددة.
- تطوير فهم واضح للبيئة السيبرانية التي تعمل فيها مؤسسات القطاعين العام والخاص وذلك لزيادة الوعي بالتهديدات والتدابير الأمنية السيبرانية.
- توفير آليات لجمع ونشر التنبيهات السيبرانية لكافة موظفي المؤسسات التي تعد مستخدماً نهائياً، مما يُمكن المؤسسات الوطنية من إدارة آثار الحوادث السيبرانية إلى أقصى حد ممكن.
- وضع وتنفيذ منهجية متّسقة وفعالة لإدارة الحوادث السيبرانية لضمان قدرة المؤسسات على احتواء تلك الحوادث واتخاذ الدور القيادي حيثما لزم الأمر.
- تطوير الإمكانيات الوطنية والمؤسسية من أجل تحقيق الاستجابة السريعة للحوادث السيبرانية، وذلك من خلال تطوير الأدوات وتأهيل الأشخاص والعمليات التي يجب أن يتم تفعيلها أثناء حصول الحوادث.
- توفير تقنيات وأساليب التحقيق الفني والجنائي في الحوادث السيبرانية التي يمكن الاعتماد عليها كأدلة للإثبات القانوني عند الحاجة.
- تحديد وتقليل المخاطر التي قد تلحق بالمعلومات، والمتصلة بالعنصر البشري المخوّل رسمياً بالوصول إلى تلك الأصول (المطلعون الداخليون Insiders).

- 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.

- التحقق من امتثال المؤسسات لمتطلبات الأمن السيبراني سواء المتطلبات الخاصة بها أو المتطلبات الخارجية وذلك من خلال تقييم الممارسات على ضوء السياسات والمعايير والتوجيهات وتقديم التغذية الراجعة البنّاءة الهادفة إلى التحسين.
- تحديد التدابير الأمنية المادية اللازمة لحماية الأصول السيبرانية من الأعمال العرضية أو المتعمدة.

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

سيُمكّن إنشاء الهيئة الوطنية للأمن السيبراني وتفعيل دورها كمؤسسة تتمتع بالموارد اللازمة والمناسبة الحكومة والقطاع الخاص من العمل معاً بفعالية أكبر من أجل تعزيز قدرة وكفاءة أمن المعلومات.

Immediate priorities for the newly established National CyberSecurity Commission are:

وتتمثل **الأولويات الملحة للهيئة الوطنية للأمن السيبراني** عند نشأتها بما يلي:

Leadership and Governance to:

القيادة والحوكمة، وذلك لتحقيق الغايات التالية:

- Develop 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.
- Ensure that the National CyberSecurity Commission has the authority and skills to influence entities to comply with policies and direction and to intervene where necessary 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.

- تطوير الاستراتيجية الوطنية للأمن السيبراني وإدامتها لتوجيه عملية تطوير الإمكانيات الوطنية في مجال الامن السيبراني
- قيادة التعاون على المستوى الوطني ودعم تبادل المعلومات بين جميع الجهات الوطنية لتعزيز الأمن السيبراني.
- ضمان تمتع الهيئة الوطنية للأمن السيبراني بالمهارات والصلاحيات الكافية للتأثير على الجهات المختلفة والزامها بالسياسات والتوجهات وللتدخل عند الضرورة بما يكفل التزام مختلف الجهات بالأولويات والسياسات والتوجهات الوطنية .
- تخويل الجهات المناسبة لدى مختلف المؤسسات بالصلاحيات اللازمة لتتولى بدورها تطوير وتفعيل الأمن السيبراني على مستوى المؤسسة لتطوير وإدارة عمليات الأمن السيبراني داخل المؤسسة ومساءلة هذه الجهات.

