COMMONWEALTH APPROACH FOR DEVELOPING NATIONAL CYBERSECURITY STRATEGIES

A guide to creating a cohesive and inclusive approach to delivering a safe, secure and resilient cyberspace

Revised 2015

ABOUT COMMONWEALTH TELECOMMUNICATIONS ORGANISATION (CTO)

The Commonwealth Telecommunications Organisation is the Commonwealth agency mandated in the field of Information and Communications Technology and works towards helping its members leverage ICTs for socio-economic development. Its two-tier membership facilitates consultations between Commonwealth countries, non-Commonwealth countries, industry and civil society to arrive at harmonised approaches on ICT related issues with Global implications.

1 INTRODUCTION

Cyberspace, which encompasses the internet and all forms of Information and Communication Technologies (ICTs), presents enormous opportunities for socio-economic development across the world. It is therefore imperative to assure the safety, security and resilience of the infrastructure, of the information content that runs through it and of the users. However, the complexity of this vast and sometimes difficult to define network, along with the people involved, requires a cohesive approach involving a broad range of stakeholders that extend well beyond individual governments.

National Cybersecurity strategies provide the framework to support such an all-encompassing approach to protect the Cyberspace infrastructure, its content and users. It states national priorities and goals, assigns roles and responsibilities and resources.

Indeed, an effective Cybersecurity strategy is critical for each country to engage fully in the increasingly Cyber-dependant trade and commerce. It enables individuals, companies and nations to realise the full potentials of the Cyberspace, without fear or reservation. It engages all parties in addressing the challenges and opportunities.

Based on its mandate, the CTO developed this proposed approach in 2014 to serve as a guide for countries to develop their individual National Cybersecurity Strategies. The guide provides practical advice and proposes actions that can be adapted by countries to suit their individual circumstances. This revised version was issued in 2015.

2 THE COMMONWEALTH CYBERGOVERNANCE MODEL

The world is witnessing the emergence of contrasting views and approaches on how to govern the Cyberspace. Mindful of the unique nature of Cyberspace and of the importance of maintaining it as a place that fosters interactions, innovation and entrepreneurship, the CTO embarked on a project to develop the Commonwealth Cybergovernance Model that draws on the shared values and principles of the Commonwealth as encompassed in the Commonwealth Charter. (http://thecommonwealth.org/our-charter).

This initiative was launched at the 53rd Council meeting of the CTO in Abuja, Nigeria which was followed by a range of consultations with stakeholders. The Commonwealth Cybergovernance Model was adopted by the Commonwealth ICT Ministers at the meeting held in London in March 2014.

The Model is a unique Commonwealth approach based on four key principles, each steeped in the Commonwealth values, set out in table 1.

Table 1: Commonwealth Cybergovernance Principles

Principle 1: "We contribute to a safe and an effective global Cyberspace"

- as a partnership between public and private sectors, civil society and users, a collective creation;
- with multi-stakeholder, transparent and collaborative governance promoting continuous development of Cyberspace;
- where investment in the Cyberspace is encouraged and rewarded;
- by providing sufficient neutrality of the network as a provider of information services;
- by offering stability in the provision of reliable and resilient information services;
- by having standardisation to achieve global interoperability;
- by enabling all to participate with equal opportunity of universal access;
- as an open, distributed, interconnected internet;
- providing an environment that is safe for its users, particularly the young and vulnerable;
- made available to users at an affordable price.

Principle 2: "Our actions in Cyberspace support broader economic and social development"

- by enabling innovation and sustainable development, creating greater coherence and synergy, through collaboration and the widespread dissemination of knowledge;
- respecting cultural and linguistic diversity without the imposition of beliefs;
- promoting cross-border delivery of services and free flow of labour in a multi-lateral trading system;
- allowing free association and interaction between individuals across borders;
- supporting and enhancing digital literacy;
- providing everyone with information that promotes and protects their rights and is relevant to their interests, for example to support transparent and accountable government;
- enabling and promoting multi-stakeholder partnerships;
- facilitating pan-Commonwealth consultations and international linkages in a globally connected space that also serves local interests.

