
NATIONAL
CYBER SECURITY
STRATEGY 2023 - 2026

Publication Date: **October 2021**

National Cyber Security Strategy 2023-2026

Contents

Foreword by the Minister for the Economy, European Funds and Lands

The fourth version of the Industrial Revolution is happening as we speak. No longer are disruptive technologies in the realm of science fiction; they are creating an abundance of possibilities for business, Government and humankind itself.

Malta's political will to embrace, adapt and adopt these seismic changes has positioned our country at the forefront of the technological revolution. Only a negligible number of countries have managed to emulate the pace of our country's progress in digitalisation and even fewer have recognised and fully embraced the potentiality of new technologies.

Our pioneering stance, with a wholehearted commitment to continue with the further implementation of technologies, has placed Malta as a leading digital innovator, a cut well above the rest of its European peers. The recent global health and economic challenges demonstrated our reliance on information and communications technology. Malta, by dint of its solid and unwavering commitment to digitalisation, has weathered the storm quite competently.

However, as empowering as our vision is, we also recognise that with great power comes great responsibility. While interconnectedness, through further implementation of technologies, shall allow us to forge further ahead in our administrative, business and personal activities, we shall continue to launch fiscal measures to strengthen Malta's appeal as a hub for foreign investment in this sector, while identifying the underlying skill base and infrastructure required for it to flourish. But not only this. As we have done in the past, with the launching of AI, Space, E-Commerce and E-Skills strategies, we shall continue to identify regulatory policies for the implementation of ethically aligned, transparent and socially responsible technologies.

We are also acutely aware of the dangers lurking within this field and recognise that it would be an exercise in futility if we do not ensure the maximum security and resilience possible in the face of relentless cyber threats. With the extensive growth of digitalisation, the exposure to cybercrime will increase inevitably and therefore the National Cyber Security Strategy 2023-2026 has been designed with our country's future wellbeing in mind. It lays the groundwork for further investment by Government in cyber security for the next three years. Government has a clear leadership role in cyber security, but it cannot act alone. Together, we can foster increased confidence and trust in the digital world. This includes a greater propensity towards cyber hygiene, a drive towards attracting minds within the cyber security domain as well as further co-operation on a national, European and global scale.

Ultimately, the cyber threat can never be discounted or ignored. The consequences of suffering a cyberattack would be massive, resulting in data loss, system outage and reputational damage. Unfortunately, it is a threat that can never be fully eradicated. The open nature of the cyber world shall always expose us to such risk, irrespective of measures taken. Nonetheless, together, we can minimise the level and impact of these threats, whilst successfully forging ahead in digitalisation. This Strategy will pave the way for such action.

Hon. Silvio Schembri

Minister for the Economy, European Funds and Lands

Foreword by the Minister for Home Affairs, Security, Reforms and Equality

The significant leaps we have made in digitalisation on a national scale in recent years has made us increasingly aware of the danger of threats within cyber space.

Cyber space is ever evolving, and it is an ever-growing dependency for our national security. It does not eliminate spatial boundaries. Its cross-border nature allows for anonymity, bringing about issues and challenges of jurisdiction, conflict and criminality. Cyber criminals are fully aware of this and are causing damage and harm, stealthily and craftily infiltrating systems from anywhere around the globe, stealing identity and sensitive data and defrauding unsuspecting organisations and individuals. They are targeting critical infrastructures upon which our day to day lives and activities depend and are exploiting vulnerable situations we face on a personal or wider scale, even fuelling uncertainty, fear and distrust through the spread of fake information.

The National Cyber Security Strategy 2023-2026 aims to protect our national interests in a planned and coordinated fashion for the next three years. The attainment and success of the Strategy is contingent upon a variety of diverse participants, not only within Government but also the private sector and Maltese society as a whole.

I am confident that we shall use this Strategy as an opportunity to all work together as one nation in a responsible and coordinated manner. Ultimately, cyber security not only protects our assets but ensures vigilance to the essential tenets of our free, European and democratic society in a time of heightened global digital transformation.

Hon. Dr Byron Camilleri
Minister for Home Affairs, Security, Reforms and Equality

Executive Summary

Heightened online activity at social and economic levels, spurred by further developments and applicability of Internet based technologies and concepts have led to bolder and more complex cyber threats. A global focus on health and economic risks has aggravated further the susceptibility to wider and bolder attacks by criminals.

Cyber attacks are also being increasingly orchestrated as part of a mixed array of tools by external state and non-state actors aimed at interfering with the stability, effectiveness, and legitimacy of the European Union and Member States. This calls for cyber security to be addressed as part of a broader whole-of-government approach which recognises the existence of such multi-faceted and multi-layered hybrid threats.

Government and society needs to be prepared and resilient. There is a need for cyber security to be addressed on a national scale with a planned, collective and systemic effort from all stakeholders. The National Cyber Security Strategy 2023-2026 follows an initial one published in 2016, which laid the foundation blocks for such an approach in Malta.

Several regulatory activities and initiatives in cyber security have occurred, or are in process, on a national, EU and global scale in areas such as network and information systems, electronic communications, technology and research competency, cross border public service delivery and information sharing and diplomacy.

Digitalisation, including wider diffusion and consumption of broadband, mobile technologies and data, has progressed further in Malta, with the Public Administration being at the forefront of related service provision, along with increased use of social and business digital interactions.

The National Cyber Security Strategy 2023-2026 is being articulated with such considerations in place, whilst allowing for evolving challenges and realities.

The Strategy is based upon four key principles:

- **Shared responsibility** of stakeholders in tackling cyber security. This is necessary to protect against and deter potential cyber-attacks as well as to respond to disruptions that do occur.
- **An inclusive, comprehensive and integrative approach** whereby cooperation, coordination and collaboration are ensured on a national, European and global scale.
- **Balanced risk management** that assesses cyber risk and takes a proportionate degree of measures, ensuring that innovation is not stifled in the process.
- **A balanced compliance approach** that engenders conformance to cyber security standards commensurate to the context and focus to which they are intended.

The principles need to be put into practice by the **Maltese public administration, the private sector and all Maltese society including a community of cyber security experts and practitioners.** Indeed, these stakeholders constitute the core of the Strategy's overall vision that:

Malta is more secure and resilient to cyber threats, leading to more trust and confidence within the digital world.

The Vision reflects continuity in Malta's pursuit of bolstering its cyber security and capability to return to normality within the shortest time possible in case of disruption due to a cyber-attack. No country, entity or individual can be totally immune from potential cyber-attack despite measures taken to protect against such an event. Ultimately, as indicated by the Vision, such a dual strategic thrust should lead to increased confidence and trust in a digital environment that enhances economic and societal activity.

The Vision reaches fruition through a number of proposed actions based upon sub-objectives emanating from the following four domains:

Domain 1: Cyber Security Governance Capacity

This domain aims to promote and maintain a robust cyber security governance framework so as to ensure that risks effecting Malta in cyberspace are adequately addressed. They are to be tackled from legislative, regulatory, policy, standard and best practice aspects and, most importantly, from a risk management and supplier management perspective.

Domain 2: Cyber Defence Capacity

This domain is based upon the premise that the complexity of cyberspace makes it hard to prevent all attacks, which, in a number of instances, are likely to be more disruptive and costly than natural disasters. Hence, it aims for a stronger multi-stakeholder concerted effort, in terms of operations, for dealing with cybersecurity challenges from a reactive as well as a proactive perspective, including consolidating and sharing cyber threat intelligence.

Domain 3: Cyber Competence and Culture

This domain recognises that cyber security needs to be addressed from a human resource and cultural perspective. It focuses on the academic and training aspects of cyber security in various professions and the need to establish a strong *security first* ethos. The establishment of a National Coordination Centre, in line with EU legal requirements, shall be instrumental. It shall also promote research development and innovation in cyber security.

Domain 4: International Cooperation

This domain aims to foster active cooperation and engagement by Malta at bi-lateral, multi-lateral, European and international levels in areas of international security in cyberspace, cyber capacity building, cyber response and cybercrime.

The actions proposed by each of the four domains translate into more specific activities which are assigned to respective owners for implementation within stipulated timelines, as part of an Action Plan.

In general, though, resources in cyber security on a national scale are limited, and technology and its use keep on evolving, leading to new cyber security challenges. Additionally, the regulatory landscape in cyber security is evolving, particularly at EU level, leaving its mark on Malta as a Member State. Thus, coordination and monitoring of progress of the Action Plan, through the National Cyber Security Steering Committee, shall be accompanied by regular reviews to reflect these considerations over the next three years.

Whilst the National Cyber Security Strategy 2023-2026 acts as the national focal point on cyber security from a strategic perspective, it shall not exclude related strategies focusing on sectors/disciplines of Maltese society and its economy.

Cybersecurity is a global concern of national importance. Hence it is in everyone's interest to ensure that it is addressed effectively.

Acronyms

AI	Artificial Intelligence
ASEAN	Association of Southeast Asian Nations
ARF	ASEAN Regional Forum
AU	African Union
CBM	Confidence Building Measures
CoE	Council of Europe
CSIRT	Computer Security and Incident Response Team
DORA	Digital Operational Resilience Act
DSP	Digital Service Providers
ENISA	European Union Agency for Cyber Security
EC	European Commission
EU	European Union
EU CCCN	European Cyber Security Industrial, Technology and Research Competence Centre and Network of National Coordination Centres
EuroQCI	European Quantum Communication Infrastructure
FDI	Foreign Direct Investment
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IOC	Indicators of Compromise

ITA	Innovative Technology Arrangements
IXP	Internet Exchange Points
LN	Legal Notice
NATO	North Atlantic Treaty Organisation
NIS	Network and Information Security
OAS	Organisation of American States
OES	Operators of Essential Services
OSCE	Organisation for Security and Co-operation in Europe
OECD	Organisation for Economic Co-operation and Development
OOP	Once Only Principle
R&D	Research and Development
RDI	Research Development and Innovation
SOC	Security Operations Centre
SME	Small to Medium sized Enterprises
UN	United Nations
UN GGE	UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the context of International Security
UN OEWG	UN Open-Ended Working Group on Developments in the Field of ICTs in the context of International Security

chapter 01

Strategic Context

1.1
Background

The demands of cyber security[1] on society and the economy are an increasingly evolving challenge in an era of digital transformation. The global pandemic has further accentuated the use of digital activity with remote ways of working, interacting and doing business. It has increased dependency on digital platforms and technologies by organisations and individuals.

Cyber-attacks[2] have increased relentlessly, in sophistication and in ubiquity. They have been spurred by further growth in internet connected technologies such as e-commerce, the Internet of Things, social media, mobile payments and cloud computing.

International conflicts show that, escalated disputes between nation states are incorporating cyber space. Thus wars are being fought through rigorous cyber-attacks on nation states, with the intent to disrupt a country's stability.

An increased dependency on technology in matters from health to the economy aggravates further the susceptibility to wider and bolder attacks by criminals. Therefore, cyber-security cannot be tackled in isolation. There needs to be a concerted and strategic approach that keeps in view of the increasingly digital ecosystem nationally and internationally.

