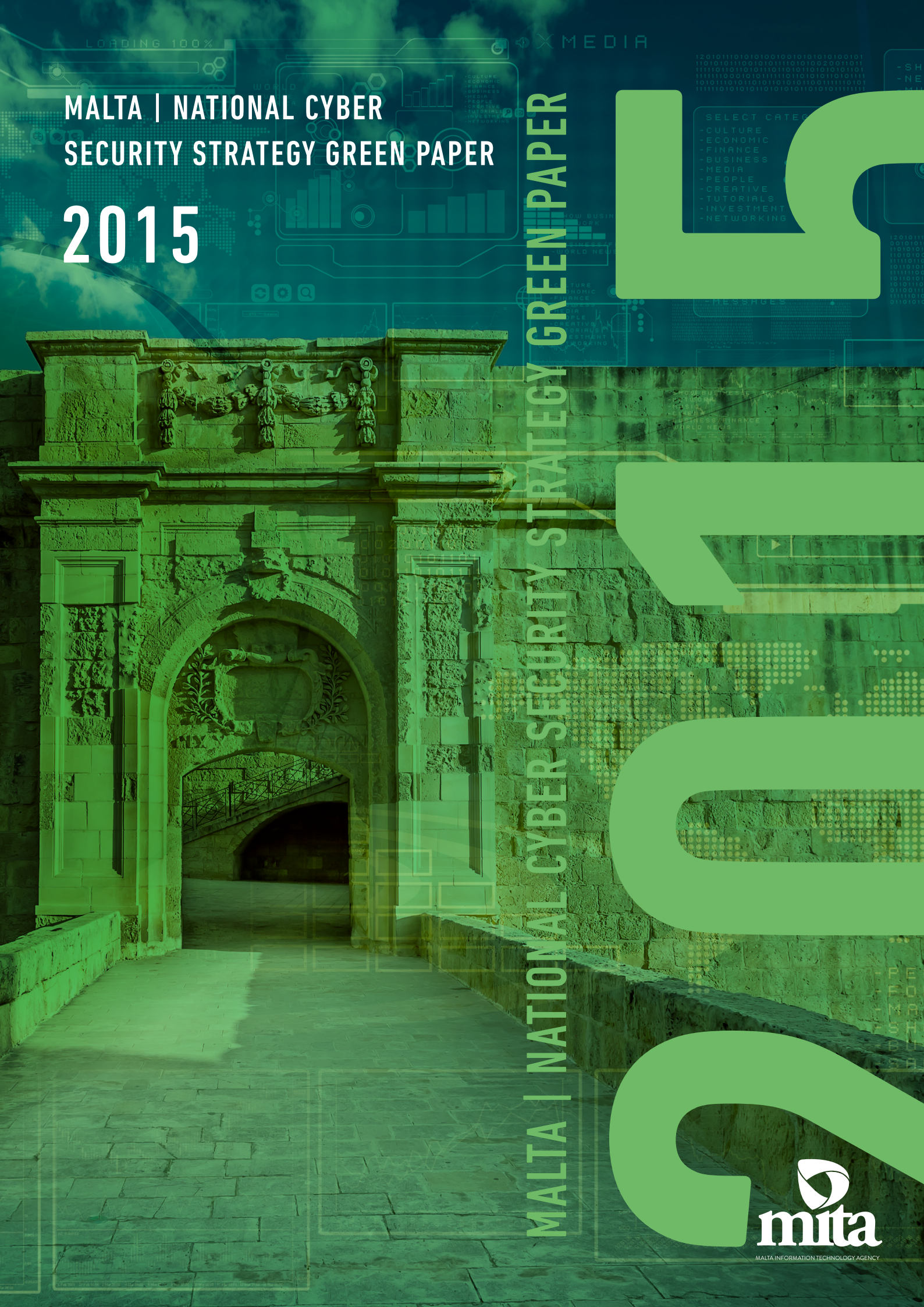
MALTA | NATIONAL CYBER SECURITY STRATEGY GREEN PAPER

2015



MALTA | NATIONAL CYBER SECURITY STRATEGY GREEN PAPER

mita

MALTA INFORMATION TECHNOLOGY AGENCY

MALTA | NATIONAL CYBER SECURITY STRATEGY GREEN PAPER

2015

CONTENTS

MINISTER'S FOREWORD

THE FIRST STEP TOWARDS POSITIONING CYBER SECURITY AS ANOTHER INVESTMENT TOWARDS THE WELL-BEING OF THE MALTESE ECONOMY FROM WHICH WE CAN ALL BENEFIT.

There is no doubt that Information and Communications Technology (ICT) has revolutionised the way that business is conducted; enhancing business effectiveness, widening competitive opportunities and generating opportunities for innovation within our national economy in the process. Indeed, Information and Communications Technology is, today, a key investment for the Malta's economic well-being.

However, threats to the safe and secure use of Information and Communications Technology are not to be under-estimated. Hence the need to safeguard one of Malta's key economic pillars using a holistic and methodological approach on an ongoing basis.

It is in this light that the Green Paper for a National Cyber Security Strategy has been prepared for feedback and consultation on a national scale. It proposes a way forward, based upon key goals and measures that focus on the need for related awareness, knowledge, expertise, good practice, regulatory and legislative updates as well as cooperation and collaboration on a national, European and on a global basis.

Ultimately, it is the first step towards positioning cyber security as another investment towards the well-being of the Maltese economy from which we can all benefit.

Hon. Dr. Chris Cardona

Minister for the Economy, Investment and Small Business

EXECUTIVE SUMMARY

THIS GREEN PAPER, ALONG WITH ITS SUPPORTING DOCUMENT INTENDS TO INCULCATE AN AWARENESS OF CYBER SECURITY, ITS EXTENT AND ITS IMPLICATIONS WHICH MALTA NEEDS TO CONSIDER.

"THE STRATEGIC DIRECTION OF THE GREEN PAPER PROPOSES 6 GOALS, EACH CARRYING A NUMBER OF MEASURES"

Malta's day to day interactivity, within and beyond its shores, is increasingly dependent upon the use of Information and Communications Technology (ICT), to the extent that its disruption may affect service, business and potentially, life. Inherently, the technology, its logical and physical constituent elements, the data it carries, as well as its users, which together constitute cyber space - are far from perfect. Cyberspace is thus at risk of vulnerabilities, some of which involve genuine human error, whilst others are exposed to malicious intent. Hence the need for cyber security, that is, ensuring the safety, confidentiality, integrity and availability of cyberspace.

This Green Paper, along with its supporting document intends to inculcate an awareness of cyber security, its extent and its implications of which Malta, as an integral part of cyberspace, needs to consider. Launching cyber security on a national scale, essentially calls for a planned, collective and systemic approach, thus leading to the need of a National Cyber Security Strategy. Digital Malta – the National Digital Strategy for the period 2014-2020 recognises and proposes the fulfilment of such need. Thus, the Green Paper presents a high level, strategic approach for cyber security on a national scale, for detailed consultation. The consultation is intended to consolidate further the proposals, thus leading to the launch of the first National Cyber Security Strategy.

The Green Paper recognises that tackling cyber security, also entails the need to:

- Safeguard **fundamental human rights** at all times
- Adopt a **multi-disciplinary approach**
- Ensure that all stakeholders of cyberspace – government, private sector, and civil society understand their **shared responsibility** and thus commit to collaborate and cooperate, to ensure a safe, stable and secure environment
- Adopt a **risk based approach**, based upon the premise that it is impossible to guarantee immunity from any cyber attack

All of the above constitute the **fundamental principles** upon which the overall vision is based. In essence, the vision covers the need and expectations of three key national stakeholders – **the public sector,** the **private sector** and **civil society** to ensure cyber security. Five dimensions enable articulation of the vision

MaltaCIP

mita
MALTA INFORMATION TECHNOLOGY AGENCY

mca
MALTA COMMUNICATIONS AUTHORITY

MINISTRY FOR THE ECONOMY, INVESTMENT AND SMALL BUSINESS

EXECUTIVE SUMMARY

into the strategy. They are **Policy, Legislation**, **Risk Management, Awareness** and **Education** upon which the subsequent proposed strategy is based.