Principle 3: "We act individually and collectively to tackle cybercrime"

- nations, organisations and society work together to foster respect for the law;
- to develop relevant and proportionate laws to tackle Cybercrime effectively;
- to protect our critical national and shared infrastructures;
- meeting internationally-recognised standards and good practice to deliver security;
- with effective government structures working collaboratively within and between states;
- with governments, relevant international organisations and the private sector working closely to prevent and respond to incidents.

Principle 4: "We each exercise our rights and meet our responsibilities in Cyberspace"

- we defend in Cyberspace the values of human rights, freedom of expression and privacy as stated in our Charter of the Commonwealth;
- individuals, organisations and nations are empowered through their access to knowledge;
- users benefit from the fruits of their labours; intellectual property is protected accordingly;
- users can benefit from the commercial value of their own information; accordingly, responsibility and liability for information lies with those who create it;
- responsible behaviour demands users all meet minimum Cyberhygiene requirements.

3 CREATING AND USING A NATIONAL CYBERSECURITY STRATEGY

This chapter offers guidance to countries in the development, deployment and revision of their national Cybersecurity Strategies, emphasising the need for each country to take into account its culture, its national priorities, the risks it faces and the impact of its strategy both regionally and globally. The approach described in this guide embraces the Principles of Commonwealth Cybergovernance and draws on published Cybersecurity strategies and good practice from a range of countries. The next chapter outlines the key areas a National Cybersecurity Strategy should address.

3.1 Development of the Strategy

The success of any national strategy depends on the practical circumstances within the government and the country. It is important that the project to develop a national Cybersecurity strategy attracts the strong and visible support of the highest levels of Government. However, due to the nature of Cybersecurity, it is also imperative that the National Cybersecurity strategy is developed in a multi-stakeholder partnership that brings together the public sector, private sector, academia and the civil society while also drawing on the knowledge, expertise and competencies of the international community. This requires a delicate balance of strong leadership coupled with an inclusive approach.

The exercise of developing the strategy will also benefit those participating stakeholders by improving their awareness and mutual understanding of the disparate opportunities, risks, needs and capabilities of the different stakeholders. Reflecting the global and connected nature of Cyberspace, these stakeholders may be national and international bodies, both regional and global, both public and private sector plus civil society.

The strategy should reflect the cultural values of the country and be based on principles against which choices can be judged. The Commonwealth Cybergovernance Model has been accepted by Commonwealth Ministers as a foundation upon which to build the Commonwealth's strategic approach to Cyberspace.

3.1.1 An approach to design of the strategy: risk-based and outcome-focused

The following guidance might be considered during the strategy's design. These points are based on guidance published by Microsoft, considered by CTO to reflect best practice and listed alongside other sources in appendix 1:

- Risk-based. Assess risk by identifying threats, vulnerabilities, and consequences, then manage the risk through mitigations, controls, costs, and similar measures.
- Outcome-focused. Focus on the desired end state rather than prescribing the means to achieve it, and measure progress towards that end state.
- Prioritised. Adopt a graduated approach and focus on what is critical, recognising that the impact of disruption or failure is not uniform among assets or sectors.
- Practicable. Optimise for adoption by the largest possible group of critical assets and realistic implementation across the broadest range of critical sectors.

- Globally relevant. Integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible.

Developing Microsoft's second and third points: the strategy should identify or propose national level goals that describe outcomes associated with cyberspace, for example "Be a trusted location to do business online". This establishes a link between the Cybersecurity strategy and the wider public agenda. The current state of Cybersecurity will present risks (and sometimes opportunities) to those national level outcomes. For example, cybercrime, if unchecked, will harm trust in online commerce. Having made a case to consider measures to reduce such risks (or exploit any opportunities), the strategy can describe a set of corresponding objectives, which can be seen to support the national level goals. For example, those objectives could include "develop modern laws, liaise with other countries and train law enforcement officials".

Figure 1 illustrates the cycle of assessing risk, setting priorities, monitoring implementation and reassessing risks, within well-defined governance and management. This all sits within a broader national and international multi-stakeholder context.