This Strategy is Malta's second in cyber security, following the previous one published in 2016. The first Strategy provided the foundation, outlining a series of actions that need to be addressed. It sought to align itself to the requirements of the EU 2016/1148 Directive of the European Parliament and Council of 6 July 2016 concerning 'measures for a high common level of security of network and information systems across the European Union' (EU)[3]. This was the first piece of EU-wide legislation on cyber security which, at the time of publication of the Strategy, was still not applicable across Member States

but which has since been transposed into Maltese network and information security legislation as L.N. 216 of 2018[4]. Awareness of the need to deal with cyber security on a national scale came with the implementation of a strategic awareness and education campaign, which, along with other measures such as those related to cybercrime and further activities involving multi-stakeholder cooperation, were proposed by the initial Strategy.

The General Data Protection Regulation (GDPR) has also come into force since then, increasing awareness on cyber matters, albeit from a privacy perspective, particularly within businesses[5]. One cannot discount the further evolution of digitalisation in all of the nation's economic and societal spheres which, though positive, also pose higher probabilities of cyber risk.

In recent years, a higher share of online sales has been indicated by Maltese businesses relative to their EU counterparts[6], whilst there has been a consistent growth in online purchases by Maltese consumers[7]. Indeed, online social[8] and business interaction[9] have maintained an upward trend, spurred by an increased growth in broadband penetration[10], mobile telephony usage and data consumption[11]. Government maintained momentum in being at the forefront in digital service provision of public services[12]. The digitalisation of Malta's Public Administration[13], enabled by strategic approaches in its adoption of mobile telephony and technologies including AI[14], continues at a steady pace, in line with EU related developments. The Single Digital Gateway Regulation, now in force, provides the basis for EU-wide implementation of the once-only principle (OOP) and is expected to be applied at cross border level by 2023. The 2020 legislation *Re-use of Public Sector Information Act (CAP 546)* facilitates implementation of the OOP, whilst extending the definition and concept of re-use of documents within the Public Administration. Additionally, the implementation of the EU Digital Single Market Strategy calls for high-speed, secure and trustworthy infrastructures and services supported by the right regulatory conditions. Indeed, in 2018, Malta took a proactive stance by introducing a new regulatory framework on innovative technologies[15].

All such developments call for various multi-disciplinary cyber security measures to counter increased possibilities of technology, data and, ultimately, service compromise. Furthermore, it is increasingly clear that cooperation and coordination at a European and international level is crucial in addressing cyber security effectively.

In December 2020, the European Council and the European Parliament reached a provisional agreement on a proposal to set up a European Cyber Security Industrial, Technology and Research Competence Centre and a network of national coordination centres to invest in stronger and pioneering cyber security capacity in the EU. Additionally, new EU regulations set out a European cyber security certification framework for Information and Communications Technology (ICT) products, services and processes, in addition to granting a permanent mandate to the European Union Agency for Cyber Security (ENISA). The European Commission (EC) has also presented a new EU Cyber Security Strategy which aims to introduce an agile means for detecting and deflecting cyberattacks across Europe while strengthening internet security globally, fostering information sharing and collective responses, enhancing cyber defence cooperation, strengthening further the EU cyber diplomacy toolbox, strengthening external cyber capacity building, actively contributing to international security in cyberspace at UN level and ensuring security in the Internet of Things[16]. The Strategy complements a number of legislative proposals that have been made at European level such as those related to an EU wide cyber diplomacy toolbox, 5G cyber security and a wider in scope Network and Information Security Directive, among other proposals some of which are largely sectorial in nature.

Therefore, whilst the strategic approaches of the initial National Cyber Security Strategy are still valid, societal, political, economic and technological evolvements at a national and European level need to be kept in view.

Ultimately, increasing complexity, coupled with a constantly changing scenario within cyber security, calls for a multi-disciplinary effort that factors in the relevance and horizontal nature of cyber security, addressing it in a systemic, comprehensive and coordinated manner.

1.2

Purpose and Scope

This Strategy intends to serve as a continuation to the National Cyber Security Strategy 2016. It aims to deliver further progress by:

- Aligning to specific domestic, EU and international regulatory requirements.
- Taking into account of present realities, challenges and evolvements in cyber security on a national and global scale through a number of strategic, operational and cultural measures, beyond the regulatory ones.

Whilst encouraging the articulation of Cyber Security Strategies and their subsequent implementation at an organisational or even business sectoral level, the National Cyber Security Strategy 2023-2026 is wider in scope, ensuring that its overall implementation has a nationwide impact. It has several objectives with timely, speci ic and actionable measures, aimed at:

- Strengthening protection of digital infrastructure and its dependencies on a national scale, not only from a technological point of view but also from strategic, operational, legal and regulatory perspectives.
- Ensuring a cyber risk assessment approach across the business and economic sector.
- Ensuring national cyber security consciousness and increased capabilities in cyber security.
- Fostering cooperation in cyber security on a national, European and international scale.

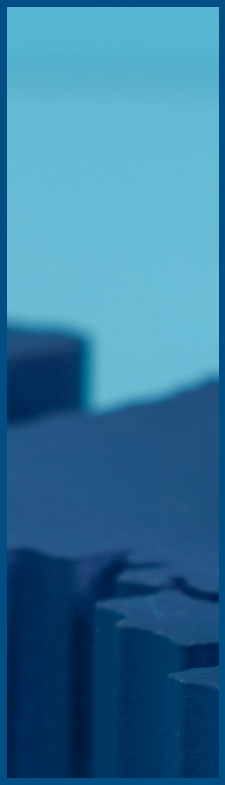
These measures apply for all stakeholders of the Maltese economy and society as increasingly active participants in cyber space as well as contributors to its security and resilience.

chapter 02

Overall Direction

2.1
Introduction

This Chapter sets the scene for the National Cyber Security Strategy 2023-2026, in light of the considerations detailed in the previous Chapter.
It outlines the principles underpinning the Vision of the Strategy for the next three years. The Vision is seen to come into fruition by means of a Model with four domains, each encapsulating a number of objectives to be reached.



2.2

Guiding Principles

The Strategy shall be guided by four principles, all of which call for a balanced, multi- disciplinary and multi-stakeholder approach, encapsulating the notions of subsidiarity, complementarity and proportionality.

Shared responsibility

In essence, this is a principle of subsidiarity, whereby cyber security is a shared responsibility between all stakeholders. The Government assumes a leading role but cannot have sole responsibility and accountability given that the private sector, as well as society as a whole are also users, beneficiaries and owners of infrastructure. They too contribute to a secure and stable cyber space. Hence, all users have the responsibility of taking steps to protect the cyber landscape on an individual and collective basis. They all need to be aware of privacy protection methods and of ensuring security against cyberattacks.

Inclusive, Comprehensive and Integrative Approach

The interdependencies inherent within the connectedness of cyber space, and the potential consequent spread of impact from a related incident, call for complementarity action and shared trust. This is enabled by cooperation, collaboration and coordination mechanisms amongst the various stakeholders on a domestic, European and international scale.

Balanced Risk Management

The continuous growth and evolvement of cyber space renders it impossible to guarantee a scenario devoid of risks from any form of threat. Risk management is an ongoing concern that covers all elements of cyberspace in terms of their constitution as well as their use. It does not come without cost. Thus, the allocation and adequacy of resources needs to be proportionate to the risk identified, within its particular context, and to the course of action to be taken. Overall, risk management should not stifle innovation but reflect a proportionate level of investment that allows for its secure utilisation.

Balanced Compliance Approach

Additionally, apart from risk management, within the notion of proportionality is the need to establish and ensure compliance to necessary security safeguards and measures that are commensurate to the context and to what needs to be protected within the cyber space domain.

2.3
Vision

Taking into perspective these principles, the overall cyber security scenario, as well as Malta's drive towards attaining further **social and economic progress** through **digital evolution**, the following overall Vision shall guide the National Cyber Security Strategy for the next three years:

> **Malta is more secure and resilient to cyber threats leading to more trust and confidence within the digital world.**

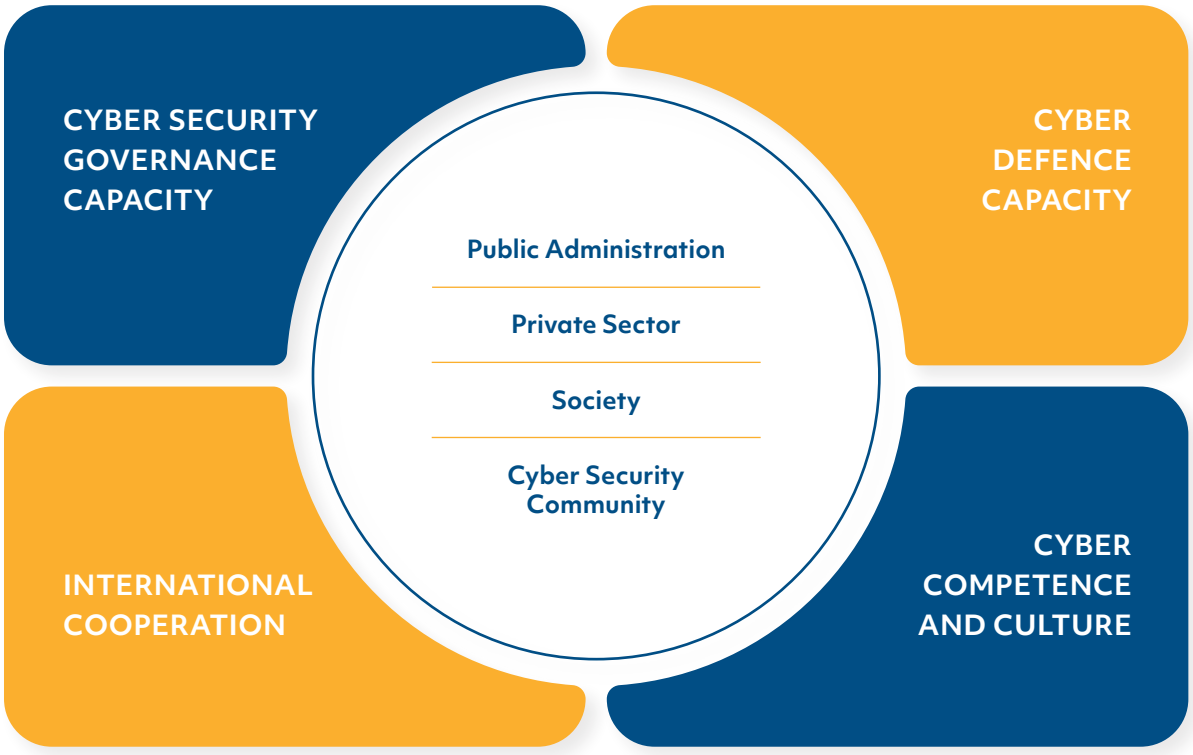
The drive towards further cyber resilience and cyber security will serve to underpin trust and confidence in the use of digital facilities which can enhance economic and societal activity for all.

2.4

Model

The components bringing the Vision to fruition can be summed up through the following model which encompasses the:

- Key National Stakeholders at its core.
- Four Key Domains, all inter-related, that need to be tackled.