Prior to proposing the strategy however, research and assessments have been made so as to enable a high level pragmatic approach towards cyber security within the local context. The Supporting Document is a compilation of such an activity, serving as a rationale for the Green Paper's approach in the process. It focuses on the global cyber threat scenario, leading to concerns, experiences and current preparedness and a further focus on stakeholders on the domestic front.

The ensuing strategic direction within the Green Paper is proposed to be attained by six goals, each of which carry a number of proposed measures, as follows:

1. **Establish a governance framework** - Is based upon the premise that a cyber security strategy needs to be established, and more importantly, be effectively implemented and maintained on a continuous basis. Hence the need to ensure the key coordination structures, processes, roles and practice with particular focus on risk management within the public and private sector.
2. **Combat cyber crime** - Aims to ensure and consolidate capabilities to tackle cyber crime
3. **Strengthen national cyber defence** - Aims to foster sharing of cyber security knowledge and intelligence, review current legislation and regulations in line with cyber space developments and ensure digital resilience on a national and organisation wide scale.
4. **Secure cyberspace** - Aims to foster self regulation and voluntary self commitment, bearing in mind that legislation is not a panacea to cyber security commitments. It also aims to stimulate use of standards and best practices that guarantee security whilst allowing for interoperability. Special focus is also given to promote security of online public services and to consolidate support to the private sector.
5. **Cyber security Awareness and Education** - Aims to target academia, the public and private sector and citizens as a means to sensitize awareness, knowledge as well as expertise in cyber security. A strategic approach towards a national awareness and advice campaign is especially recommended.
6. **National and International Cooperation** - Aims to ensure effective cooperation and collaboration on a national level, on a European and

"DEFENDING AND PROTECTING NATIONAL INFORMATION INFASTRUCTURE FROM CYBER THREATS. ENSURING THE SECURITY, SAFETY AND PROTECTION OF USERS OF CYBER SPACE."

MaltaCIP

mita
MALTA INFORMATION TECHNOLOGY AGENCY

mca
MALTA COMMUNICATIONS AUTHORITY

MINISTRY FOR THE ECONOMY, INVESTMENT AND SMALL BUSINESS

EXECUTIVE SUMMARY

on a global basis, enabled by EU institutions and activities, based on the understanding that cyber security has no national boundaries.

All six goals aim to cover **two key strategic outcomes expected** of the Strategy, namely:

- **Defending and protecting the national information infrastructure from cyber threats**.
- **Ensuring the security, safety and protection of users of cyber space.**

The proposed strategic approach is by no means the end in itself. It aims to set the stage for feedback and detailed consultation. The consultation ensuing from the launch of this Green Paper is envisaged to:

- Consolidate the high level requirements into more timely, specific and actionable measures
- Potentially include further initiatives and requirements for cyber security within the local context

The exercise is ultimately expected to lead to the launch of the National Cyber Security Strategy. The Strategy in itself would be expected to be periodically reviewed and updated so as to ensure its currency to evolving cyber security risks, realities and maturity of cyber security capabilities on the domestic front.

MALTA INFORMATION TECHNOLOGY AGENCY

MALTA COMMUNICATIONS AUTHORITY

MINISTRY FOR THE ECONOMY, INVESTMENT AND SMALL BUSINESS

INTRODUCTION - BACKGROUND

MALTA IS NO ISLAND WITHIN THE REALM OF CYBER SPACE! CYBER SPACE KNOWS NO BOUNDARIES.

Up to a few decades ago, a country's security interests focussed on protecting its borders, its waters and its airspace. Today, cyber space forms an integral part of a country's day to day reality. Information and Communications Technology (ICT) leads the way in interaction within and outside of a country's territory and its disruption may potentially affect life. Hence, cyber space cannot be left out of a country's span of protection.

Malta is no island within the realm of cyber space. Cyber space knows no boundaries. It transcends national borders, promoting online opportunities of dialogue and cooperation beyond our shores. However, the cyber world makes no distinction between its users of good intent or not. Therefore, as opportunities are limitless, so are cyber threats. Such malicious attempts in cyber space may be launched anywhere, in any vulnerable area of a digital network, instantaneously leaving no time for an appropriate response and with very minimal traceability or detection of its perpetrator. Ultimately, cyber space is man-made and like anything else of its sort, it is never perfect. The rapid advances of technology itself and the opportunities that arise from it do not allow it either.

Malta's security of cyber space ultimately calls for a planned, collective and systemic approach that respects fundamental rights and freedoms whilst ensuring confidentiality, integrity and availability of cyberspace on a day-to-day basis. Such is the intention of Digital Malta – the National Digital Strategy for the period 2014 till 2020 – which identifies a National Cyber Security Strategy as one of its required actions.

"MALICIOUS ATTEMPTS IN CYBER SPACE MAY BE LAUNCHED ANYWHERE, IN ANY VULNERABLE AREA OF A DIGITAL NETWORK, INSTANTANEOUSLY LEAVING NO TIME FOR AN APPROPRIATE RESPONSE AND WITH VERY MINIMAL TRACEABILITY OR DETECTION OF ITS PERPETRATOR"

2 PURPOSE AND SCOPE

THIS GREEN PAPER IS INTENDED AT SETTING AN OVERALL, HIGH LEVEL DIRECTION IN CYBER SECURITY, ON A NATIONAL LEVEL, FOR CONSULTATION.

"ESSENTIALLY, CYBER SECURITY IS BASED UPON THE FOUNDATIONS OF INFORMATION SECURITY, NAMELY CONFIDENTIALITY, INTEGRITY AND AVAILABILITY"

It also intends to inculcate an awareness of the extent of the cyber security scenario and recognition of the need for a planned and concerted effort so as to protect Malta and its interests on a national scale.

Consultation based upon this Paper should ultimately lead to the launch of the National Cyber Security Strategy. Hence, future updates based upon the consultations are envisaged to:

- Consolidate the high level requirements into more timely, specific and actionable measures
- Potentially include further initiatives and requirements for cyber security within the local context

Apart from this **Introductory Part,** the Paper includes:

- **Part Two – Overall Direction** sets a broad, high level direction for the National Cyber Security Strategy, through a definition of what is meant by cyber security and identification of the principles leading to the vision expected to be attained through the strategy
- **Part Three - Proposed Strategy** outlines the proposed a way forward made up of a number of key goals and corresponding measures. It is based upon the overall direction and a current assessment in cyber security.

The assessment of the current cyber security scenario, including a broad identification and assessment of related stakeholders can be seen into more detail in the Supporting Document of National Cyber Security Strategy Green Paper which is also published along with the Paper. The supporting document serves to record the key rationale for the proposed strategy.

THE CONSULTATION PROCESS

Extensive research has been undertaken, as can be especially indicated by the **Supporting Document of National Cyber Security Strategy Green Paper.** It is however understood that , both the need for a pragmatic approach to the strategy proposals as well as the national scope of the strategy call for a consultation process that involves various actors within the public sector, the private sector as well as civil society.

Thus, all entities and members of the public are invited to consider the proposals of the Green Paper. Feedback is welcome, with opportunities for consultation to be announced in due course.

3 OVERALL DIRECTION

WHAT IS MEANT BY CYBER SECURITY?