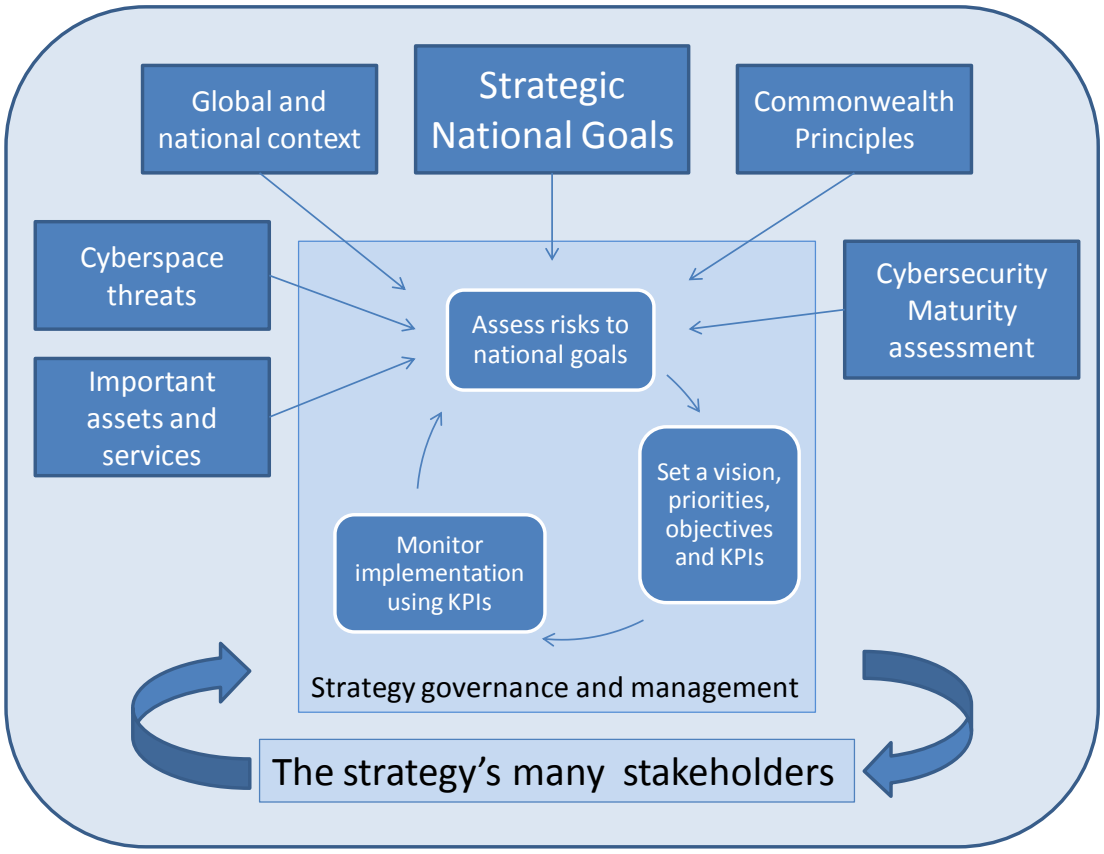

Figure 1 - illustrating a risk-based approach to delivering a national Cybersecurity strategy

The Cybersecurity Strategy's objectives should be derived from a risk-based assessment that considers the assets and services that are important to the country in the delivery of its national strategic goals, set against the prevailing Cyberspace threats and the practical mitigations that the strategy can put in place. The international standard, ISO-31000, describes risk management in considerable detail. For those who are not risk management professionals, there is a short guide that is aligned with ISO-31000, written by the Institute of Risk Management. Both are listed in appendix 2.

Elaborating on Microsoft's final point, there is a range of technology-neutral Cybersecurity standards and good-practice, starting with the internationally-recognised ISO-27000 series, augmented by more detailed controls, such as the Information Security Forum's Standard of Good Practice, listed in appendix 3. Countries should avoid creating their own Cybersecurity standards where possible because this will increase costs and risks for delivery of ICT systems and services from the global supply chain.