2.5

Key National Stakeholders

The vision is all encompassing in that it involves the main national stakeholders, entailing that:

- **The Public Administration leads the way in ensuring secure and resilient cyber space on a nationwide scale.**
- **The Private Sector cooperates with the Public Administration, securing its product/service portfolios and protecting its client bases from known cyber vulnerabilities.**
- **Society practices secure online behaviour and makes informed decisions on digital transactions and interactions.**
- **The Cyber Security Community of individuals and organisations, that significantly contribute to the Maltese cyber-security scene in a professional capacity or otherwise, is encouraged to grow further to play an increasingly crucial role.**

Not everything can be protected against every type of threat and risk but each of the stakeholders has roles and responsibilities which clearly reflect the underlying principles of shared responsibility and cooperation and coordination by all. Technical security needs to be further strengthened, but human factors have to be taken into account too since they are the underlying cause of cyber incidents or the key vector to exploit for cyber-attack. Hence, stakeholders' obligations inherently carry such needs and expectations by the stakeholders themselves that need to be fulfilled accordingly. The four domains presented within the model embody such perspectives to ensure a comprehensive and inclusive approach.

2.6
Key Domains

Four domains, which aim to address the domestic and international evolvement of the cyber security landscape, have been identified.

Domain 1: Cyber Security Governance Capacity

Governance is a key element in cyber security as it determines the responsibility and accountability structure, ensuring oversight to mitigate cyber risks. On a national scale, it stipulates the laws, regulations, policies, processes, standards and best practices required to determine how the country can respond to and limit cyber incidents effectively.

Domain 2: Cyber Defence Capacity

Cyberspace has become so complex that preventing all attacks is impossible. Such attacks can be exponentially more harmful and costly than damage caused by natural disasters. This challenge is addressed through the capacity to conduct continuous monitoring for potential threats, rapid detection of potential attacks, ensuring a network of information sharing and coordination and, ultimately, being in a position to respond to occurrences of cyber disruptions effectively. Technology, along with the suitable skills and processes to detect and respond, acts as one key enabler to defend against cyber threats.

Domain 3: Cyber Competence and Culture

In addition to political, technological, organisational and legal measures, a progressive digital culture is needed and this comes from a strong capacity building regime. Capacity building includes ongoing and comprehensive cyber security awareness programmes to promote and foster a *security-first* culture. It also includes competence and knowledge development through certifications, increased academic focus on cyber security and professional training and educational programmes targeting not only ICT practitioners but also professions in other fields. Human and institutional capacity building in cyber security and its human, socio-economic and political implications cannot be side-stepped so cyber security must not be addressed from a technological perspective only.

Domain 4: International Cooperation

Cyber security is a global challenge. It knows no bounds of national territory or sectoral scope. Thus, it requires a multi-stakeholder approach involving cooperation from various functions and disciplines, nationally and internationally. It calls for strategic engagements such as bi-lateral and multi-lateral agreements, participation in European and international fora, co-operation and information sharing frameworks and agreed international/European related norms of behaviour. Apart from indicating a country's willingness and commitment to the peaceful use of cyberspace, international cooperation can strengthen capacity building, threat detection and deterrence capabilities as well as increase the scope of enforcement and judicial powers in tackling cybercrime.

2.7

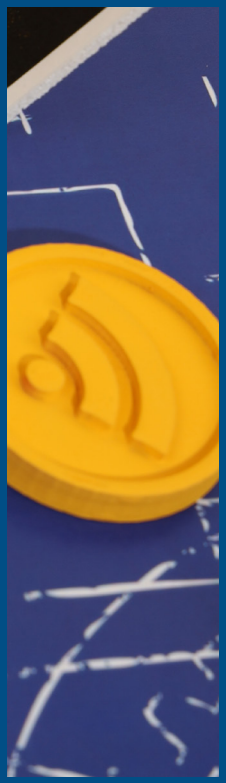
Focus for each Key Domain

The next four Chapters expand each corresponding domain in further detail. Each domain shall carry an overall objective, in line with what the domain embodies. In turn, the overall objective embodies a number of sub-objectives, each of which include a strategic context and rationale, leading to a number of proposed high-level actions that are envisaged for realisation of the Strategy.

chapter 03

Cyber Security Governance Capacity


CYBER
SECURITY



3.1
The Key Objective

Promote and maintain a robust cyber security framework of responsibility, accountability and strategic direction to protect, respond to and minimise threats and challenges that compromise the security of Malta in cyberspace.

3.2
The Sub-objectives

A. Adaptation of the domestic legal framework to meet changing needs and challenges in cyber security.

The legal framework, including legislation and regulation, ensures Malta's ongoing preparedness in terms of response through investigation and prosecution of cybercrimes, the imposition of appropriate sanctions for non-compliance or breach of law as well as the basis for a level of appropriate behaviour expected within cyberspace. The increasingly global, complex and dynamic nature of cyber security challenges necessitate the need for a domestic review and update of such legal measures to ensure their currency and relevance, including alignment with EU legal developments.

The transposition of EU Directive (EU) 1148 of 2016 (NIS) into Legal Notice L.N. 216 of 2018 led to the identification of its National Competent Authority of the National Computer Security and Incident Response Team (CSIRT). It has also defined the Operators of Essential Services (OESs) and the Digital Service Providers (DSPs) within the local context. This led to the implementation of security and notification requirements and several cooperation and coordination mechanisms. Such activities shall continue, with a focus on having a more comprehensive list of OESs, as well as further policy direction regarding the obligations of both OESs and DSPs.

The transposition of the legal framework for security and integrity of networks and services, as well as other related EU regulatory requirements, complements this further. Specifically, in early 2020, the EC called on Member States to take steps to implement the set of measures recommended in the 5G toolbox conclusions[17]. The growth of 5G will enable newer connection and service opportunities spurred by higher transmission rates and lower latency, their potential criticality of which would render them highly susceptible to cyberattack.
Other legislative proposals, related to cyber security, have been made at European level during 2020, such as that for a renewed Network and Information Security Directive and a Digital Operational Resilience Regulation (DORA) for the Financial Sector. The latter sector is increasingly reliant upon information and communications technologies through an increased demand in Europe for remote access to financial services[18]. This has led to a significant rise in cyberattacks on financial institutions[19], which call for increased risk mitigation in their digital transformation so as to ensure stronger operational resilience through the Regulation. The Regulation also complements the EU Digital Finance Strategy which, as part of an EC Digital Finance Package, aims to foster customer access to innovative financial products whilst ensuring consumer protection and financial stability[20]. Thus, the importance for such robust cyber security regulation within the financial sector, as well as in sectors such as gaming and the services industry, is vital within the Maltese economic context[21]. One particular notion that is gaining importance at EU level is vulnerability disclosure. This would enable well-intentioned individuals to investigate and report, in a safe and transparent manner, systems vulnerabilities they have detected without incurring the risk of criminal action against them.

However, cyber security legal frameworks cannot simply be devised around interests of legal entities and the personal lives of individuals. It is increasingly the case that cyber breaches may be specifically intended to impair the security, sovereignty and integrity of a nation. This is compounded by the fact that cybercrime knows no geographical boundaries and the inherent possibilities of anonymity in cyber space make it harder to attribute with certainty.

This in turn may potentially cause grave diplomatic consequences between states, calling for increased focus on nation state behaviour in cyber space as well as diplomatic preparedness in case of related transgression. Developments at a European scale have become increasingly crucial following the introduction in June 2017 of the EU cyber diplomacy toolbox through the *Conclusions on the Framework for a Joint EU Diplomatic Response to Malicious Cyber activities*. In addition to participating at a European level, Malta is also actively contributing to work being done by the UN Group of Governmental Experts on Advancing responsible state behaviour in cyberspace and by the UN-mandated Open-Ending Working Group on Developments in the Field of ICTS within the context of International Security. However, Malta still needs to clarify its position with respect to the applicability of international law in cyberspace. Malta would then be in a stronger position to play a role in international cyberspace policy.

International legal and regulatory developments have had an impact upon various parts of the Maltese legal framework. Cyber security has also been addressed in other parts of the domestic legal framework such as the Criminal Code. Hence there is a need for a consolidated view of the various legal and regulatory references on cyber security within the Maltese legal framework for a better and more comprehensive understanding of its coverage and its applicability.

ACTIONS	
1.1	Establish a consolidated view of the coverage and applicability of cyber security within the Maltese legal framework.
1.2	Review and update the national legal framework to ensure its currency with respect to the cyber security challenges in an increasingly digital economy and society in areas including: • **Cybercrime investigations and electronic evidence.** • **Transposition of new EU cyber related Legislation (sectoral or otherwise), within stipulated timeframes, following agreement by the EU Council and European Parliament.**
1.3	Adopt and implement measures resulting from cyber/cyber-related regulations and legislation nationally.
1.4	Establish Malta's position on (i) cyberoperations against it in peacetime and (ii) applicability of international law with respect to cyberoperations in armed conflict situations, keeping in view related EU requirements.
1.5	Issue a Vulnerability Disclosure policy covering critical areas falling within the scope of Maltese network and information systems security legislation for reporting parties such as security experts and consultants.
1.6	Issue vulnerability disclosure policies or guidelines, as well as other cyber security specific policies or guidelines within specific economic sectors, as applicable.

B. Ensure consolidation of national cyber security at a strategic level.

The publication of a National Cyber Security Strategy alone is not sufficient for ensuring effective harmonisation in cyber security strategic development. The National Cyber Security Committee, composed of diverse national stakeholders in cyber security, is one means of facilitating the conduct of cyber security efforts in a coordinated fashion. However, as the cyber security challenge becomes more intense, there is a need for a stronger strategic role to ensure improved governance, including more effective implementation of the Strategy. There is a need to promote further engagement and interaction with other stakeholders within the realm of national cyber security to ensure the dissemination of cyber security knowledge, best practice and expertise.

ACTIONS

1.7 Work to consolidate further the National Cyber Security Committee's role, ensuring consolidation of national cyber security at a strategic level.

C. Strengthen cyber security in the supply chain.

A high level of security of network and information systems and, ultimately, trust of digital processes and services calls for a supply chain that complies with widely recognised security standards and protocols. Such degree of security compliance is expected from the inception of digital products, processes or services, calling in effect for the implementation of the *security by design* concept.

The EU Cyber Security Act, which entered into force in 2019, reinforces such notion of quality assurance in the supply chain through a proposed introduction of EU wide rules for cyber security certification of products, processes and services, which are currently being followed by Malta.

Furthermore, the European Electronic Communications code, being transposed on the domestic front, shall ensure that the integrity and security of public communications networks are maintained with risks related to the security of networks and services appropriately managed. The code includes further regulatory powers to enforce security provisions.