Definitions for cyber security abound, however they all essentially point to the **security** of the **cyber space;** namely all:

- Interconnected ICT hardware and software infrastructure
- Data in transit and at rest on the networks
- Connected users
- Logical connections established among them

In view of the above[1], the following definition of cyber security is being adopted:

It is the safeguards and actions that can be used to protect cyber domain from those threats that are associated with or that may harm its interdependent networks and information infrastructure. It strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.

Essentially, cyber security is based upon the foundations of information security, namely confidentiality, integrity and availability. However, whilst information security is business driven and results in prudent investment in safeguards and countermeasures, cyber security is *threat driven* where all cyber space is at risk. The inherent interconnectedness of cyber space exposes all of its constituents to a failure of their most vulnerable elements[2].

Additionally effective cyber security cannot be reached by technological measures alone as modern cyber attacks could bypass all defence layers by exploiting the human factors through techniques such as social engineering[3]. Hence, safeguards and actions hereby refer to ongoing and planned measures which may potentially be of technical, governance, legal, educational, behavioural or disseminative nature.

Above all, cyber security cannot be seen from a technological aspect only, but needs to cover the needs and expectations of the state, the economy and society, all of which are increasingly active participants in an interactive digital world.

"ABOVE ALL, CYBER SECURITY CANNOT BE SEEN FROM A TECHNOLOGICAL ASPECT ONLY, BUT NEEDS TO COVER THE NEEDS AND EXPECTATIONS OF THE STATE, THE ECONOMY AND SOCIETY, ALL OF WHICH ARE INCREASINGLY ACTIVE PARTICIPANTS IN AN INTERACTIVE DIGITAL WORLD."

3 OVERALL DIRECTION

GUIDING PRINCIPLES

Within this context, the following principles are proposed:

Rule of Law

The approach on cyber security shall respect and promote fundamental rights and freedoms as chartered within European Union and national legislation. All measures shall comply with the principles of necessity, proportionality and legality, with appropriate safeguards to ensure accountability and redress.

Multi-stakeholder, cooperative and collaborative approach

The pervasive nature of cyber space, essentially calls for a multi-stakeholder approach towards its security – both at a national level as well as beyond Malta's shores. Hence, on a national level, cooperation and collaboration of various stakeholders, including the public sector, the private sector, academia and civil society is necessary. A cooperative and collaborative approach at an EU and international level is also required.

Shared responsibility

Whilst leading in its commitment towards cyber security on a national scale, Government cannot assume sole responsibility for protecting all of cyberspace. All users of ICT are responsible to take reasonable steps to protect systems and data on an individual and on a collective basis.

Risk Management

The widely diffused use of cyberspace coupled with its rapid and continuous evolvement, renders it impossible to guarantee immunity from any form of cyber attack. Hence a risk-based approach to assess, prioritise and take measures to ensure cyber security, along with any technology investment is necessary.

"ON A NATIONAL LEVEL, COOPERATION AND COLLABORATION OF VARIOUS STAKEHOLDERS, INCLUDING THE PUBLIC SECTOR, THE PRIVATE SECTOR, ACADEMIA AND CIVIL SOCIETY IS NECESSARY. A COOPERATIVE AND COLLABORATIVE APPROACH AT AN EU AND INTERNATIONAL LEVEL IS ALSO REQUIRED."

3 OVERALL DIRECTION

OVERALL VISION

Within the context of the articulated principles, an overall vision for the Malta Cyber Security Strategy is:

To ensure a secure, resilient and trusted digital interactive environment that supports Malta's safety and security well-being whilst maximising on the benefits of a digital economy.

In specific terms, the vision entails that:

- Civil society is aware of cyber risks and undertakes necessary precautions to protect its confidentiality, personal integrity, identity and financial well-being
- The Private Sector, whilst tapping the opportunities resulting from the technology developments, actively ensures that it operates in a secure and resilient digital economy, whilst ensuring effective delivery of their services and/or goods and protection of their customer's privacy and integrity
- The Public Sector leads the way in ensuring a secure and resilient digital environment for its interaction with and/or service delivery to civil society, private enterprise and with regional and international partners.

The National Cyber Security Strategy will seek to address the needs and expectations of each of the above stakeholders, in the light of the proposed vision.

OVERALL DIRECTION - PART TWO

A CYBER SECURITY STRATEGY MODEL

As outlined in **Figure 1,** the strategy is enabled by five dimensions which are based upon those of the **Cyber Security Capability Maturity Model** of the Global Cyber Security Capacity Centre, University of Oxford.

The Proposed goals and related measures underscore in more specific terms how the strategy is expected to be implemented. They are based upon a broad assessment of the current cyber security scenario, which is presented in the supporting document of this Paper.

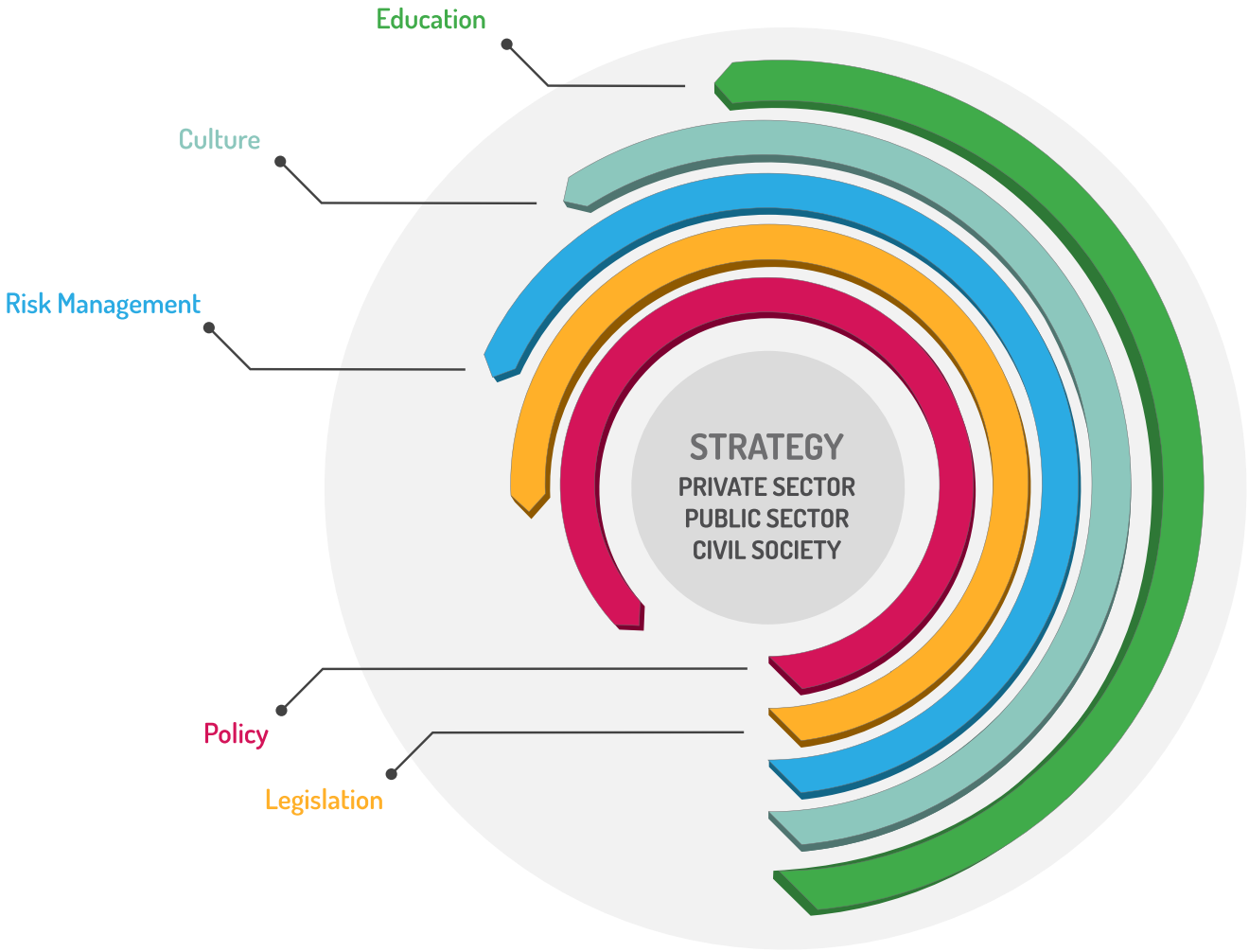


Figure 1 - A Cyber security Strategy Model for Malta

Policy	Legislation	Risk Management	Culture	Education
Devising cyber security policy and strategy that sets the direction on a national level.	Creating effective legal and regulatory frameworks to support all aspects of the strategy.	Controlling risks through organisation, standards and technology.	Fostering awareness to encourage a responsible cyber culture throughout society.	Building cyber skills into the workforce and leadership through effective education.