3.1.2 The use of a maturity model

A maturity model can indicate where a country lacks intrinsic capacity in aspects of Cybersecurity. Those capacities may be needed to reduce risks to national goals or to create opportunities for the country. For example, a maturity model might offer a measure of a country's Cybersecurity legal frameworks. Weaknesses in that framework for example may mean that the country must invest there first in order to make any progress. This maturity assessment information can be used in conjunction with the assessment of risks to national outcomes to make the complex determination about where investments are best placed, in line with the country's other priorities, for maximum practical effect. This is not a simple, deterministic process but a subjective activity requiring considerable multi-stakeholder consultation.

It is unlikely that a country will want to devote the necessary resources towards achieving the highest levels of maturity in all aspects of Cybersecurity, as soon as possible. Every country will have to consider the stages of maturity that can be attained and must prioritise this against competing demands for resources to meet other national strategic goals, as described in the previous section. An example model for the maturity of Cybersecurity of countries is listed in appendix 1.

3.1.3 Key performance indicators

To ensure the objectives of the national Cybersecurity strategy are being achieved, appropriate mechanisms should be put in place to monitor and validate its implementation. Effective monitoring and evaluation relies on the careful choice of key performance indicators (KPI) that ideally complement the key risks to national level outcomes identified earlier. In this way, the measure of performance is tied to the desired outcome, not to the consumption of resource. For example, one could measure the time taken to put laws on the statute book or the number of trained policemen but a better KPI would be to test the level of trust in online business, acknowledging that this is much harder to do. The use of a maturity model may support the generation of KPIs.

3.1.4 Resources and market forces

Some actions called for by the strategy will be delivered under the direct control of government agencies but those agencies are quite likely to lack the necessary skills and resources. Therefore, a key part of the strategy's design should consider, where necessary, including the allocation and development of those resources in order to respond to the strategy. Some actions will fall on the private sector and it is important that expectations are realistic and sympathetic to their commercial environment, to avoid perverse outcomes that may result when market forces respond to government intervention. A collaborative multi-stakeholder approach is vital to avoid such damaging outcomes.

3.1.5 Communicating its concepts and ideas

The choice of vocabulary used in Cybersecurity can represent a challenge because in English some words related to Cybersecurity can convey quite different meanings to different audiences across different sectors. Further, nuances are often lost in translation between languages. It is important that the specialist Cybersecurity words used in the national strategy are defined, in consultation with the key stakeholders, and recorded in a glossary. An example glossary accompanies this guide as appendix 4.

In preparation for launching a national Cybersecurity strategy and throughout its delivery, it may be beneficial to inform and educate media, politicians and other influential individuals, to harness their ability to influence the wider audience whose support will contribute to the strategy's success.

3.2 Delivering the Strategy

Once adopted and published, a national Cybersecurity strategy sets the direction for all participating stakeholders to follow in order to deliver its objectives and provides a vital communication of intention to the wider audience. Continuing professional communication to the public on progress is important to maintain that engagement and avoid a loss of confidence in the strategy's delivery.

A predominant and continuing risk to delivery of the national Cybersecurity strategy will be the fragmentation of stakeholders when they discover the details of its delivery to be in direct conflict with their other priorities. This fragmentation may occur between departments within the same government, between private sector interests, or any other combination. The strategy cannot be written to mitigate this risk entirely and a governance mechanism must provide the means to resolve these tensions. It is quite likely to require the appointment of a lead organisation or institution, ideally supported by respected and independent experts, to drive the delivery of the objectives set out in the strategy.

Trinidad and Tobago established the *Trinidad and Tobago Cyber Security Agency* (TTCSA)

The authority, design and operation of this multi-stakeholder governance mechanism is a key factor in the

success of the strategy and should take into account the particular needs and circumstances of each country, guided by the principles of the Cybergovernance Model and the values of the Commonwealth. The design of sub-committees and stakeholder engagement activities should be chosen carefully to reflect the goals and objectives (to be covered below) and how they fall across existing activities, relationships and structures in the country.