Action Plan	خطة العمل
1. Identification and appointment of the right people into key leadership roles within the new organisational structures.	1. تحديد وتعيين الأشخاص الملائمين في الأدوار القيادية الرئيسية ضمن هياكل المؤسسات الجديدة
2. Development of the terms of reference for each key leader.	2. تطوير الأحكام المرجعية لكل قائد رئيسي
3. Establishment of the appropriate authorities for each leader to operate.	3. تحديد الصلاحيات الملائمة لكل قائد
4. Establishing appropriate responsible and accountable owners for cyber security at executive leadership and operational levels within entities.	4. تحديد المسؤولين عن الأمن السيبراني ضمن مستويات الإدارة التنفيذية والمستويات التشغيلية ضمن تلك الجهات

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.

التعاون الدولي، وذلك بهدف تحقيق ما يلي:

- إنشاء العلاقات الإقليمية والدولية الملائمة من أجل التعاون بفعالية مع الحكومات والمؤسسات المماثلة فيما يتعلق بقضايا الأمن السيبراني لتحقيق المنفعة الوطنية.
- بناء وإدامة تحالفات وشراكات دولية متينة لردع التهديدات المشتركة وتعزيز الأمن والاستقرار الدولي.

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.

خطة العمل

1. الدخول في الاتفاقيات الإقليمية والدولية على أعلى المستويات الحكومية من أجل التعاون في تبادل المعلومات الاستخباراتية السيبرانية بالشكل المناسب.
2. الدخول في الاتفاقيات الدولية التي تعمل على تمكين الأردن من المساهمة في التطوير والأبحاث السيبرانية الهامة والاستفادة منها.
3. الدخول في الاتفاقيات القانونية الدولية التي تمكن من التعاون في تقديم المجرمين السيبرانيين للعدالة.
4. التأثير على تشكيل السياسات الإقليمية والدولية المتعلقة بالأمن السيبراني.
5. الدخول في الاتفاقيات الإقليمية والدولية المتعلقة بالضوابط السيبرانية المطبقة في كل دولة.

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.

إشراك القطاعات، وذلك بهدف تحقيق ما يلي:

- العمل مع مختلف القطاعات للتوصل إلى فهم قطاعي مركزي لقضايا الأمن السيبراني وتطوير قدرات قطاعية مركزة تمكن من التعامل مع تلك القضايا بالشكل الأمثل.
- تفهم مختلف القطاعات وأشكال التهديد الخاصة بكل قطاع منها وذلك انطلاقاً من أن التهديد يعد نتيجة لأسلوب استعمال تلك القطاعات للمعلومات ولقيمة تلك المعلومات بالنسبة لجهات التهديد والأنظمة التشغيلية والخدمات المطبقة.
- تركيز دعم الأمن السيبراني بدءاً من مرحلة الإرشاد الأساسي، مروراً بتشارك المعلومات الاستخباراتية ووصولا إلى إطلاق أدوات أمنية مركزية من خلال مراكز العمليات الأمنية.
- بناء الثقة من خلال المشاركة في مختلف القطاعات وتمكين المشاركة المناسبة للمعلومات والدعم بما يتوافق مع الأولويات الاستراتيجية للأمن السيبراني.
- توفير المشورة والإرشادات المؤهلة المتعلقة بالأمن السيبراني لدعم المؤسسات الوطنية في تحقيق أهدافها المنصوص عليها في هذه الاستراتيجية.

Action Plan		خطة العمل
1. Create and maintain sector cyber security interest groups for the discussion and exchange of information and intelligence within and between sectors.	1. إنشاء وإدامة مجموعات قطاعية مهتمة بالأمن السيبراني؛ لمناقشة وتبادل المعلومات والاستخبارات داخل القطاع ذاته وفيما بين القطاعات المختلفة.	
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	2. تحديد الفجوات في مهارات أمن المعلومات الخاصة ضمن كل قطاع وإعداد استراتيجية لبناء وتطبيق الخبرة المكتسبة حيثما يكون لذلك أهمية استراتيجية.	
3. Develop and implement arrangements for formal downwards sharing of central intelligence and information based on strategic cyber security priorities including threat alerts	3. تطوير وتنفيذ ترتيبات المشاركة الرسمية البينية للاستخبارات المركزية والمعلومات على المستوى الأساسي بناءً على الأولويات الاستراتيجية الخاصة بالأمن السيبراني بما في ذلك إخطارات التهديد.	
4. Draw on sector expertise to inform Government strategy and capability.	4. الاعتماد على الخبرة المكتسبة لكل قطاع لرفد الاستراتيجيات والقدرات الحكومية.	