4 PROPOSED STRATEGY

THE PROPOSED GOALS AND ACCOMPANYING MEASURES

4.1 THE PROPOSED GOALS

Digital Malta, and in particular, Action 53, proposes four high level goals for a National Cyber Security Strategy, which are:

- **Combat Cyber Crime:** Law enforcement agencies are to identify gaps and strengthen their capability to investigate and combat cyber crime.
- **Strengthen National Cyber Defence:** Public and private entities are to be guided and assisted in strengthening their cyber defence capabilities.
- **Secure Cyberspace:** Higher levels of trust are to be instilled through awareness programmes and the delivery of trustworthy, ICT-enabled services that assure confidentiality, integrity, availability and privacy.
- **Build Capacity (Cyber Security Awareness and Education):** The skills and educational frameworks required are to be identified and developed.

All four goals are essential building blocks for the National Cyber Security Strategy. Additionally, through the analysis conducted - and which can be found on the Supporting document - two other goals are identified as essential for inclusion. They are:

- **Establish a governance framework to attain a National Cyber Security Strategy** – given that at this stage, only the technical and operational structures are in formation. The strategic level that focuses on the long term trends and analysis of cyber security is also necessary.
- **National and International Cooperation** – given that the borderless nature of cyber-related activity, essentially calls for particular regard to the global and regional aspect, apart from the national focus of related security.

In this manner, a holistic and comprehensive outlook towards a cyber security for Malta can be presented. Furthermore, all six goals aim to cover two key strategic outcomes expected from the Strategy, namely:

- **Defending and protecting the national information infrastructure from cyber threats**
- **Ensuring the security, safety and protection of users of cyber space.**

4.2 THE PROPOSED MEASURES

A set of measures to each corresponding goal are proposed below. Apart from the analysis, they are also based upon:

- Best practices noted in cyber security strategies within the European Union and worldwide,

4 PROPOSED STRATEGY

- Official EU documentation
- Relevant action items within **Digital Malta** and other local strategy documents such as **e-Commerce Malta** - the National e-commerce Strategy (2014-2020) - published by the Malta Communications Authority.

1 GOAL: ESTABLISH A GOVERNANCE FRAMEWORK

The governance framework covers the necessary key functions and corresponding roles and responsiblities, as well as policies and processes necessary to constitute a robust foundation for an effective National Cyber Security Strategy.

"THE GOVERNANCE FRAMEWORK COVERS THE NECESSARY KEY FUNCTIONS AND CORRESPONDING ROLES AND RESPONSIBILITIES, AS WELL AS POLICIES AND PROCESSES NECESSARY TO CONSTITUTE A ROBUST FOUNDATION FOR AN EFFECTIVE NATIONAL CYBER SECURITY STRATEGY."

1.1 ESTABLISH THE NECESSARY KEY COORDINATION STRUCTURES

It is envisaged that the following functions (involving multiple stakeholders) shall be required to ensure sustainability of the Malta Cyber Security Strategy:

a. At the strategic level:

I. A function for the **articulation and periodic review of the National Cyber Security Strategy.** The creation of this function is required in the short term. This body would need to work in close cooperation with the strategy implementation function(s) referred to below

II. A strategy implementation function to oversee **implementation of the strategy and monitor cyber security operations.** Such function needs to have the necessary funding, resources and mandate to:

- Take a leading, active role in the implementation of the National Cyber Security Strategy
- Ensure security preparedness of the public and private sector of their ICT, in line with established security requirements.

The structure[4] and responsibilities of these functions are subject to further consultations and may need to be aligned to any relevant European Union requirements.

b. At the operational level, **function(s) for the national coordination of cyber detection and response.** Computer Security Incident Response Teams (CSIRTs) tend to be of such technical and operational nature. This entails ensuring consolidation of a top level coordinating CSIRT[5]. It also implies close communication and coordination of the CSIRT with the proposed strategy implementation function, given that it would need to be involved on:

- Real-time information sharing and response to calls
- Longer term planning[6]

Communication and coordination, as the need arises, with other CSIRTs existing in Malta may also be necessary.

4 PROPOSED STRATEGY

1.2 FOSTER THE COORDINATION TO PROTECT NATIONAL CRITICAL INFORMATION INFRASTRUCTURE

Measures of preparedness, response and recovery, including cooperation and ongoing coordination mechanisms are particularly necessary to protect national critical information infrastructure. It is thus necessary to ensure that such national coordination between all stakeholders concerned [7] is fostered.

1.3 ENSURE CLEAR DELINEATION AND COMMUNICATION OF ROLES AND RESPONSIBILITIES

Cyber related roles and responsibilities – such as those identified above and potentially those arising from the proposed measures need to be clearly delineated and agreed upon accordingly. Communication of their establishment further ensures the effective coordination that may be necessary between the effected stakeholders themselves.

1.4 ENSURE THE ESTABLISHMENT OF A NATIONAL CYBER RISK ASSESSMENT PLAN AND PROCESSES THAT ARE REGULARLY VALIDATED AND TESTED

The Public Sector and key market operators[8] need to **identify cyber risks and assess impacts of potential incidents.** This calls for the need to develop a national cyber risk assessment exercise as the basis to assess, prioritise and take measures to ensure cyber security.

Such an assessment plan entails coordination between all stakeholders involved and it needs to be updated on a regular basis, so as to ensure its currency with:

- The cyber threat vector landscape
- Evolution in the adoption of existing and emerging ICT.

The **cooperation and communication processes** needed to ensure prevention, detection, response, repair and recovery (including communication), that are modulated according to the alert level are to be ensured. Such processes also refer to national incident cyber handling procedures and business continuity plans to ensure resilience. Furthermore, it is understood that the above plans and processes need to be subject to a schedule of **regular testing and validation exercises**[9] with the resulting outcome (including lessons learnt) used as a basis for any related updates.

The emphasis made to the Public Sector and key market operators[10] through such measures should not however construe that other organisations need not adopt similar activities.

"THE PUBLIC SECTOR AND KEY MARKET OPERATORS NEED TO IDENTIFY CYBER RISKS AND ASSESS IMPACTS OF POTENTIAL INCIDENTS."

4 PROPOSED STRATEGY

An assessment of financial risks related to cyber-related incidents may also indicate the identification of a market in cyber insurance, which may in turn contribute to information sharing among its participants, apart from availability of financial coverage to mitigate consequential losses.

1.5 CONSOLIDATE THE INFORMATION SECURITY FRAMEWORK WITHIN THE PUBLIC SECTOR AND ENSURE AN AGREED PROTECTION LEVEL FOR KEY MARKET OPERATORS.

The Government of Malta Information Security Policy is expected to come into force by the second quarter of 2016. It is based upon ISO 27001 Information Security international standard and applies to all of the Public Sector.
It also needs to be ascertained that all key market operators[11] do apply an agreed level of information security.