Malta has taken its own regulatory initiatives that contribute to bolstering cyber security within the supply chain, especially in innovative technologies being adopted in day-to-day business and personal life at a rapid pace. In 2018, it introduced a new regulatory framework for the voluntary certification of Innovative Technology Arrangements (ITA). Among other activities, the Regulation led to the introduction of an ITA Certification Programme for Digital Ledger Technology/ Blockchain based systems. An equivalent programme for Artificial Intelligence-based systems, to ensure ethical alignment, transparency and social responsibility in their development, was also devised [22]. Moreover, network and information systems security legislation supports the use of internationally recognised cyber security related standards by entities falling within its scope of applicability. From a policy perspective, in 2017 a Government Information Security Policy[23], based upon the internationally recognised ISO 27001 Information Security standard, came into force. This policy is applicable to all of the Public Administration. Further entity specific information security initiatives have taken place to promote a cyber security ethos within the Public Administration. Other economic sectors are also applying such a security standard.

Increasingly, regulatory technical standards related to cyber security are being mandated as part of regulation in sectors such as financial services[24]. However, EU Regulation 2019/452, which became applicable in October 2020 and aims to establish a common system among EU Member States to screen foreign direct investments (FDI), calls for an even more in-depth focus on cyber security from a supply chain perspective at a national level. This comes from a desire to exercise greater control over economic activities within Member states, in light of recent economic and global health developments[25]. This Regulation allows for ad hoc screening mechanisms on operations where this is potential impact on security and public order, with an additional instrument to protect strategic activities. According to Article 4 of the Regulation, the potential effects on critical infrastructure (whether physical or virtual), critical technologies, including cyber security[26], and access to sensitive information are factors to be considered in determining whether or not a foreign direct investment may affect security or public order.

ACTIONS	
1.8	Actively participate in the design of the European wide cyber security evaluation and certification framework, eventually ensuring its implementation in Malta.
1.9	Adopt and promote sector specific standards, best practices and/or guidelines related to the security of networks and information systems in collaboration with the national body for accreditation and standardisation[27].
1.10	Further promote Government ICT Policy on Information Security within the Public Administration and review it periodically to ensure that it reflects the evolving cyber security profile within Government.
1.11	Propose a standard set of information security provisions within Government procurement framework for digital products and services.

D. Implement cyber risk management on a national scale.

The increasing digital inter-connectedness between infrastructures, networks and various organisations – several of which are essential to the country's day to day running - implies that a deficiency in one area can cause major disruption across others. Hence, risk management must focus on cyber, as well as natural and human hazards that may compromise a country's stability and security. Recent proposals at EU level, with respect to the new five-year term EU Cyber Security Strategy as well as to a Directive on the resilience of critical entities, highlight such a need.

Network and information systems security legislation addresses the need for cyber risk assessment exercises nationally, and specifically within the critical areas it identifies. However, cyber risk assessments are not a one-off exercise and should not be limited to those falling within the scope of legislation. Risk factors in any digitalisation process within organisations are numerous; they include concerns about the nature of the security of new systems introduced, privacy of data and ethical use of technology or its data. The risk is amplified by emerging technologies since the unknowns are greater than with mature technologies. The requirement for appropriate oversight of digital transformations intensifies the need for a strong cyber risk management regime within organisations.

Additionally, the proposed EU Cyber Security Certification framework should contribute to the development of tailored and risk-based EU certification schemes that would specify the *intended level of assurance* of products, services and processes. These are crucial for the proper functioning of the European Digital Single Market, of which Malta forms part. [28] The same goes for certification frameworks introduced in Malta with respect to Innovative Technology Arrangements, referred to in the previous sub-objective, related to cyber-security in the supply chain.

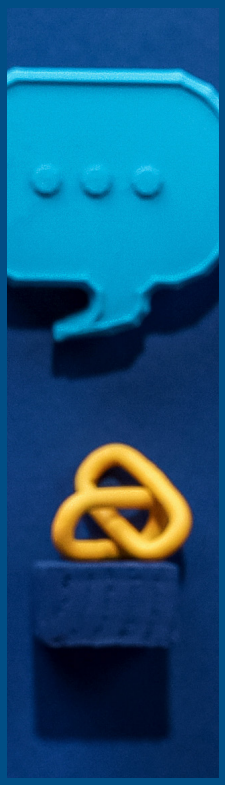
Above all, a watchful eye on a national scale for any noted emerging misuse or malign use of digital technologies and data and collective efforts to mitigate such risks is needed.

ACTIONS	
1.12	Ensure regularly updated cyber risk assessments, both nationally and on a sectoral scale, with the implementation of measures required.
1.13	Ensure regular conduct of individual cyber risk assessment exercises by all organisations falling within the scope of Maltese network and information systems security legislation.
1.14	Seek to encourage the management of cyber risk in organisations nationally.
1.15	Seek ways nationally to mitigate risks related to emerging misuse or malign use of digital technologies and data.


CYBER SECURITY MALTA
Digital Security Your Priority

chapter 04

Cyber Defence Capacity



4.1

The Key Objective

Strengthen commitment to augment operational and cooperation capacity to prevent and defend against cyber threats and address cybercrime, including cyber-attacks that may undermine Malta's security.

4.2
The Sub-objectives

A. Maximise national security and defence information capabilities to ensure technical and operational capability as well as national and international cooperation and coordination in cyberspace.

Any organisation or even a nation thriving upon digitalisation derives value not only from preventing cyber-attack but also from responding promptly and coherently when an attack occurs, so as to minimise its effect.

Through network and information systems security legislation, an incident management process, especially for significant cyber incidents in critical areas in Malta as well as incident reporting requirements at EU level, has been established. The primary incident responder, in case of a major cyber incident involving Government, has also been identified. Such developments have been an essential step in bolstering security in areas where cyber activity is critical.

However, the need to ensure a more inclusive response to threats and hazards is growing as the ramifications of cyber-attacks are felt domestically and worldwide. Indeed, recent EU Council conclusions called for such a need in the light of increased vulnerability to hybrid threats[29] posed through 'malicious cyber activities, disinformation and threats to economic security'[30]. Ultimately, cyber security is like a chain - it is as strong as its weakest link. Hence, the need to identify and engage more multi-functional stakeholders not necessarily covered by present cyber legislation.

Ultimately, this exercise is aimed at fostering national cooperation to detect threats, mitigate vulnerabilities, share cyber threat intelligence and coordinate responses to cyberattacks, as expounded further within the following sub-objective.

ACTIONS

2.1 Ensure that all stakeholders of Malta's national security and defence information systems and networks are identified on an ongoing basis, keeping in view pertinent legislation.

B. Establish a National Cyber Security Response Centre.

Closely tied to the requirement for comprehensive identification of all national stakeholders in cyberspace is the need for a centralised operations, cooperation and coordination framework, utilising all expertise. Through such framework, stakeholder organisations shall still operate independently on a day-to-day basis, whilst stronger mutual collaboration is ensured, when and where necessary.

Apart from serving as a means to a more structured and effective response to cyber security incidents, the framework will serve as a powerful collective mechanism to better understand a constantly changing cyberspace, as well as serve towards further education and increased cyber security preparedness. In the process, it may also serve to promote cyber threat intelligence on a wider national scale.

Cyber criminals and attackers scale up their efforts through stealth and sophistication whilst defenders gradually update their security measures. Cyberspace is diverse in its topological structures, networks and types of users. It is an uncertain place characterised by difficulties in traceability of perpetrators, inconsistencies and constant change. The sheer scale of data generated in online activity and traffic make it very hard, if not impossible, to inspect each and every event. From the defence perspective, this calls for an early warning system to alert cyber perpetration. Such a system should not simply rely on the availability

of the appropriate technology and skills. It calls for cooperation, streamlined coordination and collaboration processes, especially for data sharing and fusion. This may be achieved through the proposed centralised operations and cooperation framework and could be facilitated further by the promotion of voluntary information sharing about security breaches and incidents[31].

The early warning system could serve as the central mechanism for handling creeping, slow-burn and sudden crises[32] from cyber-attacks with the potential to cripple parts or all of the country's economic and social systems. Ultimately, it should contribute to the development of integrated cyber threat intelligence capabilities involving multiple sources.

The Government is actively contributing to cyber threat intelligence online through CSIRTs, Indicators of Compromise (IOCs) and threat and malware information so as to facilitate effective detection and preventive action in real time. Additional multi-stakeholder collaboration would see further contributions.

The ultimate aim of this sub-objective is to intensify cooperation and cyber security information sharing.

ACTIONS	
2.2	Define, agree and implement an operations, coordination and cooperation framework for cyber security response on a national scale, incorporating all identified stakeholders.
2.3	Establish an early warning system as part of the formation of an operational, cooperational and coordination framework for cyber security response.
2.4	Seek ways to promote further cyber security information sharing, voluntary or otherwise, involving the Public Administration, the private sector and society. This could be enabled through policy direction, agreed procedures and information sharing tools.

C. Conduct security monitoring of cyberspace.

CSIRTs and Security Operations Centres (SOCs) are important means of constant monitoring and analysis to detect intrusions and anomalies in real-time, in addition to allowing cyber threat intelligence exchange amongst stakeholders.

The National CSIRT and Government CSIRT already play important roles in coordinating incident management and in contributing to cyber threat intelligence at a national level. This is facilitated by cooperation networks of EU and international counterparts, as well as by investments in tools for detection and data dissemination. However, this does not exclude the need for other CSIRTs at organisation and sectoral level.

Collaboration and sharing among various CSIRTs would further strengthen their role and the sustainability of the country's cyber security ecosystem.

A SOC has been established for enhanced cyber monitoring and threat detection capabilities within Government. It is a vital tool for contributing to information security investigations within the Public Administration, such as for law enforcement and auditing purposes. Further investments to consolidate security monitoring of cyberspace are envisaged. The proposed development of an EU wide network of SOCs, as part of the EU Cyber Security Strategy, may consolidate further the establishment of such centres. This in turn would enhance collective knowledge, sharing of best practice and, ultimately, more comprehensive situational awareness.

The establishment of the national cyber security response centre, referred to earlier, should also complement further to such sub-objective.

ACTIONS	
2.5	Plan further and secure investments to monitor cyber security of critical infrastructures and critical information infrastructures, including Government.
2.6	Ensure ongoing risk management and resilience of such key areas.
2.7	Establish a network of SOCs and a community of CSIRTs in Malta.

D. Investigation and prevention of crimes committed in cyber space.

According to the 2019 Eurobarometer survey on Europeans' attitudes towards cybercrime, fewer Europeans feel they can protect themselves sufficiently: 59%, down from 71% in 2017, even though cybercrime awareness is rising. Cybercrime continues to be a global menace, increasing in terms of sophistication and expense. The recent surge in the world's population working remotely and online[33] has opened further avenues for cyber-criminals[34]. In the case of Malta, experiences of cybercrime registering a higher incidence than the EU average were claimed, particularly in relation to online fraud involving ransomware, virus and malware exposure, fraudulent emails or phone calls and online banking[35].

One of the three priority areas of the EU's Security Union Strategy 2020-2025 is fighting crime in a digital age, ensuring Member States have the necessary tools to do so and to engage in information exchange. Further investments and capacity building are taking place, nationally, including enhancing laboratory facilities for cybercrime investigations.

ACTIONS	
2.8	Invest in new tools and equipment to enhance cybercrime capabilities in investigation and prevention, both from a proactive and reactive perspective.

E. Conduct ongoing threat and vulnerability analysis.

An essential element of cyber security is having the capability to assess threats and vulnerabilities within and across organisations to ensure proactivity and preparedness. Various measures using processes, standards, best practices and technical tools need to be applied.