Education and Training to:

التعليم والتدريب لتحقيق ما يلي:

- Establish a school curriculum to ensure that we attract, develop and nurture future talent to address the shortage of young people entering the cyber security profession;
- تطوير مناهج دراسية هدفها جذب وتطوير وتغذية المواهب المستقبلية لمعالجة النقص في أعداد الشباب المنخرطين في المهن المتعلقة بالأمن السيبراني.
- 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.
- تطوير التعليم والتدريب والمسارات المهنية للمهنيين العاملين في قطاع الأمن السيبراني وتحديد الكفاءات لدى المؤسسات التجارية والشركاء ممن يمكنهم تقديم هذه الكفاءات.

Action Plan		خطة العمل
1. Establish mechanisms for measuring National Cyber capabilities;	1. وضع آليات قياس القدرات الوطنية السيبرانية	
2. Assess the Nation's current Cyber Security capabilities and capacities;	2. تقييم كفاءات وقدرات الأمن الوطني السيبراني الحالية	
3. Develop national and organisational cyber security capability targets for qualifications, skills, structure and capacity;	3. تطوير أهداف الإمكانيات الوطنية والمؤسسية للأمن السيبراني من حيث المؤهلات والمهارات والهياكل والقدرات.	
4. Prioritise and sequence the development of capabilities in support of the National CyberSecurity Strategy;	4. تحديد أولويات وتسلسل تطوير الإمكانيات في دعم الاستراتيجية الوطنية للأمن السيبراني	
5. Assess the most critical gaps that needs addressing	5. إعطاء الأولوية لتقييم الثغرات الأكثر أهمية ومعالجتها.	

as a priority;

6. Learn from international allies about what works and what does not in growing national cyber capability and capacity;

6. الاستفادة من الحلفاء الدوليين في تطوير الكفاءة السيبرانية الوطنية من حيث التعرف على الأساليب الناجعة لهذه الغاية

7. Develop a short-term plan to buy in the right capabilities where they are needed before they can be developed internally;

7. تطوير خطة قصيرة المدى لاستقطاب الكفاءات الضرورية داخلياً لسد مواطن الحاجة إلى حين التمكن من تأهيل الكفاءات داخلياً.

8. Procure and deliver international education courses and qualifications to fix near to medium term skills gaps;

8. استقطاب وتطوير المساقات التعليمية الدولية والمؤهلات من أجل إصلاح الثغرات في المهارات على المدى شبه المتوسط.

9. Develop career paths and benefits that encourage capability direction in support of the National CyberSecurity Strategy;

9. تطوير المسارات الوظيفية والحوافز التي تعمل على تشجيع وتوجيه الكفاءات لدعم الاستراتيجية.

10. Develop internal education, training and development to grow skills and capacity;

10. تطوير التعليم والتدريب الداخلي لتنمية المهارات والكفاءات

11. Invest in the right technologies and facilities needed to enable the development, establishment and operation of cyber capabilities;

11. الاستثمار في التكنولوجيات والمرافق اللازمة لتمكين تطوير وإنشاء وتشغيل الكفاءات السيبرانية

12. Develop national and organisational policies and standards that enable capabilities to be realised

12. تطوير السياسات والمعايير الوطنية والمؤسسية التي تعمل على بناء الكفاءات وتمكينها

13. Establish appropriate National legal frameworks where appropriate to support the successful development and working of Cyber capabilities.