2 GOAL: COMBAT CYBER CRIME

2.1 ESTABLISH FORUM FOR INTERNET SAFETY AND PROTECTION OF MINORS

This measure is referred to in **Digital Malta,** and it proposes a number of relevant public sector stakeholders and industry respresentatives as the Forum's members. The Forum aims to:

- Share knowledge
- Monitor developments
- Put forward policy ideas
- Represent Malta on European bodies working in this field

This Forum could potentially help out in reviewing the Cyber Security Strategy itself with respect to combating cyber crime activity.

2.2 IDENTIFY GAPS AND STRENGTHEN CAPABILITY TO INVESTIGATE AND COMBAT CYBER CRIME

A regular assessment of present state cyber crime capability in Malta among all relevant law enforcement authorities is indeed a prerequisite in the light of the continuously evolving threat vector landscape.

Internal security is crucial. Yet, it also needs to be borne in mind that threats to EU citizens are increasingly cross border and varied in nature. EU Member states, including Malta, can thus no longer succeed on their own. **The European Agenda on Security** – the EU's strategy to tackle security threats in the EU for period 2015-2020[12] is intended to contribute in this respect. Cybercrime is one of the Agenda's priority for the years 2015-2020.

"INTERNAL SECURITY IS CRUCIAL. YET, IT ALSO NEEDS TO BE BORNE IN MIND THAT THREATS TO EU CITIZENS ARE INCREASINGLY CROSS BORDER AND VARIED IN NATURE. EU MEMBER STATES, INCLUDING MALTA, CAN THUS NO LONGER SUCCEED ON THEIR OWN."

4 PROPOSED STRATEGY

The Agenda aims to strengthen and make more effective the exchange of information and operational cooperation between Member states, EU Agencies and the critical information infrastructure sector; by aiming to:

"CYBERCRIME IS ONE OF THE AGENDA'S PRIORITY FOR THE YEARS 2015-2020."

- Reinforce the capacity of law enforcement authorities in Member states, in particular through the Europol's European Cybercrime Centre
- Address obstacles to criminal investigations on cybercrime, notably with respect to access to evidence
- Prioritise the implementation of existing legislation on attacks against information systems and on combating child abuse.

2.3 ASSESS AND CONSOLIDATE ON-LINE MECHANISM TO REPORT CYBERCRIME

The mechanism is needed to report illicit online activity for the required action to be taken as well as to determine the extent of cybercrime. It entails:

- The ability of the mechanism to track cybercrime at a national level
- Ensuring nation-wide awareness and use of the mechanism, especially among citizens and small businesses.

It is also recommended to ensure that a strategic approach on the applicability of hotlines related to cyber crime handling is taken, so as to facilitate the one-stop shop concept, whilst maximising the use of resources.

3 GOAL: STRENGTHEN NATIONAL CYBER DEFENCE

3.1 ESTABLISH A COLLECTIVE APPROACH FOR SHARING CYBER SECURITY KNOWLEDGE AND INTELLIGENCE

A collective approach, involving both the public and private sector, potentially through the use of ICT is needed to:

- Exchange information on cyber threats and to strengthen response to cyber incidents efficiently and effectively
- Analyse new trends and identify opportunities and emerging threats
- Work to strengthen cyber security
- Provide framework for sharing best practice
- Potentially improve professionalism in information assurance and cyber defence across the private and public sector through schemes for certifying related competence and specialist training.

4 PROPOSED STRATEGY

The approach may also allow for intra-business sectoral communication, particularly in areas where particular information may be deemed as of a highly sensitive nature to be shared across all participants.

3.2 REVIEW EXISTING LEGISLATION AND PROVIDE MEASURES THROUGH LEGISLATION AND REGULATION TO ENSURE RELEVANCE AND EFFECTIVENESS TO THE CYBER WORLD

This measure builds upon two objectives of **Digital Malta**, as follows:

- **Objective 43** – review existing legislation to ensure relevance and effectiveness in the cyber world.
- **Objective 44** – provide measures to maintain privacy, safety and security while surfing, transacting and operating on-line. Legislation will address several matters such as safeguarding intellectual property rights, patents, sensitive and personal information, cloud computing and data ownership, contentious content, net neutrality, vendor lock-in and exit management strategies; online contracts and license agreements.

The measure is also highly relevant taking into consideration:

- The requirements arising from the **European Agenda on Security**, referred to in **Measure 2.2.**
- **Action 38 - Digital Single Market** – of **Digital Malta**, which states Government's intention to maximise the benefits and opportunities deriving from legislation adopted within the EU such as those related to data protection, electronic identification and trust, etc.
- Relevant EU Directive and regulation developments arising.

3.3 ENSURE THE COUNTRY'S DIGITAL RESILIENCE TO CYBER ATTACK AS WELL AS THE CAPABILITY TO PROTECT ITS INTERESTS

Such a measure entails ensuring that the following are addressed:

- Cyber space defences
- Structures to counter terrorist attacks
- Ability and capacity to detect threats in cyber space
- Capability to disrupt attacks on the country from cyber space

4 PROPOSED STRATEGY

3.4 CONDUCT CYBER DEFENCE EXERCISES

Cyber defence exercises are to be scheduled and conducted from time to time. Such a measure contributes to the need to review the ability to anticipate, prepare for, identify and attribute, combat hostile cyberspace acts. Apart from technical considerations, cyber defence exercises should also assess non-technical areas both at an operational, tactical as well as at a strategic level such as testing national and international coordination and any relevant Standard Operational Practices.

Although crucial for stakeholders such as the public sector and key market operators[13], such exercises should also be conducted by other organisations.

"SUCH MEASURE (CONDUCT CYBER DEFENCE EXERCISES) CONTRIBUTES TO THE NEED TO REVIEW THE ABILITY TO ANTICIPATE, PREPARE FOR, IDENTIFY AND ATTRIBUTE, COMBAT HOSTILE CYBER ACTS."

4 GOAL: SECURE CYBERSPACE

4.1 ESTABLISH REGULATION AND VOLUNTARY SELF-COMMITMENT FOR GUARANTEEING CYBER SECURITY

The current scenario analysis of cyber security in Malta indicates areas of regulation and policy particularly within the local regulated industry sectors. Focus appears to be mainly on policy frameworks covering the licensing approaches which seek to mitigate risk.

Whilst legislation may help, Maltese regulatory authorities may also need to address further emerging technology such as cloud computing applicability, through regulation within their respective sectors.

On the other hand, it is understood that legislation and regulation cannot necessarily cover all aspects of cyber security; particularly considering potential financial and human resource constraints for robust cyber security. Voluntary self commitment is, thus, also key to cyber security. The notion of the applicability of a European trust mark, applied also in a number of EU states[14] may encourage voluntary self commitment and may therefore be one item to considered locally.

Local national strategy may already serve as potential opportunities for further consideration in fostering self commitment, such as:

- **e-Commerce Malta** which highlights three pillars as its basis:
  - I. Engendering trust in ecommerce
  - II. Transforming micro-enterprises
  - III. Taking Small to Medium sized Enterprises and industry to the next level; which specifically also refers to an audit-kit – through a Specialist advisory service (Measure 2) and the European trust-mark (Measure 9)

4 PROPOSED STRATEGY

Digital Malta which refers to the Forum for the transformation of industries through ICT that aims to raise awareness about how ICT can help industries transform themselves and to discuss items such as self-regulation.

4.2 STIMULATE USE OF INTEROPERABLE AND SECURE STANDARDS ON THE BASIS OF GOOD PRACTICE

Digital Malta, through **Action 42 – Standards and Good Practice,** states Government's intention to collaborate with stakeholders to support and promote National and EU cross-border interoperability, ICT standards based on industry best practices and Green ICT.