3.3 Reviewing the Strategy

Monitoring the implementation of the strategy helps identify gaps that may exist within the strategy for future review. The outcomes of the monitoring and evaluation should feed back into the strategy so that it is continuously improved. Given the rate of change of the underlying technology upon which Cyberspace operates, the strategy is likely to require reviewing and refreshing every 3 or 4 years. It may be most effective to align this to national budgetary and planning cycles. Within that cycle, some aspects of the strategy's delivery may require more frequent monitoring and revision, even quarterly. This will reflect the urgency of some tasks, the rapid rate of development of the threat and the developing skills and knowledge of the participants.

4 KEY ELEMENTS OF A CYBERSECURITY STRATEGY

This chapter of the guide offers a recommended structure for a National Cybersecurity Strategy and each of the following sub-chapters offers a short commentary on the purpose of the strategy's sections. Examples are provided to illustrate how some countries have approached particular aspects in their own national strategies, tailored to their needs. Appendix 5 provides a more detailed guide on the contents of each section including further examples from published strategies and other good practice.

4.1 Introduction and background section

Providing a broad context for a reader that is not immersed in the subject, this section explains the importance of Cybersecurity to national social and economic development, summarising background information on the use of Cyberspace, the risks and opportunities facing the country. This section should include an explicit assessment of the current state of Cybersecurity in the country, outlining the challenges being faced in securing Cyberspace, providing the justification for developing the Cybersecurity strategy. The use of a maturity model may help provide this assessment, offering a benchmark against other countries with similar circumstances.

This section should also explain how the Cybersecurity strategy aligns to the country's development goals and plans; and how it relates to any other relevant national strategies and initiatives such as for broader national security, telecommunications, education, energy, trade and industry, tourism, law enforcement and defence.

4.2 Guiding principles section

This section should reflect the culture of the country expressed as some national principles, as appropriate, and the Commonwealth Cybergovernance principles as the guidance in the development of national strategic goals.

In particular, the strategy should reflect the conscious and continuous balance of the achievement of security goals while respecting privacy and the protection of civil liberties. This section should explain how this active balance will be maintained.

4.3 Vision and strategic goals section

Framed by the principles set out above, the national Cybersecurity strategy should set a clear direction to establish and improve Cybersecurity for government, academia, consumers and service-providers who serve those communities. This may be expressed as a set of national strategic goals that place demands on the Cybersecurity strategy. As shown in figure 1 above, these goals are generally created outside the Cybersecurity strategy from the wider national agenda. Examples, from a range of sources in appendix 1, include:

- Promote economic development. Providing a safe environment for users of Cyberspace engenders a level of trust among international business community to develop, with confidence, trade relations with such countries. Those trade relations also enable the country to participate in the global economy. In the long run, this contributes towards the economic development of the country;
- Provide national leadership. This demonstrates a strong commitment of government to work with and bring cohesion to the necessary stakeholders in addressing Cybersecurity;
- Tackle Cybercrime. For many countries, this is a priority, to reduce the corrosive and pernicious effects of on-line crime;
- Strengthen the critical infrastructure. Identifying the scale, scope and approach to securing the country's critical national infrastructure;
- Raise and maintain awareness. One major challenge facing national economies in addressing the subject of Cybersecurity is the low knowledge levels of users in Cyberspace. With improved awareness, Cyberhygiene improves;
- Achieve shared responsibility. Citizens and businesses have a responsibility, with their service providers, for their own security. The owners of ICT networks bear the responsibility, with their suppliers, of putting the necessary measures in place to secure their own systems;
- Defend the value of Human Rights. It is important to achieve the right balance between national security objectives and citizens' right to freedom of expression, to privacy and access to information. Governments need to be alert not to introduce

> Austria has declared a goal of using "self-regulation" to encourage the private sector to set its own detailed standards on Cybersecurity whilst the state creates the necessary overarching regulatory framework.

disproportionate censorship when addressing concerns about the inappropriate use of the Cyberspace including social media;
- Develop national and international partnerships. A key component in delivering security in Cyberspace is the collaboration within and beyond national boundaries. This covers national and international initiatives;

For many national strategies, these goals are combined to form the pillars on which the strategy is built. They are chosen carefully to offer a simple-to-grasp expression of what the strategy seeks to achieve. These strategic goals can be a powerful aid in communicating the strategy to a wider audience.