13. إنشاء الأطر القانونية الوطنية الملائمة حيثما أمكن لدعم التطوير الناجح للكفاءات السيبرانية وأدائها لعملها.

8 Strategy Milestones for 2023

8.1 Key Milestones

The key milestones for this Strategy are as follows:

- Clearly define the membership, lines of communication, roles and responsibility, and empower the CyberSecurity Council to prioritise and coordinate Jordan's approach towards cyber security.
- To establish the Jordanian National CyberSecurity Commission that will lead on the implementation of cyber security and development of a national implementation and action plans, and the development of the needed capabilities. The Commission will be operating across Government, Defence and Security, Finance and Private sectors.
- 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- initiatives, 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 has been 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 Commission will play a crucial role in enabling Government, industry and society to deliver all these strategic outcomes within this strategy and the monitoring and measurement of success.

8 معالم الاستراتيجية حتى العام 2023

8.1 المعالم الرئيسية

ستكون المعالم الرئيسية لهذه الاستراتيجية على النحو الآتي:

- تحديد آلية الانتساب إلى مجلس الأمن السيبراني وطرق التواصل معه والأدوار والمسؤوليات المنوطة به؛ وتمكينه من تحديد الأولويات وتنسيق المنهجية الأردنية تجاه الأمن السيبراني.
- إنشاء الهيئة الوطنية الأردنية للأمن السيبراني لتتولى قيادة تطبيق الأمن السيبراني الوطني وتطوير وتنفيذ خطط العمل الوطنية وكذلك تطوير الكفاءات اللازمة، وستعمل الهيئة على مستوى الحكومة والجهات الدفاعية والأمنية والقطاعات المالية والقطاع الخاص.
- زيادة الاستثمار في الأمن السيبراني بما يضمن حماية المصالح الوطنية بما في ذلك تحديث التكنولوجيا في القطاع الحكومي.
- تحقيق الفوائد ومتابعة التطوير والتشارك في الحماية التي تُقدمها الفرق الحكومية وفرق المؤسسات الدفاعية وفرق الاستجابة لحوادث الأمن السيبراني الحالية التابعة للجهات الحكومية والأجهزة الأمنية (JoCERT, JAFCERT)).
- وضع مجموعة شاملة من مؤشرات الأداء الرئيسية والمقاييس وإجراء مراجعات دورية ومنتظمة للتقدم المُحرز في تحقيق أهداف الاستراتيجية.
- إصدار خارطة طريق لتبين أسلوب تنمية وتطوير الإمكانيات الوطنية في مجال الأمن السيبراني وفقاً للمبادرات الإلكترونية الأخرى والمهارات الوطنية والعلاقات الدولية.

8.2 قياس مدى النجاح في تحقيق الأهداف الاستراتيجية الوطنية للأمن السيبراني

إن التفاوت والتباين في تعريف "الحوادث الأمنية" وعدد "الثغرات" و"التهديدات" بل وحتى ما يندرج تحت "الأمن السيبراني" يجعل من وضع معايير لقياس النجاح في إحراز التقدم نحو إنجاز هذه الاستراتيجية أمراً في غاية الصعوبة.

لذلك فقد تم إعداد هذه الاستراتيجية بناءً على مجموعة محددة وشاملة من المقاييس ومؤشرات الأداء الرئيسية التي ستُستخدم لقياس التقدم المحرز في سبيل تحقيق النتائج المرجوة. وستلعب الهيئة الوطنية للأمن السيبراني (التي تعد بحد ذاتها واحداً من أهم مخرجات الاستراتيجية) دوراً أساسياً في تمكين الحكومة والقطاع والمجتمع من تحقيق هذه النتائج الاستراتيجية ضمن هذه الاستراتيجية ومراقبة وقياس مدى نجاحها.

9 Conclusions

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 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.