The implementation of ISO 27001 controls through the Information Security Policy across the Public Sector, as well as implementation of the standard within industries, may potentially contribute to further secure ICT on the local scenario.

With respect to the notion of nationally and EU recognised interoperability, which also effectively promotes the use of safe secure standards, Digital Malta states as one of its objectives, Government's commitment to revise and revamp the current National Interoperability Framework including related policies.

On the other hand, such a measure cannot depend solely on Government for its implementation, but requires private sector collaboration.

Whilst standards like ISO 27001 may serve as a good initial basis, however consideration of industry led standards and guidance that put in place a series of measures specifically aimed to address cyber threats[15] are to be encouraged for use. This could form an integral part of what is proposed in **Measure 4.1.**

In particular, special consideration needs to be given by operators and users of emerging technologies such as those referred to by the threat landscape of the Supporting Document. In such areas, related standards and security controls, may still be in the very early stages of maturity and may thus pose cyber security vulnerability challenges for interoperability which need to be carefully assessed.

4.3 PROMOTE ROBUST LEVELS OF CYBER SECURITY IN ONLINE PUBLIC SERVICES

Such a measure may alleviate concerns expressed within Euro barometer findings with respect to Maltese accessing online services. The applicabilityof interoperable and secure standards, as referred to in **Measure 4.2**, may potentially contribute for the attainment of such a measure.

4 PROPOSED STRATEGY

4.4 CONSOLIDATE SUPPORT TO THE PRIVATE SECTOR ON CYBER SECURITY

Measure 4.1 outlines how cyber security can be facilitated in the private sector. Furthermore, private sector participation in awareness and advice programmes as well as cyber related exercises to specific sectors may additionally help. For example, ways may potentially be sought with business service providers (e.g. lawyers, insurers) of how they can potentially develop services to help businesses manage and reduce risks[16].

"WITHIN THE CURRENT CYBER SECURITY SCENARIO, THERE APPEAR TO BE RELATED AWARENESS CAMPAIGNS IN SCHOOLS. IT IS IMPORTANT THAT SUCH CAMPAIGNS ARE SUSTAINED ON THE LONG TERM, POTENTIALLY THROUGH A CONCERTED STRATEGIC APPROACH."

5 GOAL: CYBER SECURITY AWARENESS AND EDUCATION

5.1 ENSURE CYBER SECURITY AWARENESS AND EDUCATION

Such measures may primarily entail:

- Review of existing curricula that includes cyber security along with ICT and media competencies
- Academic programmes designed to consolidate cyber security expertise

Action 2 - Empowering the young through a safer Internet - of Digital Malta may contribute in this respect. The action item states that "Digital Citizenship will become part of the National Education Curriculum, to equip children and youths with the abilities to interact and use the Internet safely and intelligently. Parents and carers will be involved together with educators and youth workers. This action will stimulate the production of creative online content, empower the younger generation and help create a safer environment. With the support of competent authorities this measure will help combat cyber child abuse and exploitation".

Additionally **Action 60 - Building national capacity in specialist skill sets** - of **Digital Malta** states Government's commitment, through educational institutions and industry to support the creation of specialist educational pathways, addressing labour market requirements and to develop the curriculum and provide technical materials. The possibility of cyber security expertise within such initiative needs to be actively considered.

Within the current cyber security scenario, there appear to be related awareness campaigns in schools. It is important that such campaigns are sustained on the long term, potentially through a concerted strategic approach.

4 PROPOSED STRATEGY

5.2 ENSURE RELEVANT EDUCATION AND TRAINING TO PUBLIC SECTOR STAFF AND THOSE WORKING WITHIN CRITICAL INFORMATION INFRASTRUCTURE

Training and education on cyber security is one key priority within the public sector, especially given the sector's wider extensive use of ICT and sensitive data, compared to other sectors.

In any office environment it needs to be kept in view, that technology controls are not sufficient to protect data from related cyber security threats as outlined in the **Supporting Document.** The controls need to go hand in hand with human resource, awareness and employee guidance programs[17].

The development of cyber security expertise within the public sector is another key area that merits particular attention. In the process, it also needs to be ensured that a comprehensive list of public sector professionals certified under internationally recognised certification programs in cyber security is established and maintained.

Furthermore, it needs to be ensured that ICT personnel are trained so as to enable them to recognise cyber incidents, to detect anomalies in their ICT systems and to report them accordingly.

5.3 FOSTER APPLICATION OF RESEARCH AND DEVELOPMENT ON CYBER SECURITY

Such a measure aims to ensure cyber security as among key research priorities. It effectively calls for encouragement and support for research in any national and EU research projects and initiatives on cyber security. Essentially, it entails participation not only from Government but also from the private sector and the academia.

It also calls for an emphasis to ensure security and privacy in the design of ICT products and services for Government as well as in other areas of application.

5.4 A STRATEGIC, TARGET-ORIENTED NATIONAL AWARENESS AND ADVICE CAMPAIGN

It is highly recommended that a concerted strategic approach is undertaken, potentially through a nationwide Communications strategy for cyber security[18]; aimed at addressing the various strata of society, business and public sector during the short, medium to long term. Such an approach may ensure:

- Avoiding piecemeal, potentially one-off approaches to awareness campaigns
- No duplication of effort

"IT IS HIGHLY RECOMMENDED THAT A CONCERTED STRATEGIC APPROACH IS UNDERTAKEN, POTENTIALLY THROUGH A NATIONWIDE COMMUNICATIONS STRATEGY FOR CYBER SECURITY".

4 PROPOSED STRATEGY

- Maximisation of cyber security related financial and human resources
- Imparting effective awareness and knowledge that is commensurate to the target audience and to the medium used[19]
- A measure of the extent of national awareness and understanding of cyber security over time.

Most measures highlighted within **Goals 4** and **5** of this strategy as well as any established national way of sharing related knowledge, experience and insight as referred to in **Measure 3.1**[20] may potentially serve as key sources for the establishment and maintenance of such a concerted strategic campaign.

Ultimately, the key factor in any training and awareness programmes on cyber security is:

- Finding the right way to raise awareness
- Establishing training programmes that effectively increase security level of an organisation and maintaining such increased level of security in the long term
- Ensuring motivation of users to learn and pay particular attention to various signals of fake communications on a day to day basis (particularly to counter social engineering threats).

Prior and post assessment of such programmes is one way of ensuring their effectiveness. However, consideration should also be taken that such programmes may not necessarily focus only on traditional modes of education and awareness but also on experimentation of innovative ways of their conduct[21].

5.5 ENCOURAGE 'CYBER HYGIENE' AND PERSONAL RESPONSIBILITY

Ultimately, citizens are expected to apply at least some form of **basic 'cyber hygiene'** in using ICT, such as through careful disposition and use of personal information on-line, installing software updates, using basic security controls such as passwords and anti-virus software. The national awareness campaign as highlighted earlier should help in reaching this objective.

In particular, **a responsible disclosure policy** that enables well-intentioned citizens to safely inform Government, businesses or institutions about detected vulnerabilities in their ICT systems or services may also be considered[22].

4 PROPOSED STRATEGY

6 GOAL: NATIONAL AND INTERNATIONAL COOPERATION

6.1 EFFECTIVE COOPERATION AND COLLABORATION ON CYBER SECURITY ON A NATIONAL , EUROPEAN AND GLOBAL BASIS

Malta is no island in cyberspace. Hence the ongoing cooperation and collaboration on cyber security on a national, European and on a global basis needs to be sustained on the long term.

Above all, a co-ordinated approach, among all key local stakeholders in cyber security interacting locally and overseas needs to be ensured so as to ensure synergy of national and international effort, knowledge and expertise within the domain.