Network and information systems security legislation specifically calls for simulated runs of operator security plans in the critical areas identified. A number of cyber simulation exercises, forming part of wider EU-wide initiatives, have been conducted since the launch of the initial Strategy. Cyber simulation exercises act as training processes, making management, employees and organisations aware of potential threats and how to respond efficiently.

The Government regularly conducts scans and penetration tests on its web applications, looking for known vulnerabilities as well as to determine the degree to which a malicious attacker might impact confidentiality, integrity and availability.

There is a need to promote such threat and vulnerability analysis in the private sector too, in collaboration with Government stakeholders and service providers, taking into consideration human and financial resource limitations, particularly among Small to Medium sized Enterprises (SMEs).

The Government also issues advisories related to vulnerabilities on devices and software, together with relevant mitigation measures and security updates.

The proposed actions shall further develop and intensify efforts in the establishment of ongoing monitoring of vulnerabilities and threats so as to maintain a level of cyber security that is proportionate to the risk.

ACTIONS	
2.9	Sustain a programme of regular testing of digital networks and automated scans of Government critical infrastructure and services and devise a framework to facilitate a similar programme for testing of Government non-critical infrastructure and services.
2.10	Conduct pen testing and red-teaming exercises in critical areas.
2.11	Actively promote the conduct of vulnerability assessment exercises within the private sector.
2.12	Promote further an automated National Cyber Notification System whereby notifications on security vulnerabilities are sent to Internet Exchange points (IXPs) for their onward communication to respective customer bases.
2.13	Plan and conduct national and sectoral cyber simulation exercises at operational, management and political levels.
2.14	Issue annual information on national cyber threats and vulnerabilities.
2.15	Actively consider the adoption of an internationally or EU recognised framework for multi-disciplinary stakeholders[36] to collaborate in performing controlled cyber-attack tests.


CYBER SECURITY
Digital Security is our Priority

chapter 05

Cyber Competence and Culture

5.1
The Key Objective

Increase national cyber competence, capability, knowledge and ongoing awareness of cyber security.

5.2
The Sub-Objectives

A. Establish a National Coordination Centre.

In September 2018, the EC presented a proposal for a Regulation establishing a European Cyber Security Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres (EU CCCN). The proposal aimed to strengthen technology and industrial cyber security capabilities of the EU and help create a safe online environment. Political agreement on this initiative was reached by EU institutions in December 2020[37].

Specifically, the EU CCCN Regulation provides for the setting up of a National Coordination Centre in each Member State.

Malta has made its nomination for a National Coordination Centre. Along with its EU network and EU Cyber Competence Centre, the National Coordination Centre would contribute in areas of cyber security capabilities, research, industry competitiveness and EU grants to support national ecosystems.

ACTIONS

3.1	Establish a National Coordination Centre, in line with the *EU Regulation of the European Parliament and of the European Council, European Cybersecurity Industrial, Technology and Research Competence Centres and a Network of National Coordination Centres*.

B. Promote cyber security awareness at a national level.

Awareness of cyber security risks and issues, and how to deal with them, are essential in building a more resilient society and economy. The knowledge gained through ongoing awareness amongst all members of society, especially business – from management to employees – is the cornerstone of cyber security culture. Indeed, *Skills and Awareness raising* is identified in '*A strong European security ecosystem*' as one of the four strategic priority areas of the EU Cyber Security Strategy. This focus is crucial as, unfortunately, a considerable percentage of European firms do not understand the extent of their exposure to cyber risks[38]. In Malta, recent survey findings indicate a degree of cyber security awareness among businesses that is comparable to the EU population average [39] and an increasing percentage of Maltese respondents say they are fairly well or well informed about cybercrime[40].

A national cyber security awareness and education campaign was launched in 2018, aimed at various audiences such as academia, the Public Administration, the private sector, professionals, policy makers and the general public, and is still ongoing. The delivery method depends upon the particular audience targeted. Prevalent cyber risks at the time are highlighted so as to ensure effectiveness. The campaign involves collaboration on the domestic front and at EU level for consistency as well as to facilitate the sharing of guidance and support. Focussed campaigns, such as those specifically on cybercrime and public relations exercises including the issue of cyber security advisories targeting stakeholders within particular sectors, are also carried out.

Such campaigns are needed on an ongoing basis to cover developments within the cyber security threat landscape as well as increased trends in digitalisation, remote working[41] and online business interactions. Initiatives by various stakeholders is also actively encouraged such as through fora within and/or across economic sectors. Such initiatives could involve sharing of cyber security best practice, helping organisations to deal with:

- **Cyber risk management measures, including the applicability of the basic tenets of cyber hygiene.**
- **Cyber security related legislative or regulatory requirements in specific sectors and how to enact them.**
- **New digital work patterns requiring respect for employee privacy.**

Most importantly, awareness needs to reinforce the notion of cyber security as a behavioural concern in all work disciplines, recognising human weaknesses, rather than as an afterthought or as a technical issue to be delegated to IT practitioners.

It is only through such a comprehensive and intensive awareness campaign that a 'security first' culture amongst everyone in Maltese society can be guaranteed[42]. This would, in turn, lead to a stronger recognition and inculcation of security in skills and product and service development and delivery.

ACTIONS	
3.2	Further pursue an intensive cyber security education and awareness campaign on a national scale.
3.3	Establish a national forum for sharing of best practice and experiences related to cyber security.

C. Upgrade the skills of the current workforce and revisit the academic framework to bring it into line with cyber security industry requirements.

The cyber security industry is in a continuous state of flux. The global demand for cyber security skills continues to exceed supply as threats become more sophisticated[43].

From an ICT specialist perspective, Eurostat[44] indicates a growth in the number of ICT specialists in the EU that is more than 6 times as high as the increase of total employment in the EU between 2011 and 2019. Of these, about two thirds completed a tertiary education. The profession is male dominated with only 17.9% of ICT specialists in the EU being women[45].

The EC's *Country Report Malta 2020* records that Malta had the highest share of ICT graduates within the EU in 2019, with the percentage of ICT specialists representing a high proportion of the workforce[46] relative to the EU[47]. It said that although "the share of female ICT specialists is slightly above the EU average, it is important to further increase the participation of women in this field, given the focus of the country on the ICT sector". Additionally, the EC 's *Country Report Malta 2019* states that "although some measures back technical and highly qualified training and provision in environmental, engineering or ICT studies (e.g. Malta's College of Arts Science and Technology training programmes), they are modest in scope and budget. The majority of schemes (e.g. PhD support) are generic and they would benefit from targeting specific disciplines or sectors. In addition, systematic coordination between the different governmental bodies on this issue would benefit from further strengthening."

The areas requiring improvement underline cyber security as a specialist area within ICT. There is a need for more focus within the educational curriculum[48], from primary schoolyears up to post-tertiary level, and collaboration between educational and training institutions. Additionally, cyber security needs to be covered in more depth in academic and work disciplines.

Cyber security education and training should not only cover cybercrime from a law enforcement perspective but also from a judicial point of view. From a teaching perspective, cyber security needs to be seen not just as something for review of existing curricula but as a training issue for all educators. Cyber security training and education needs to cover handling of cyber crisis response situations, with simulation exercises and public relations activity.

Such development of cyber security expertise is especially important within the Public Administration given the sector's extensive use of sensitive data. In this regard, a drive towards more transparent and secure handling of data within the Public Administration should contribute positively.

It is important that, in addition to training and development, cyber security is actively considered across all of an organisation's human resource functions including performance management, recruitment and job development. Indeed, for cyber security to be imbued within an organisational culture, it needs to be fully embraced within all management disciplines, starting with human resources, and actively supported by senior management. Furthermore, soft skills are not to be overlooked in the security and technology field, as they are the tenets that shape a more security responsive culture.

Several actions shall aim to address the need to ensure skills capacity in the short, medium and long term, covering various segments of society and economic sectors.

ACTIONS	
3.4	Plan and execute cyber security training and development in Government, targeting both ICT specialists as well as non-ICT professionals who need a level of knowledge of cyber security to carry out their duties.
3.5	Support staff certification and accreditation of professional development curricula in cyber security, seek to address human resources gaps and the establishment of specialist teams related to cyber security.
3.6	Encourage the participation of women in cyber initiatives[49].
3.7	Provide training support initiatives to assist management and employees within the private sector.
3.8	Consider education plans at primary and secondary levels which may include further curriculum enhancement as well as continuous teacher training on cyber security and digital skills.
3.9	Consider new opportunities in higher level education such as development of new related modules, research, promotion of advanced technical training and partnership agreements with national and overseas bodies and institutions.

D. Promote a heightened security posture within private industry.

Private industry is increasingly capitalising on trade opportunities that digitalisation offers, which should potentially lead to new job opportunities, enhanced competitiveness and sustainable growth. But trade activity, that depends upon free cross-border data flows requires security safeguards and the attraction of investment requires robust infrastructure and well developed cyber security.

A recent surge in online operational and trading activities, to counter a global health emergency, accentuated this need for ways to safeguard the livelihood, competitiveness, development and innovation potential of industry.

The cyber security landscape in Malta features regulation, policy and supervisory functions, particularly within regulated sectors. But legislation and regulation may not cover all aspects of cyber security necessarily, particularly considering resource constraints in small organisations. Hence, support initiatives and incentives are necessary to encourage organisations to make a voluntary commitment to improving their cyber security.

At the National Cyber Security Summit, in October 2019, the Government launched the B SECURE Scheme, to help businesses assess their vulnerability against cyber security threats and train employees at various levels of the organisation. Further initiatives and incentives – including by the private sector itself - are to be actively promoted to meet the guidance and support needs of SMEs in particular.

ACTIONS

3.10	Actively consider and embark upon various initiatives and incentives to promote good cyber security posture within the private sector in Malta.

E. Support Research, Development and Innovation initiatives in cyber security.

Investment, skills development and innovation are required to sustain economic growth[50]. This includes further Research and Development (R&D) expenditure[51] , to support innovation potential. *'A Strong European security ecosystem'* - one of the four priority areas of the EU Cyber Security Strategy 2020-2025 - includes a specific objective of 'strengthening research and innovation' to contribute to further capacity building in cyber security.

Related efforts, initiatives and funding programmes, facilitated through the National Coordination Centre, as well as from various national and EU entities at academic and industrial levels, should help Malta improve its Research, Development and Innovation (RDI) capabilities in cyber security. Establishing a research cluster relevant to the Maltese landscape should be explored. Indeed, Malta views cyber security as a niche area in digital technology. It is identified as a smart specialisation area, carrying high RDI potential[52]. Of particular value would be for the results of RDI to be used to actively promote a wider understanding of the potentialities of cyber security on a national scale. Through the

potential use of pre-commercial procurement procedures, the Public Administration could become a first customer of Maltese cyber security RDI, kickstarting its growth.