9 الاستنتاجات

تقدر الحكومة المنافع الكبرى التي تحققها تقنيات المعلومات وعالم الإنترنت، وعليه فقد تم اقتراح الاستراتيجية الوطنية للأمن السيبراني (2018-2023) بعد مراجعة الحكومة للتهديدات والتحديات الحالية التي تواجه أمن المعلومات.

منذ العام 2012، تم اتخاذ خطوات حقيقية وملموسة للوصول إلى منهجيات متكاملة، كما وتم تنفيذ سياسات وإجراءات منتظمة ومتسقة مع المعايير الدولية التي تتعامل بفعالية مع التهديدات التي تنشأ عن الفضاء السيبراني، ويجري كذلك تحديد وفهم المخاطر والتهديدات وطرق التعامل معها على المستوى الوطني من أجل حماية المؤسسات الحكومية والبنية التحتية الوطنية الحساسة.

تحدد هذه الاستراتيجية الأهداف الاستراتيجية الوطنية و الأولويات اللازمة للأمن السيبراني الوطني.

تطلب هذه الاستراتيجية إعداد خارطة طريق تنفيذية تضمن وجود بيئة فضاء سيبراني موثوقة عالية الاستجابة، تدعم الأمن الوطني وتعزز الاقتصاد وترفع الوعي ومستوى الثقة لدى المواطنين، وتسهم الأولويات الرئيسية الوطنية الست لأمن المعلومات مجتمعة في تحقيق الأهداف الاستراتيجية الوطنية وكذلك في منع وتخفيف الأضرار أو الهجمات التي تستهدف البنى التحتية الوطنية الحساسة وحمايتها مع تقليل الزمن اللازم للتعافي من الهجمات والأضرار الناجمة عنها في حال وقوعها.

لغايات التنفيذ؛ تؤكد الاستراتيجية على الحاجة لإنشاء هيئة وطنية تشرف على الجهود المطلوبة لتنفيذ هذه الاستراتيجية والمشاريع المرتبطة بها

لا يمكن إغفال أهمية الدور الذي ستلعبه هذه الاستراتيجية في رسم مستقبل الأردن وتعزيز وحماية أنشطة وممارسات المؤسسات الحكومية وغير الحكومية والمنهجية المتبعة في ضمان أمن المعلومات وجميع المسائل المتعلقة بالأمن السيبراني.

Annex A – Glossary of Terms and Acronyms		الملحق أ – قاموس المصطلحات الاختصارات	
Term	**Meaning / Definition**	**المعنى / التعريف**	**المصطلح**
Active Cyber Defence (ACD)	The principle of implementing layered security measures to strengthen the security of a network or system to make it more robust against attack.	مبدأ تنفيذ التدابير الأمنية على مستويات من أجل تعزيز أمن الشبكة أو النظام وجعله منيعاً ضد الهجمات.	**الدفاع السيبراني الفعال**
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.	يُعرّف اللاعبون البرامج على أنها شخصيات الذكاء الاصطناعي في اللعبة بينما تعتبر شبكات البرامج مجموعات من الحواسيب المسروقة، يستخدمها المجرمون السيبرانيون لغايات عدة منها إرسال ملايين رسائل البريد الإلكترونية المؤذية أو حتى تعطيل المواقع الإلكترونية.	**روبوتات الويب المصنعة بالذكاء الاصطناعي**
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.	مجموعات البيانات الكبيرة جداً إلى الحد الذي يستحيل معه معالجتها وإدارتها من خلال أدوات البرمجيات المتاحة عادة بشكل اعتيادي، بحيث تتطلب إمكانيات معالجة متخصصة لغايات إدارة أحجامها وتمكين تعدد المصادر وتحقيق السرعة في التسليم.	**البيانات الضخمة**
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.	الأساليب التي بموجبها تُقيم المؤسسات الخسائر المحتملة ومن ثم تتخذ إجراءً لتنفيذ التدابير المصممة إما لتقليل تلك التهديدات أو إزالتها.	**أساليب التحكم**
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.	الأصول التي يترتب على تعطلها عواقب وخيمة، وتكون هذه الأصول غالباً جزءاً من شبكة يؤدي توقفها عن العمل -على سبيل المثال- إلى تعطيل أداء الشبكة بأكملها.	**الأصول الحساسة**
Cyber attack	Deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm.	الاستغلال المتعمد لأنظمة الحاسوب والمؤسسات التي تعتمد على العالم الرقمي والشبكات من أجل إلحاق الضرر.	**الهجمات السيبرانية**
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).	الجرائم التي تعتمد على الفضاء السيبراني (الجرائم التي يمكن ارتكابها فقط من خلال استخدام أجهزة الاتصالات وتكنولوجيا المعلومات؛ حيث تكون الأجهزة هي أداة ارتكاب الجريمة والهدف منها)، أو الجرائم التي يمكّن الفضاء السيبراني من ارتكابها (وهي الجرائم التي يمكن ارتكابها دون استخدام أجهزة الاتصالات وتكنولوجيا المعلومات كالاحتيال المالي، ولكنها تتغير بشكل كبير من حيث النطاق وحجم الوصول عند استخدام أجهزة الاتصالات وتكنولوجيا المعلومات).	**الجريمة السيبرانية**
Cyber Crime marketplace	The totality of products and services that support the cyber-crime ecosystem.	مجموعة المنتجات والخدمات التي تدعم النظام البيئي للجرائم السيبرانية.	**سوق الجرائم السيبرانية**