Cyber related activities such as those conducted by ENISA is one area of national and international cooperation that may potentially involve both local public as well as private sector organisations.

On a national level, most of the measures highlighted earlier essentially call for national cooperation and coordination.

On a wider international perspective, activities such as those undertaken by the Council of the European Union on cyber-diplomacy[23] aim to foster increased global cyber capacity building, as well as international cooperation and judicial capacity on cyber crime.

"MALTA IS NO ISLAND IN CYBERSPACE. HENCE THE ONGOING COOPERATION AND COLLABORATION ON THE CYBER SECURITY ON A NATIONAL, EUROPEAN AND ON A GLOBAL BASIS NEEDS TO BE SUSTAINED ON THE LONG TERM"

PROPOSED STRATEGY - PART THREE

5 CONCLUSION

5.1 THE CYBER SECURITY STRATEGY MODEL REVISITED

Figure 2 indicates how all of the proposed measures intend to address the five dimensions of the Cyber Security Strategy Model, referred to earlier.

		Policy	Legislation	Risk Management	Culture	Education
		Devising national cyber security policy and strategy that sets the direction on a national level.	Creating effective legal and regulatory frameworks to support all aspects of the strategy.	Controlling risks through organisation, standards and technology.	Fostering awareness to encourage a responsible cyber culture throughout society.	Building cyber skills into the workforce and leadership through effective education.
GOAL	**MEASURE**					
Establish a governance framework	**1.1** Establish the necessary key coordinating structures					
	1.2 Establish the coordination structure to protect national critical information infrastructure					
	1.3 Clearly delineate roles and responsibilities					
	1.4 Ensure the establishment of a cyber risk assessment plan and processes that are regularly validated and tested					
	1.5 Consolidate the IS Framework within the public sector and ensure an agreed protection level for key market operators					
Combat Cyber Crime	**2.1** Establish Forum for Internet safety and protection of minors					
	2.2 Identify gaps and strengthen capability to investigate and combat cyber crime					
	2.3 Assess and consolidate on-line mechanism to report cybercrime					

PROPOSED STRATEGY - PART THREE

		Policy	Legislation	Risk Management	Culture	Education
		Devising national cyber security policy and strategy that sets the direction on a national level.	Creating effective legal and regulatory frameworks to support all aspects of the strategy.	Controlling risks through organisation, standards and technology.	Fostering awareness to encourage a responsible cyber culture throughout society.	Building cyber skills into the workforce and leadership through effective education.
GOAL	**MEASURE**					
Strengthen National Cyber Defence	**3.1** Establish a collective approach for sharing cyber security knowledge and intelligence					
	3.2 Review existing legislation and provide measures through legislation and regulation to ensure relevance and effectiveness to the cyber world					
	3.3 Ensure the country's digital resilience to cyber attack as well as the capability to protect its interests					
	3.4 Conduct cyber defence exercises					
Secure Cyber Space	**4.1** Establish regulation and voluntary self commitment for guaranteeing cyber security					
	4.2 Stimulate use of interoperable and secure standards on the basis of good practice					
	4.3 Promote robust levels of cyber security in online public services					
	4.4 Consolidate support to the private sector on cyber security					

PROPOSED STRATEGY - PART THREE

		Policy	Legislation	Risk Management	Culture	Education
		Devising national cyber security policy and strategy that sets the direction on a national level.	Creating effective legal and regulatory frameworks to support all aspects of the strategy.	Controlling risks through organisation, standards and technology.	Fostering awareness to encourage a responsible cyber culture throughout society.	Building cyber skills into the workforce and leadership through effective education.
GOAL	**MEASURE**					
Cyber Security Awareness and Education	**5.1** Ensure cyber security awareness and education at all educational levels					
	5.2 Ensure relevant education and training to public sector staff and those working within critical information infrastructure					
	5.3 Foster application of research and development on cyber security					
	5.4 A strategic, target-oriented national awareness and advice campaign					
	5.5 Encourage 'cyber hygiene' and personal responsibility					
National and International Cooperation	**6.1** Effective cooperation and collaboration on cyber security on a national, European and global basis					

It is understood that updates are likely to be made following consultations leading to potential further developments to the measures proposed.

PROPOSED STRATEGY - PART THREE

5.2 LAUNCH OF THE STRATEGY

As highlighted earlier, the consultations are expected to consolidate the formulation, leading to the launch of a National Cyber Security Strategy.

The launch of the Strategy is definitely not a one-off activity. Cybersecurity is a continuous process. Hence the Strategy would be expected to be updated from time to time[24] so as to ensure its alignment with:

- Rapid developments within the cyber threat vector landscape
- Related ICT, legislative, regulatory, social and economic developments on a national scenario
- Malta's evolvement in the level of cyber security capability on a national scale.

"THE LAUNCH OF THE STRATEGY IS DEFINITELY NOT A ONE-OFF ACTIVITY. CYBERSECURITY IS A CONTINUOUS PROCESS."

RERFERENCES

- Council of the European Union (11 February 2015), Council Conclusions on Cyber Diplomacy, Outcome of Proceedings, Brussels, 6122/15
- Council of the European Union (12 March 2015), Global Conference on Cyberspace 2015, The Hague Natherlands , 6181/3/5/15 REV 3
- Council of the European Union (28 May 2015), Non-Paper on Fostering Cyber Security and Cyber Defence in Europe by means of Responsible Disclosure Polices, Meeting Document, Brussels, DS 1340/15
- Digital Malta, National Digital Strategy 2014-2020 – Programme of Initiatives 2014, **www.digitalmalta.gov.mt**
- **Dutton,** J.(June 2015),Ten essential cyber security questions to ask your CISO, **http://www.itgovernance.co.uk/blog/ten-essential-cyber-security-questions-to-ask-your-ciso/?utm_source=Email&utm_medium=Macro&utm_campaign=S01&utm_content=2015-06-22**
- European Commission (July 2012), Special Eurobarometer 390 – Cybersecurity **http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pd**
- European Commission (November 2013) , Special Eurobarometer 404 – Cybersecurity **http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf**
- European Commission (November 2013) , Special Eurobarometer 423 – Cybersecurity, **http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf**
- European Commission (2013), Cyber security Strategy of the European Union, An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final, **http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security**
- European Commission(28 January 2015) Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market, Press Release, **http://europa.eu/rapid/press_release_MEMO-15-3802_en.htm**
- European Commission(April 2015), Connecting Europe Facility,Digital Service Infrastructures(DSI) Maturity Study, Deloitte for the European Commission, DG Communications Networks, Content and Technology
- European Commission (28 April 2015), European Agenda on Security: Questions and Answers, Strasbourg,Fact Sheet, **http://europa.eu/rapid/press-release_MEMO-15-4867_en.htm**
- European Commission (6 May 2015), A Digital Single Market Strategy for Europe , Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee of the Regions , SWD(2015) 100 final, **http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf**
- European Network and Information Security Agency (ENISA) (2015), ENISA Threat Landscape 2014, **https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014**
- European Network and Information Security Agency (ENISA) (2012), National Cyber Security Strategies, Practical Guide on Development and Execution, Heraklion,Greece, **https://www.enisa.europa.eu**
- European Network and Information Security Agency (ENISA) (2012), National Cyber Security Strategies, **https://www.enisa.europa.eu**
- Federal Chancellary of the Republic of Austria (2013) , Austrian Cyber Security Strategy , Vienna, **https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AT_NCSS.pdf.**