One area of innovation where Malta stands to gain is in quantum computing and quantum communications. EU Member States, including Malta, have committed to working with the EC for the deployment of a secure quantum communication infrastructure for Europe (EuroQCI). Quantum communication infrastructure aims to offer secure transmission of confidential information to public authorities using an ultra-secure form of encryption to shield against cyberattack. The specifically assigned EuroQCI board - which is co-chaired by Malta - is finalising an action plan for a way forward in the creation of the EuroQCI and related industry, seeking EU funds in the process.

Ultimately, Malta would need to gauge its overall national cyber security capacity regularly so as to ensure that cyberspace, and its constituents, were increasingly resilient. The application of standard, widely recognised models may help in this regard.

ACTIONS	
3.11	Foster research, development and innovation, with respect to cybersecurity tools and secure network infrastructure, by institutions in Malta.
3.12	Facilitate investment in tools and equipment to tackle various aspects of cyber security through national and/or EU funding programmes.
3.13	Foster Government plans to bolster cybersecurity research, development and innovation.
3.14	Undertake a review of Malta's maturity in cyber security capacity.

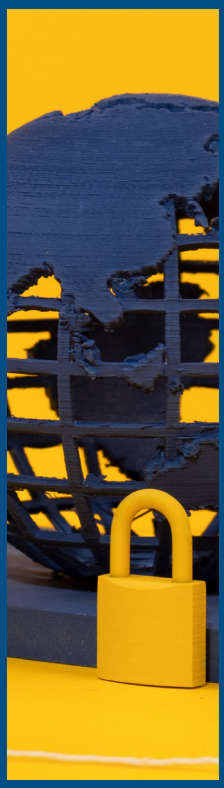

CYBER
SECURITY
MALTA
Digital Security. Your Priority.

chapter 06

International Cooperation

6.1
The Key Objective

Promote and maintain a strong presence in the cyber security field internationally, in cooperation with all relevant stakeholders.



6.2
The Sub-objectives

A. Strategic engagement with key partners and international organisations.

There are mounting concerns about the dual-use nature of today's emerging technology, for public safety and national security, considering global geopolitical tensions. Since countries view such technologies as central to their security, they recognise that their malignant use or misuse could lead to adverse consequences on a large scale. Greater economic integration and connectivity has meant that the effects and consequences of technological advances are far less localised than before. Indeed, they can spread to countries and industries worldwide. Hence, it is crucial for a nation state to foster international cooperation in order to reduce its vulnerability and enhance resilience.

Cyber space discussions have taken place in various international organisations, including the United Nations (UN), the Council of Europe (CoE), the Organisation for Security and Co-operation in

Europe (OSCE), the Organisation for Economic Co-operation and Development (OECD), the Commonwealth, the North Atlantic Treaty Organisation (NATO), the African Union (AU), the Organisation of American States (OAS), the Association of Southeast Asian Nations (ASEAN), ASEAN Regional Forum (ARF) and the EU. Malta, as a member of both the EU and UN, is engaging with these organisations to further cooperation in cyber security, especially in the areas of training, education, cyber defence and technology innovation. In February 2021, Malta appointed its first-ever Ambassador for Digital Affairs, a move which has strengthened its relationship with international partners and multinational organisations.

Malta participates in the EU cyber dialogue, consultations and outreach programmes with third countries to build trust and exchange best practice. Close working relationships on aspects of cyber security have also been established with a number of EU counterparts.

Malta appreciates the need for close international collaboration so as to foster the exchange of cyber security defence intelligence and best practice, ensuring a strong knowledge base and enhanced cyber security competencies.

ACTIONS	
4.1	Continue to foster cooperation and support, including through bilateral and multilateral agreements, in the field of cyber security.
4.2	Consolidate the role of the Ambassador for Digital Affairs in strengthening Malta's relations with international like-minded partners.

B. Participation and cooperation in European and international fora.

Participation in European and international fora contribute to the successful actualisation of foreign policy in the sphere of cyber security whilst building the nation's image as a competent player.

Malta is pursuing increased co-operation within the EU and other groupings, institutions and bodies in which it is a member, such as the CoE, the OSCE, the Commonwealth, and the UN. Such matters pertain to awareness,

building measures, crisis management, and hybrid threats[53]. Effective participation calls for a multi-disciplinary and multi-stakeholder approach, requiring shared expertise, co-operation and coordination.

ACTIONS	
4.3	Intensify participation in EU, regional and international cyber related fora.
4.4	Co-operate with other countries to instill greater awareness of the threat of cyber malicious activities that may contribute to a wider hybrid threat campaign.

C. Application of existing international law and measures promoting responsible state behaviour in cyberspace within the context of international security.

As part of its international commitment, Malta has participated in the UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UN GGE) and the UN-mandated Open-Ended Working Group on Developments in the Field of ICTs in the context of International Security (UN OEWG).

The UN GGE's efforts led to the introduction of the *UN Framework of Responsible State Behaviour in Cyberspace* consisting of the applicability of international law - in particular the Charter of the UN - to cyberspace, as well as voluntary norms, rules, principles, Confidence Building Measures (CBMs)[54] and capacity building. The UN OEWG, for its part, promoted the establishment of an open, multi-stakeholder approach as well as the further development and application of the rules, norms, principles, CBMs and capacity building for responsible behaviour in cyberspace. The development of CBMs for cyberspace proves to be more difficult, given that by its very nature, cyberspace does not erase spatial boundaries and the transnational dimension allows for anonymity[55]. Hence, CBMs for cyberspace, along with political commitment to them, are significant for the progressive development of international law[56] within such realm.

Whilst Malta has committed itself to such instruments, it still needs to develop a national position on the applicability of international law and states' behaviour on the world stage. Such development, along with supporting tools and resources, should enable Malta to play a stronger role in international cyberspace policy.

ACTIONS	
4.5	Pursue and improve upon active participation in international meetings on responsible state behaviour in cyberspace within the context of international security and implement outcomes accordingly.

D. EU Cyber Diplomacy Toolbox.

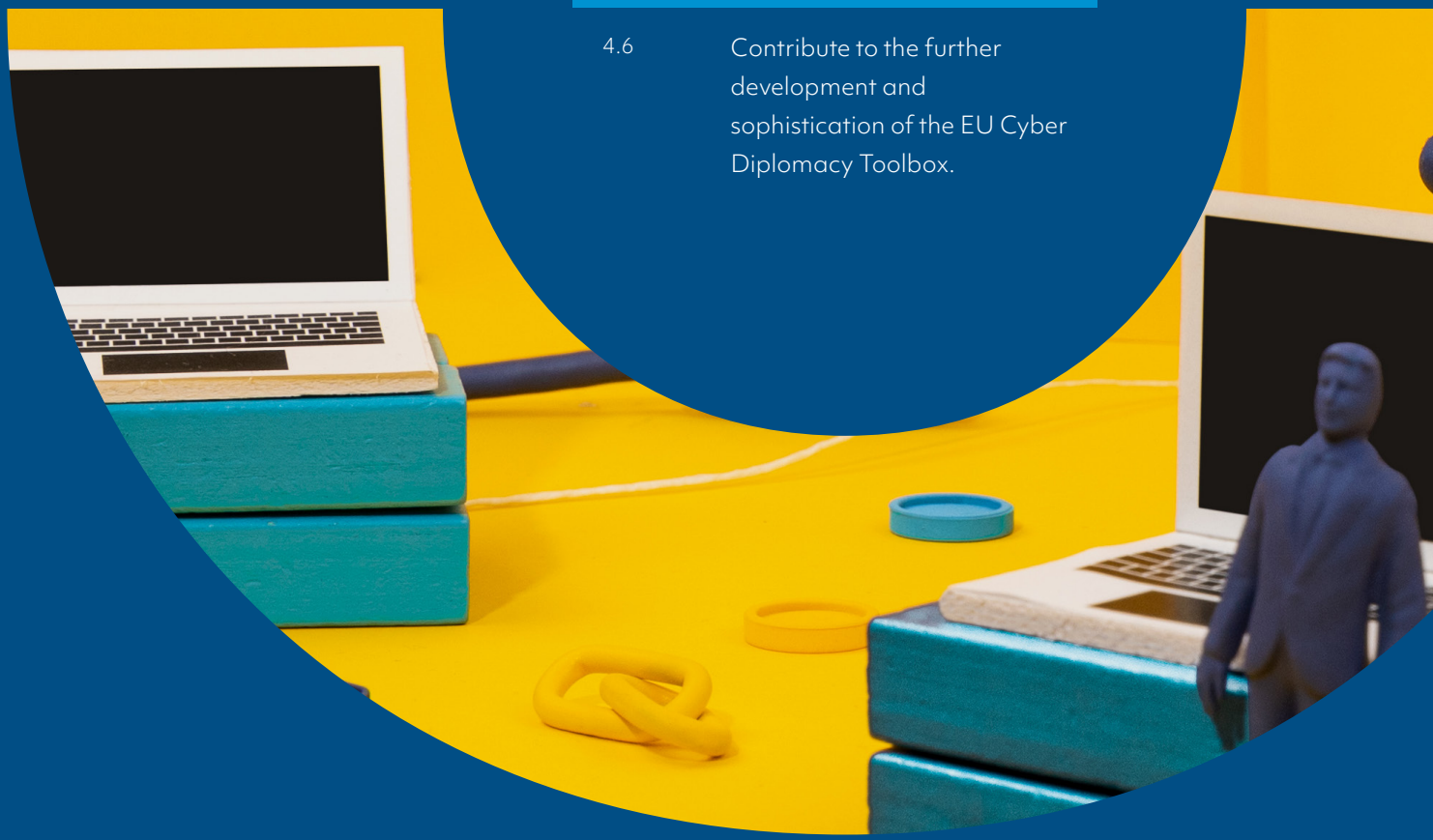
Cyber-attacks can paralyse a Government's decision-making systems, cripple a country's essential infrastructure and cause panic, potentially leading to unrest and inadvertent wars. Hence diplomacy plays a crucial role. In recent years, efforts at an EU level has intensified in this regard.

The Cyber Diplomacy Toolbox introduced by the EC's draft *Conclusions on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities* seeks to provide the EU and its Member States, in a transparent and resolute manner, a set of instruments of diplomatic, political and economic nature, for adequate and determined responses to malicious cyber activities. Through it, the EU has steadily committed itself to promote the benefits of adhering to norms of responsible state behaviour in cyberspace. It has equipped itself with restrictive measures, as a response to malicious cyber activities, and is determined to change the behaviour of state and non-state actors acting against the responsible norms of cyberspace. The fact that EU restrictive measures against cyber-attack is a horizontal sanctions regime, as opposed to a geographical sanctions regime, means that persons and entities that satisfy the designation criteria may be listed from whichever country they hail from, thus rendering the tool effective and wide reaching.

Malta, as an EU member state, has the Cyber Diplomacy Toolbox at its disposal, alongside other instruments of cyber diplomacy, to use as a deterrent against overseas actors contemplating malicious activities in cyberspace.

Malta, along with other EU Member states, is being invited to place emphasis on the further development and sophistication of the decision-making and invocation processes of the Cyber Diplomacy Toolbox by drawing lessons from its initial applications.