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.	الحادثة التي تشكل خطراً فعلياً أو محتملاً على الحاسوب أو الأجهزة المتصلة بالإنترنت أو الشبكات أو البيانات التي تمت معالجتها أو تخزينها أو نقلها على تلك الأنظمة والتي قد تتطلب خطة استجابة للتخفيف من العواقب أو الآثار.	**الحوادث السيبرانية**
Cyber resilience	The overall ability of systems and organisations to withstand cyber events and, where harm is caused, recover from them.	القدرة الإجمالية للأنظمة والمؤسسات على التعامل مع الأحداث السيبرانية والتعافي من أضرارها إذا وقعت.	**المرونة السيبرانية**
Cyber security	The protection of connected 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.	حماية بيئة الفضاء السيبراني (التي تتكون من الأجهزة والبرمجيات والبنى التحتية المرتبطة بها) وكافة البيانات الموجودة فيها والخدمات التي تقدمها من الوصول إليها بشكل غير قانوني، أو من سوء الاستخدام أو الضرر، سواء لضرر المتعمد الذي يسببه مشغل النظام، أو الضرر الحاصل بطريق الخطأ نتيجة عدم اتباع الإجراءات الأمنية أو بنتيجة التعرض للخداع بقصد التسبب بالضرر المذكور.	**الأمن السيبراني**
Cyber threat	Anything capable of compromising the security of, or causing harm to, information systems and internet connected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means.	أي شيء يمكنه التأثير على الأمن أو التسبب بالضرر لأنظمة المعلومات والأجهزة المتصلة بالإنترنت (والتي تشمل الأجهزة والبرمجيات والبنية التحتية المتصلة) والبيانات الموجودة عليها والخدمات التي تقدمها، وبشكل أساسي عن طريق وسائل سيبرانية.	**التهديد السيبراني**
Cyberspace	The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet connected devices and embedded processors and controllers.	شبكة عالمية مترابطة مكونة من البنى التحتية لتكنولوجيا المعلومات والتي تشتمل على الإنترنت وشبكات الاتصالات وأنظمة الحواسيب والأدوات المتصلة بالإنترنت والمعالجات المدمجة (المضمنة) وأنظمة التحكم.	**الفضاء السيبراني**
e-commerce or electronic commerce	Trade conducted or facilitated by the Internet.	التجارة التي تتم عبر الإنترنت أو التي تسهل الإنترنت مزاولتها.	**التجارة الإلكترونية**
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.	إدارة وتنسيق أنشطة التحري ومعالجة وقوع أو احتمال وقوع حادثة سيبرانية سلبية الأثر يمكن أن تؤثر على نظام أو شبكة أو تسبب لهما الضرر.	**إدارة الحوادث**
Incident response	The activities that address the short-term, direct effects of an incident, and may also support	الأنشطة التي تتناول التأثيرات المباشرة للحادثة ودعم التعافي منها على المدى القصير.	**الاستجابة للحوادث**