RERFERENCES

- Global Cyber Security Capacity Centre, (2014), Cyber Security Capability Maturity Model (CMM)- Pilot, Oxford Martin School, University of Oxford, **http://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/Cyber-Security-Capacity-Maturity-Model.pdf**
- Malta Information Technology Agency (MITA), MITA Strategy 2015-2017, Version 1.0, **https://www.mita.gov.mt**
- National Coordinator for Security and Counterterrorism - The Netherlands (2013), National Cyber Security 2 – From Awareness to Capability, **https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf**
- Parliamentary Secretariat for Competitiveness and Economic Growth, Malta Communications Authority (MCA), eCommerce Malta , National Strategy 2014-2020, **www.mca.org.mt**
- Parliamentary Secretariat for Competitiveness and Economic Growth, Malta Information Technology Agency (MITA), Malta Communications Authority (MCA) , Digital Malta, National Digital Strategy 2014-2020, **www.digitalmalta.gov.mt**
- Puricelli,R.(2015), The Underestimated Social Engineering Threat in IT Security Governance and Management, ISACA Journal, 3,24-28
- Ross, S.J. (2015), Frameworks of the World Unite , ISACA Journal, 3,4-6

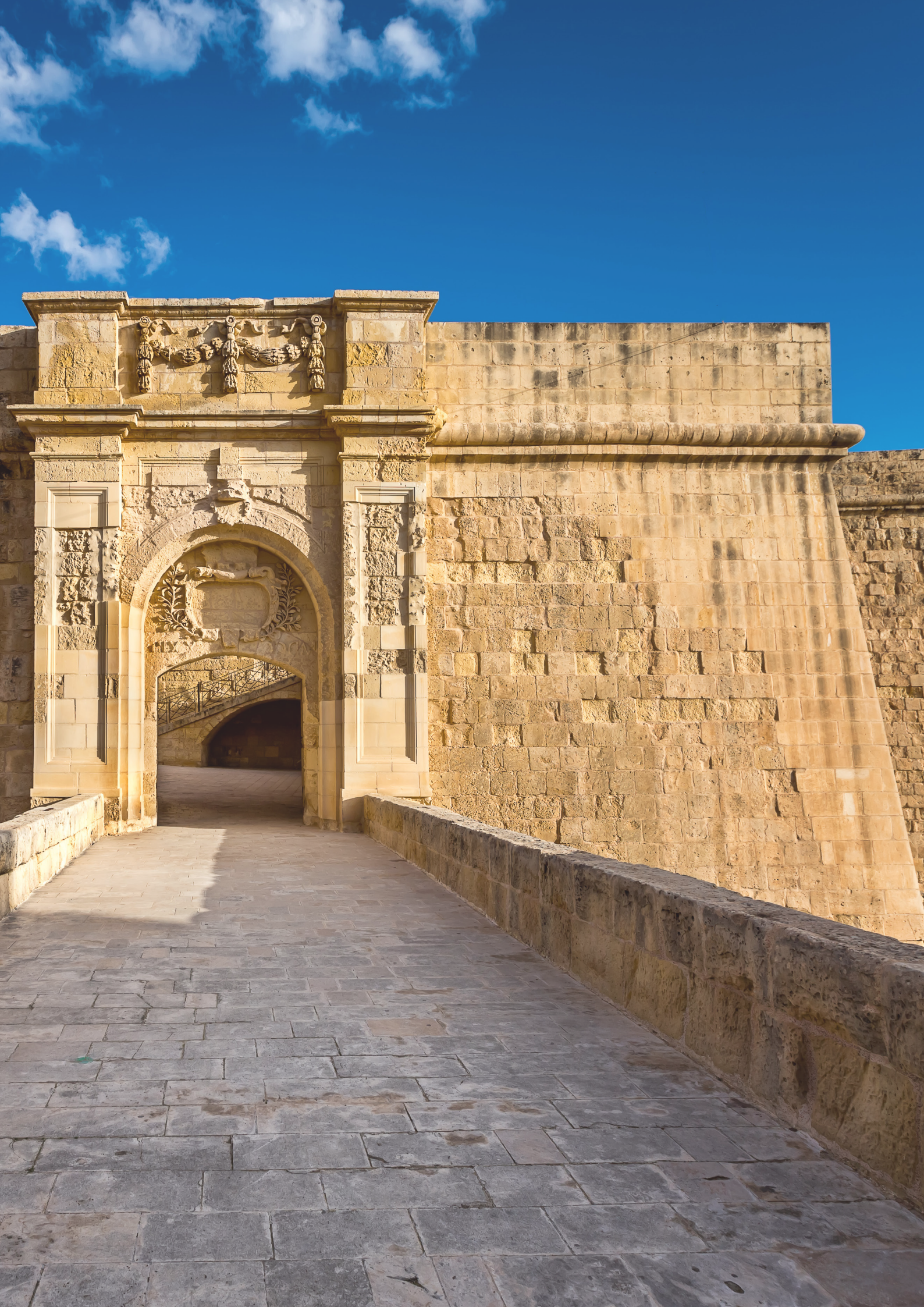
END NOTES

1. Adapted from the definition cited by the Cyber security Strategy of the European Union
2. Ross(2015)
3. Puricelli (2015)
4. Which could take the form of (i) a centralised approach – whereby a national authority has in-house responsibilities with all authorities reporting to it; OR (ii) a decentralised approach whereby roles and responsibilities are spread across a variety of actors who coordinate together to share information and exchange on a voluntary basis OR (iii) a semi-centralised (hybrid) approach whereby a central ministry coordinates implementation of the strategy with designated authorities having the necessary roles and responsibilities over operators and other stakeholders and who report to the central ministry on a periodic basis.
5. A top level coordinating CSIRT that acts as a key support to the strategy implementation function. Among the responsibilities of such CSIRT are:
    - Monitoring incidents at a national level
    - Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents
    - Providing dynamic risk and incident analysis and situational awareness
    - Establish cooperative relationships with the private sector
    - Facilitate cooperation through use of common or standardised practices for incident and risk handling procedures
6. European Commission (2015), DSI Maturity Study, p.29
7. Refer to Section 9 - 'Identification and Assessment of Stakeholders'of the Supporting document
8. Key market operators refers to providers of information society services, operators of critical information infrastructure and operators of Critical infrastructure that provide essential or critical services to critical information infrastructure. For more details, refer to the Section 9 – 'Identification and assessment of Stakeholders' of the Supporting document.
9. As part of Measure 3.4 – Conduct cyber defence exercises
10. ibid
11. ibid
12. European Agenda on Security: Questions and Answers, Strasbourg, 28 April 2015 - European Commission-Fact Sheet.
13. ibid
14. For example Austria and the UK
15. Such as those of NIST Cyber security Framework or potentially a similar initiative such as the UK's Cyber Essentials Scheme, **http://www.itgovernance.co.uk/cyber-essentials-scheme.aspx#.VaYNvLIBut8**

END NOTES

16. Potential areas that can be seen to also relate to cyber insurance, due diligence to third party with which businesses may seek strategic relationships,etc
17. Puricelli, op.cit
18. A similar approach has been taken by the Netherlands and Austria
19. For example social media, TV, radio, etc
20. Part from regular Euro barometer surveys dealing with cyber security which provide a significant insight on cyber security experiences and concerns on a domestic level.
21. For example apart from use of visual methods, rewards, social engagement and direct feedback during everyday working life; gamification may present one promising method. (Purcelli, op. cit, p.27)
22. Such policy is currently mainly applied by global and large organisations, and also by some EU member states such as the Netherlands. Reference is made to the Council of European Union meeting document 'non-paper on Fostering Cyber Security and Cyber defence in Europe by means of Responsible Disclosure Policies.
23. Reference is made to the Council Conclsuions on Cyber Diplomacy (2015) and to the Global Conference on Cyberspace (2015)
24. Time of review to be determined, following the consultation period. It is noted that such strategies normally have a time span of around two to three years.

NOTES



MALTA INFORMATION TECHNOLOGY AGENCY

mita.gov.mt/ncss