ACTIONS	
4.6	Contribute to the further development and sophistication of the EU Cyber Diplomacy Toolbox.



chapter 07

Way Forward

The Strategy has outlined high-level priority actions for attaining the sub-objectives identified for each domain for the next three years. The actions translate into specific activities assigned to respective owners for implementation within stipulated timelines as part of an Action Plan.

Strong cyber security capability and capacity is a strategic priority for Government and, in collaboration with stakeholders, it shall continue striving to ensure that the country is well equipped and prepared to manage digital risk.

Both the Public Administration and the private sector have finite resources, technology is constantly evolving and measures to address cyber security threats may not remain highly effective as technological advances bring with them a plethora of new cyber threat vectors. Additionally, further regulatory cyber security related developments at EU level, impacting upon Member States, including Malta, are envisaged. Hence, the course of action for implementation of this Strategy cannot be cast in stone.

Therefore, the National Cyber Security Steering Committee shall coordinate the Strategy's implementation by various stakeholders whilst taking measures to continually enhance Malta's security posture. It shall monitor the progress registered with respect to the action plan whilst keeping an eye on developments within the cyber security sphere at a domestic, EU and international level so as to update the Plan accordingly. Widely recognised or nationally set performance indicators may be applied to gauge Malta's relative maturity in this sphere.

Whilst the National Cyber Security Strategy shall act as the national reference point for cyber security matters, it shall not exclude, but rather encourage, the establishment of aligned strategic frameworks and/or initiatives in cyber security focusing on the various sectors/ disciplines in Maltese society and economy.

Ultimately, cyber security is a global concern and it is in everyone's interests to ensure a multi-disciplined, yet common and unified, approach to its ever-evolving challenges.

Glossary

The following definitions apply for the purposes of this Strategy.

Confidence Building Measures	Measures to address, prevent or resolve uncertainties among states. They are designed to prevent wanted, and especially unwanted, escalations of hostilities and build mutual trust. They can be formal or informal, unilateral, bilateral, or multilateral, military or political, and can be state-to-state or non-governmental[57].
Cyber Attack	**Cyber incident** triggered by malicious intent where damage, disruption or dysfunctionalities are caused[58].
Cybercrime	Encompasses criminal acts committed in **cyber space**[59], which are: • Cyber-dependent or new forms of crimes made possible with the advent of the Internet and Internet-enabled digital devices[60]. • Cyber-enabled or hybrid crimes where traditional, real-world crimes, such as online fraud, are perpetrated in cyberspace[61].
Cyber Hygiene	Covers several practices that should be implemented and carried out regularly to protect persons and organisations online[62].
Cyber Incident	Any occurrence that has impact on any of the components of **cyber space** or on the functioning of cyber space, independent of whether it's natural or human made; malicious or of non-malicious intent; deliberate, accidental or due to incompetence; development or operational interactions.[63].
Cyber Defence	Ability to prevent, mitigate or respond to **cyber attacks**[64].
Cyber Security	All activities necessary to protect **cyber space** and its users from **cyber threats**[65].
Cyber Space	A time-dependent interacting set of physical and logical (non-physical) assets which store and/or transfer digital data[66].
Cyber Threat	Circumstance or event with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data, and/or denial of service[67].

Hybrid Threat	Action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the national, regional, state or institutional level. Such actions are coordinated and synchronised and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution[68]. Such means may include malicious cyber activities such as cyber espionage, disinformation and hacking[69].
Indicator of Compromise	Activity or piece of forensic data observed on a network or device that indicates a high probability of a system being compromised. Such an indicator is used to detect malicious activity in its early stages as well as to prevent known threats[70].
Information Security	Subset of **cyber security** that covers the principles of confidentiality, integrity and availability of stored or transmitted data[71].
Network and Information Systems Security legislation	National legislation that is transposed from the EU Directive on security of network and information systems (NIS). In December 2020, the EC presented a new EU legislative proposal that builds upon and repeals the DIRECTIVE (EU) 2016/1148 or NIS Directive.
Public Administration	The Government of Malta, including its ministries and departments, specialised units and agencies, Government entities, commissions and boards, referred to in the Public Administration Act. **https://legislation.mt/eli/act/2019/3/eng/pdf**
Vulnerability	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved[72].

References

Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. (2020), *The drivers of cyber risk,* Monetary and Economic Department, Bank for International Settlements (BIS) Working Papers, No. 865, 20 May 2020. **https://www.bis.org/publ/work865.htm**

Council of the European Union (2017), *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities* – Adoption, 9916/17, 7 June 2017. **https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/**

Council of the European Union (2020), *Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic* – 14064/20, 15 December 2020. **https://data.consilium.europa.eu/doc/document/ST-14064-2020-INIT/en/pdf**

Cyber Security Malta, *Malta Cyber Security Strategy 2016*. **https://cybersecurity.gov.mt/strategy/**

European Commission (2018), Proposal for a Regulation of the European Parliament and of the Council on establishing *the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, Brussels,* 12.9.2018, COM (2018) 630 final, 2018/0328(COD). **https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research**

European Commission (2020), Proposal for a Directive of the European Parliament and of the Council on *measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148,* Brussels, 16.12.2020 COM(2020) 823 final 2020/0359 (COD). **https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union**

European Commission (2020), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a *Digital Finance Strategy for the EU, Brussels*, 24.9.2020, COM(2020), 591 final. **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591**

European Commission (2020), Proposal for a Regulation of the European Parliament and of the Council on *digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014,* Brussels, 24.9.2020, COM(2020) 595 final, 2020/0266(COD). **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595**

European Commission (2020), *The EU's Cyber security Strategy for the Digital Decade*, Joint Communication to the European Parliament and the Council, Brussels, 16.12.2020 JOIN(2020) 18 final. **https://ec.europa.eu/digital-single-market/en/news/eus-cyber security-strategy-digital-decade**

European Commission (2020), Special Eurobarometer 499: *Europeans' attitudes towards cyber security.* **https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG**

European Commission (2021), *The future is quantum: EU countries plan ultra-secure communication network,* Shaping Europe's Digital Future. **https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network**

European Commission Staff Working Document (2019), *Country Report Malta 2019 Accompanying the*

document: Communication from the Commission to the European Parliament, The European Council, The European Central Bank and the Eurogroup 2019 European Semester: Assessment of progress on structural reforms, prevention and correction of macroeconomic imbalances, and results of in-depth reviews under Regulation (EU) No 1176/2011 {COM(2019) 150 final. **2019-european-semester-country-report-malta_en.pdf (europa.eu)**

European Union Act (CAP 460) L.N. 216 of 2018, *Measures For High Common Level of Security of Network and Information Systems Order, 2018.* **https://maltacip.gov.mt/en/Legislation/Documents/document%20(1).pdf**

European Union (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning *measures for a high common level of security of network and information systems across the Union.* **https://eur-lex.europa.eu/legal content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC**

European Union (2019), Regulation (EU) 2019/452 of the European Parliament and of the Council of 20 February 2019 on *establishing a framework for the screening of foreign direct investments into the Union.* **https://www.consilium.europa.eu/media/38347/pe00072-en18.pdf**

European Union(2019), Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA *(the European Union Agency for Cyber security) and on information and communications technology cyber security certification and repealing Regulation (EU) No 526/2013 (Cyber security Act).* **https://eur-lex.europa.eu/eli/reg/2019/881/oj**

European Union Agency for Cyber Security – ENISA(2017) *Overview of cyber security and related terminology,* Ver 1.0, Sept. 2017; **https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cyber security-and-related-terminology**

European Union Agency for Cyber Security – ENISA(2019) - *Good Practices in innovation on cyber security under the NCSS,* November 2019. **https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cyber security-under-the-ncss-1**

European Union NIS Cooperation Group(2020) *Cyber security of 5G networks EU Toolbox of risk mitigating measures, , CG Publication 1/20.* **https://ec.europa.eu/digital-single-market/en/news/cyber security-5g-networks-eu-toolbox-risk-mitigating-measures**

International Telecommunications Union- ITU(2018), *Cyber Ecosystem*, Presentation by Profs Oleksander Potii as part of ITU Seminar 15.05.2018. **https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2018/05_Kiev/ITU%20Seminar%2015.05.18%20-%20Oleksandr%20Potii.pdf**

Malta.AI (2019), Malta-The *Ultimate AI Launchpad, A Strategy and Vision for Artificial Intelligence in Malta 2030*, October 2019.

Malta.AI (2019), *Malta Towards Trustworthy AI – Malta's Ethical AI Framework,* October 2019. **https://malta.ai/wp-content/uploads/2019/10/Malta_Towards_Ethical_and_Trustworthy_AI_vFINAL.pdf**

Macintosh JP, Reid,J and Tyler L (2011) : Cyber Doctrine: *towards A Coherence Evolutionary Framework for Learning Resilience;* institute for Security and Resilience Studies. **https://www.academia.edu/1097571/Cyber_Doctrine_towards_a_coherent_evolutionary_framework_for_learning_resilience**

Malta Communications Authority (MCA), various articles from **https://www.mca.org.mt**

Malta Council for Science and Technology – MCST (2020) Public Consultation Document: *Towards a Smart Specialisation Strategy 2021-2027 for Malta*. **https://mcst.gov.mt/wp-content/uploads/2020/03/Towards-a-RIS3-2021-2027-for-Malta_March-2020_Public-Consultation-Document.pdf**

Malta Information Technology Agency (MITA), various articles from **https://www.mita.gov.mt**

Malta IT Law Association -MITLA (2019), *Raising Awareness on Cyber Security (RACS) 2019*, October 2019. **https://www.mitla.org.mt/wp-content/uploads/2019/10/MITLA-RACS-SUMMARY-REPORT.pdf**

Nachin,N., Tangmanee, C, Piromsopa, K (2019), *How to increase Cyber security Awareness, ISACA, 2,45-50.*

National Statistics Office (NSO), various articles, **https://www.nso.gov.mt**

Niculcea,T. , Ranaweera, P. and Le-Khac, N. (2020), *Security Considerations for Internet of Things: A Survey, Springer* Link. **https://link.springer.com/article/10.1007/s42979-020-00201-3**

Organisation for Security and Co-operation in Europe-OSCE(2013), Permanent Council Decision No. 1106 *Initial Set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*, 3 December 2013. **https://www.osce.org/pc/109168**

Organisation for Security and Co-operation in Europe -OSCE(2016), Permanent Council Decision No. 1202, *OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies,* 10 March 2016. **https://www.osce.org/files/f/documents/d/a/227281.pdf**

Pearce, G. (2019), *Acknowledging Humanity in the Governance of Emerging Technology and Digital Transformation,* ISACA Journal, 4, 19-24.

Saurbaugh, M. (2019), *Future Proofing a Career in Cyber security* – The Skills Gap, ISACA Journal, 5,16-19.