	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.	نظام معلومات يستخدم للتحكم بالعمليات الصناعية مثل التصنيع والتعامل مع المنتج والإنتاج والتوزيع أو للتحكم بأصول البنية التحتية	**أنظمة التحكم الصناعية**
Industrial Internet of Things (IIoT)	The use of Internet of Things technologies in manufacturing and industry.	استخدام تكنولوجيات إنترنت الأشياء في المجال الصناعي.	**الإنترنت الصناعي للأشياء**
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.)	ممارسات حماية المعلومات من الدخول والاستخدام والإفصاح والنشر والتعديل والتفحص والتحقق والتسجيل أو الإتلاف غير المرخص. أمن المعلومات هو مصطلح عام يمكن استخدامه بصرف النظر عن شكل البيانات سواء كانت ملموسة أو إلكترونية أو غيرها.	**أمن المعلومات**
Insiders	Someone who has trusted access to the data and information systems of an organisation and poses an intentional, accidental or unconscious cyber threat.	الشخص الذي يُخول بالدخول إلى أنظمة المعلومات والبيانات الخاصة بمؤسسة ويشكل تهديداً سيبرانياً مقصوداً أو عرضياً.	**المطلعون الداخليون**
Integrity	The property that information has not been changed accidentally, or deliberately, and is accurate and complete.	خاصية تدل على أن المعلومات لم تتعرض للتغيير عرضياً أو بشكل مقصود وهي كاملة وصحيحة	**السلامة**
Internet	A global computer network, providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.	شبكة حاسوب عالمية تقدم معلومات متنوعة وتسهيلات اتصال، وهي تتكون من شبكات متصلة باستخدام برتوكولات الاتصال القياسية	**الإنترنت**
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.	مجموع الأجهزة والمركبات والمباني وغيرها من الأشياء التي تحتوي على إلكترونيات وبرمجيات ومستشعرات تتواصل وتعمل على تبادل البيانات عبر الإنترنت.	**إنترنت الأشياء**
Network (computer)	A collection of host computers, together with the sub- network or inter-network, through which they can exchange data.	مجموعة من الحواسيب المستضيفة والشبكات الداخلية أو الفرعية والتي يمكن من خلالها تبادل البيانات.	**شبكة الحاسوب**
Offensive cyber	The uses of cyber capabilities to disrupt, deny, degrade or destroy computers networks and internet connected devices.	استخدام الإمكانات السيبرانية لإعاقة أو تقليل أو حجب كفاءة شبكات الحاسوب والأجهزة المتصلة بالإنترنت أو تدميرها.	**الهجوم السيبراني**
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	استخدام رسائل البريد الإلكتروني التي تبدو بأنها صادرة عن مصدر موثوق لتضليل المرسل إليهم ودفعهم للنقر على الروابط أو المرفقات الخبيثة المتضمنة لبرمجيات ضارة، أو لمشاركة المعلومات الحساسة مع	**التصيّد**