The Commonwealth (2018), *Commonwealth Cyber Declaration, London, UK, 2018.* **https://thecommonwealth.org/commonwealth-cyber-declaration**

United Nations GGE (2015), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July 2015. **https://eucyberdirect.eu/wp-content/uploads/2019/10/ungge-2015.pdf**

World Economic Forum (2020) , *Cyber Security Leadership Principles: Lessons learnt during the COVID-19 pandemic to prepare for the new normal,* published 26 May 2020. **https://www.weforum.org/reports/cyber security-leadership-principles-lessons-learnt-during-the-covid-19-pandemic-to-prepare-for-the-new-normal**

Endnotes

1. Refer to Glossary
2. Ibid.
3. Also referred to as the Network and Information Security (NIS) Directive
4. https://maltacip.gov.mt/en/Legislation/Documents/document%20(1).pdf
5. As part of the Raising awareness for Cyber-Security project spearheaded by the Malta Information Technology Law Association (MITLA) and funded through the Voluntary Organisations Project Scheme managed by the Malta Council for the Voluntary Sector on behalf of the Ministry for Education and Employment, a survey amongst SMEs and NGOs on their level of cyber security preparedness was conducted in 2019. The survey indicated that 55% of businesses undertook cyber security changes in preparation of the GDPR **https://www.mitla.org.mt/wp-content/uploads/2019/10/MITLA-RACS-SUMMARY-REPORT.pdf**
6. A share of 20 % of SMEs sell online compared with 17 % in the EU. **https://ec.europa.eu/info/sites/info/files/file_import/2019-european-semester-country-report-malta_en.pdf**
7. Maltese individuals between the ages of 16 and 34 years are considerably more active in eCommerce than their European counterparts. On average, Malta has consistently recorded a 4% growth, year-on-year for the past 8 years. **https://www.mca.org.mt/articles/79-maltese-households-today-have-broadband-connection**
8. Socialising and sending/receiving emails continue to be the most popular internet activities conducted on a mobile, followed by accessing content via APPs and retrieving information/news. Social media and messaging are still the most accessed applications among mobile data users, followed by content and games. **https://www.mca.org.mt/articles/mobile-data-registers-growth-all-fronts**
9. Source: **https://nso.gov.mt/en/News_Releases/Documents/2021/01/News2021_012.pdf**
10. A Eurostat report, published in 2019 shows that national broadband penetration currently stands at 79% of all households, ranking 3% higher than the EU average. **https://www.mca.org.mt/articles/79-maltese-households-today-have-broadband-connection**
11. The mobile telephony subscriber base grew by 8,409 subscriptions year-on-year to reach a total of 614,781 by the end of March 2019. **https://www.mca.org.mt/articles/data-report-sheet-drs-latest-figures-published-3**
12. Source: **https://ec.europa.eu/info/sites/info/files/file_import/2019-european-semester-country-report-malta_en.pdf**
13. Refer to Glossary.

14. Such as through the *Mobile Strategy, Mapping Tomorrow – A Strategic plan for the Digital Administration of the Public Administration 2019-2021* and the Public Administration undertaking of a number of AI use cases as part of Malta- *The Ultimate AI Launchpad – A Strategy and Vision for Artificial Intelligence in Malta for 2030.*

15. A comprehensive legislative package, regulating the use of distributed ledger technology platforms, including blockchain, came into force in November 2018. The new regulatory framework comprises three acts, covering: (i) virtual financial assets, including crypto-currencies (ii) innovative technology arrangements and services (iii) the establishment of the Malta Digital Innovation Authority. Such legislation aims to promote Malta as a digital innovation hub, as well as providing legal certainty in an area which is still mostly unregulated elsewhere within the EU. **https://ec.europa.eu/info/sites/info/files/file_import/2019-european-semester-country-report-malta_en.pdf**

16. Source: **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591**

17. The toolbox came in the wake of Recommendation (EU) 2019/534 on the cyber security of 5G networks, adopted by the Commission in 2019 which called for a European unified approach to the security of 5G networks.

18. Source: **https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/200924-digital-finance-factsheet_en.pdf**

19. Sources: **https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/200924-digital-finance-factsheet_en.pdf** and **https://www.bis.org/publ/work865.htm**

20. Source : **https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en**

21. 'Economic growth is fuelled by the services sector. The Maltese economy has developed a vibrant, internationally oriented services sector … the gaming industry contributes to the economic performance of other major sectors, including professional services, ICT (information and communication technology), financial activities and real estate'. **https://ec.europa.eu/info/sites/info/files/file_import/2019-european-semester-country-report-malta_en.pdf**

22. Coupled to the AI Certification, Malta is also developing an Ethical AI Framework aimed, amongst other objectives, at maximising the benefits of AI systems whilst preventing and minimising their risk, including *cyber security hazards* – Sources:
    https://malta.ai/wp-content/uploads/2019/10/Malta_Towards_Ethical_and_Trustworthy_AI_vFINAL.pdf and **https://stip.oecd.org/stip/policy-initiatives/2019%2Fdata%2FpolicyInitiatives%2F24993**

23. **https://ictpolicies.gov.mt**

24. The legal framework within the Financial Services industry mandates Regulatory Technical Standards issued by the European Banking Authority, the European Insurances and Pensions Authority and the European Security and Markets Authority.

25. In its Communication, dated 13 March 2020, the European Commission stated that "*Member States must be vigilant and use all available instruments at EU and national level to prevent the current crisis from leading to a loss of critical resources and technologies*".

26. Artificial intelligence, robotics, semiconductors, aerospace, defence, energy storage, quantum and nuclear technologies as well as nanotechnologies and biotechnologies.

27. Which is a full member of the European Cooperation for Accreditation.

28. **https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369**

29. Refer to Glossary

30. Source: **https://www.consilium.europa.eu/en/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation-in-the-context-of-the-covid-19-pandemic/**

31. LN 216 of 2018 specifically obliges Operators of Essential Services and DSPs to have their own CSIRT and promotes their voluntary sharing of information.

32. Source: **https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport**

33. Higher incidence of videoconference attacks – 39% of companies, phishing, 69% of remote workers using workplace collaboration tools with only 63% of IT managers using them – 6% using their own shadow IT which poses a security risk. **https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Readiness_Report_EN-US_200908.pdf**

34. Source: **https://ec.europa.eu/home-affairs/what-we-do/policies/internal-security_en**

35. Special Eurobarometer 499: Europeans' attitudes towards cyber security, **https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG**

36. Such as authorities, organisations, threat intelligence and red-team providers.

37. Source: **https://ec.europa.eu/digital-single-market/en/european-cyber security-industrial-technology-and-research-competence-centre**

38. Source: **https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study**

39. Awareness levels among businesses varied by sector, with the overall percentage standing at 66%. Such score is comparable to the EU population average of 50%. **https://www.mitla.org.mt/wp-content/uploads/2019/10/WP2-Assessing-cyber-security-readiness.pdf** (The Raising Awareness on Cyber Security RACS) project seeks to determine where SMEs and Voluntary Organisations (VOs) in Malta stand on cyber security and cyber threats.

40. According to the Eurobarometer survey, cybercrime awareness is rising. 52% of respondents state they are fairly well or very well informed about cybercrime, compared to 46% in 2017.

41. Awareness needs to tackle ransomware, protections of working from home. **https://cyber security.gov.mt/the-key-cyberthreats-of-2020/**

42. Reegard, K., Blackett C. and Katta V (2019), The Concept of Cyber security Culture , Conference Paper, Proceedings of the 29th European Safety and Reliability Conference – September 2019. **https://www.researchgate.net/publication/336149766_The_Concept_of_Cyber security_Culture**

43. Source: **https://cyintelligence.com/resources/blog**

44. The statistical arm of the EC.

45. Source: **https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_in_employment**

46. 4.8% as opposed to 3.9% in the EU.

47. Source: **https://ec.europa.eu/info/sites/info/files/2020-european_semester_country-report-malta_en.pdf**

48. Gamification may facilitate such learning in the process.

49. Such as in Women4Cyber initiatives. Women4Cyber is a non-profit European private foundation with the objective to promote, encourage and support the participation of women in the field of cyber security; **https://women4cyber.eu/**

50. Source: **https://ec.europa.eu/info/sites/info/files/file_import/2019-european-semester-country-report-malta_en.pdf**

51. Research and development expenditure in Malta – 0.58% of GDP in 2017 and 0.57462 % in 2018 (lower than in 2015 where it stood at 0.74% of GDP). **https://nso.gov.mt/en/News_Releases/View_by_Unit/Unit_A2/Public_Finance/Pages/Research-and-Development-in-Malta.aspx** and **https://tradingeconomics.com/malta/research-and-development-expenditure-percent-of-gdp-wb-data.html**

52. Public Consultation Document: Towards a Smart Specialisation Strategy 2021-2027 for Malta. **https://mcst.gov.mt/wp-content/uploads/2020/03/Towards-a-RIS3-2021-2027-for-Malta_March-2020_Public-Consultation-Document.pdf**

53. Hybrid Threats and EU. **https://www.consilium.europa.eu/en/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation-in-the-context-of-the-covid-19-pandemic/**

54. Refer to Glossary

55. Source: **https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2018/05_Kiev/ITU%20Seminar%2015.05.18%20-%20Oleksandr%20Potii.pdf**

56. Especially in its general principles which establish (in an abstract and general manner) several obligations of States.

57. Source: **https://www.csis.org/programs/international-security-program/isp-archives/asia-division/cross-strait-security-initiativ-1**

58. Adapted from ENISA Overview of cyber security and related terminology, Ver 1.0 Sept. 2017. **https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cyber security-and-related-terminology**

59. Adapted from **https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en** and **https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html**

60. Such as hacking malware infection for reasons such as financial gain, protest and espionage.

61. Such as on-line fraud and data theft through phishing.

62. Adapted from ENISA Overview of cyber security and related terminology, Ver 1.0 Sept. 2017. **https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cyber security-and-related-terminology**

63. Ibid.

64. Ibid.

65. Ibid.

66. Ibid.

67. ENISA Glossary (Published under risk Management); **https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary.**

68. Source: **https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/**

69. Ministry for Foreign and European Affairs – Malta.

70. Adapted from **https://encyclopedia.kaspersky.com/glossary/indicator-of-compromise-ioc/ and https://searchsecurity.techtarget.com/definition/Indicators-of-Compromise-IOC.**

71. Adapted from ENISA Overview of cyber security and related terminology, Ver 1.0 Sept. 2017. **https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cyber security-and-related-terminology.**

72. Ibid.

Acknowledgements

The following organisations, forming part of the National Cyber Security Committee, contributed to the articulation of the National Cyber Security Strategy.

GOVERNMENT OF MALTA

MINISTRY FOR THE ECONOMY AND INDUSTRY

MINISTRY FOR HOME AFFAIRS, NATIONAL SECURITY AND LAW ENFORCEMENT

SUPPORTED BY

mita

CONTRIBUTORS

MaltaCIP CRITICAL INFRASTRUCTURE PROTECTION

MCA MALTA COMMUNICATIONS AUTHORITY

MFSA MALTA FINANCIAL SERVICES AUTHORITY

mga MALTA GAMING AUTHORITY

MDIA Malta Digital Innovation Authority

GOVERNMENT OF MALTA MINISTRY FOR FOREIGN AND EUROPEAN AFFAIRS

The contribution of other various entities and individuals within the Public Administration, the Private Sector, the Academia and members of the public, through public consultation feedback, is also acknowledged.

NATIONAL CYBER SECURITY STRATEGY 2023 - 2026