	malware, or share sensitive information, with an unknown third party.	طرف ثالث مجهول.	
Ransomware	Malicious software that denies the user access to their files, computer or device until a ransom is paid.	برمجيات خبيثة تمنع المستخدم من الدخول إلى ملفاته أو حاسوبه أو جهازه لحين دفع فدية	**برمجيات الفدية**
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.	مرحلة من الهجوم يقوم فيها المهاجم بجمع المعلومات عن الشبكات ومسحها للتوصل إلى نقاط الضعف القابلة للاستغلال فيها لغايات مهاجمتها.	**الاستطلاع**
Risk	The potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm.	احتمالية قيام تهديد سيبراني محدد باستغلال نقاط الضعف في نظام معلومات وإلحاق الضرر.	**الخطر**
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.	شخص يتمتع بقدر من المهارات ويستخدم نصوصاً أو برامج جاهزة يمكن العثور عليها على الإنترنت لشن الهجمات السيبرانية مثل هجمات الشبكة.	**هاكر النصوص الجاهزة (مبتدئ)**
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.	الطرق التي يستخدمها المهاجمون لخداع الضحايا وحملهم على للقيام بفعل ما أو الحصول على معلومات سرية، وعادة ما تشمل تلك الأعمال فتح صفحة إنترنت خبيثة أو تشغيل مرفق لملف غير مرغوب.	**الهندسة الاجتماعية**
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.	هجوم سيبراني يتمثل بإرسال رسائل بريد إلكتروني بقصد الوصول بشكل غير قانوني إلى معلومات حساسة من خلال استهداف أفراد أو مؤسسات محددة. غالباً ما يُشار إلى هذا العمل- إلى جانب موجهي الهجمات الآخرين- بمصطلح الهندسة الاجتماعية	**التصيد الاحتيالي**
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.	مجموعة أو منظمة تعتبر معادية لمصالح الحكومة الأردنية، ويُصنف ممثلو التهديد وفقاً للنوايا والكفاءة وتكرار الهجمات.	**جهات التهديد**
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.	طريقة يمكن أن يستخدمها ممثل التهديد لمهاجمة مؤسسة. ويمكنه كذلك استغلال نقاط الضعف المتعددة المادية والمنطقية لشن الهجوم.	**موجّه التهديد**
User	A person, organisation entity, or automated process, that accesses a	الشخص أو المؤسسة أو المنشأة أو العملية الأوتوماتيكية التي تقوم بالدخول إلى النظام	**المستخدم**

	system, whether authorised to, or not.	سواء كان بشكل مرخص أو غير مرخص.	
Vulnerability	Vulnerability is the state of being vulnerable, exposed, or susceptible to attack.	حالة الانكشاف أو القابلية للتعرض للهجوم.	**الثغرات**
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 infect the targeted users' computers to gain access to the network	هجمات يسعى فيها المهاجمون إلى التأثير على مجموعات خاصة من المستخدمين من خلال التأثير على المواقع الإلكترونية التي يُعرف أن أعضاء تلك المجموعات يكررون زيارتها بهدف الإضرار بحواسيب المستخدمين المستهدفة، وذلك بقصد التمكن من الدخول إلى الشبكة.	**هجمات الثقوب**
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.	محاولة موجهة تستهدف سرقة معلومات حساسة من مؤسسة ما، مثل المعلومات المالية أو تفاصيل الموظفين الشخصية عن لغايات خبيثة عادة، ويستهدف احتيال صيد الحيتان بشكل خاص الإدارة التنفيذية العليا في المؤسسات مثل الرئيس التنفيذي والمسؤول المالي أو غيرهم من المسؤولين التنفيذيين الذين يمكنهم الوصول إلى البيانات كاملة. وقد أطلق عليها هذا الاسم نسبة إلى حجم أهداف تلك الأنواع من هجمات التصيّد حيث تم استخدام كلمة "الحيتان" بالنظر إلى حجم صلاحيات الأشخاص المستهدفين وإمكانيات الوصول التي يتمتعون بها داخل المؤسسة، ويكون الهدف من هجوم صيد الحيتان هو خداع المسؤولين التنفيذيين للكشف عن البيانات الشخصية أو بيانات المؤسسات، ويتم الهجوم عادة من خلال الخداع عبر البريد الإلكتروني أو الموقع الإلكتروني	**احتيال صيد الحيتان**