Canada has the following strategic Cybersecurity goals:
- Secure government systems;
- Partner to secure vital cyber systems outside the federal government; and
- Help Canadians to be secure online.

Some countries may want to define a vision or mission statement. This is a matter of choice and can also be a powerful aid in communicating the strategy by describing the end-state of the activities called for by the strategy in a more discursive form.

"Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society." UK Cybersecurity Strategy

4.4 Objectives and priorities section – using a risk-based approach

In order for the Cybersecurity strategy to deliver those high-level goals, more detailed and clearly articulated, practical and tangible objectives should be expressed in this section of the strategy. The relative priority of the objectives should be explained, as justified by the analysis of risk to strategic national outcomes. This section should also describe briefly its risk management method including how the country sets about understanding threats and vulnerabilities. The strategy may separate risks into categories, indicating that some can be managed or mitigated while others must be accepted because there is no practical treatment. In the latter case, the country's resources may be better spent in preparing to remediate in the event of an incident.

Examples of objectives found in published Cybersecurity strategies, listed in appendix 1, include:
- providing a national governance framework for securing Cyberspace
- enhancing the country's preparedness to respond to the challenges of Cyberspace
- strengthening Cyberspace and national critical infrastructure to support economic development
- securing national ICT systems to attract international businesses
- building a secure, resilient and reliable Cyberspace
- building relevant national and international partnerships and putting effective political-strategic measures in place to promote Cyber safety
- developing a culture of Cybersecurity awareness among citizens

- promoting a culture of "self protection" among businesses and citizens
- creating a secure Cyber environment for the protection of businesses and individuals
- building skills and capabilities needed to address Cybercrime
- becoming a world leader in Cybercrime-preparedness and Cybercrime-defence

Objectives of this kind should be developed further in order to make them SMART[1].

4.5 Stakeholder section

The delivery of these objectives will involve a wide range of stakeholders, who should be identified in this section of the national Cybersecurity strategy. The majority of the technical infrastructure that comprises Cyberspace is designed, built, owned and operated by the private sector. These companies are often multi-national with complex international supply chains. The threats posed by Cybersecurity transcend national borders and call for strong coordination mechanisms nationally, regionally and internationally and across sectors. In constructing the list of stakeholders, a wide range of constituencies should be considered, including policy makers, officials from across most government departments, specific agencies, private sector representatives from many industries, civil society, academics, international bodies and possibly other countries.

> "The Government of the Republic of Trinidad and Tobago (GoRTT) will partner with the private sector and civil society in the implementation of its cyber security strategy"

Stakeholders will most likely have to collaborate with a range of other stakeholders in order to achieve their objectives. For example, law enforcement may work with internet service providers in order to secure evidence of criminal activity; defence may work with owners and operators of critical national infrastructure on which military activities depend, in order to understand the potential impact of a Cybersecurity incident.

The action of making a maturity assessment can help identify issues that could otherwise be overlooked and help produce or refine a list of stakeholders. Appendix 5 offers a list of potential stakeholders to consider.

4.6 Governance and management structure

Implementation requires a governance and management structure that brings together all stakeholders and harnesses each stakeholder's strengths and competencies. This will most likely require a central body with the mandate to coordinate the activities to deliver the national strategy, under internal and external scrutiny to provide transparency of performance. In some circumstances, direct control of delivery activities through budgetary authority will be necessary.

[1] Often defined as Specific, Measureable, Achievable, Relevant and Time-bounded though other definitions exist. See http://en.wikipedia.org/wiki/SMART_criteria

Effective delivery will also most likely depend on innovative collaboration between stakeholders, without the need for explicit detailed direction from centre and direct involvement of the management structure. Collaboration should take place spontaneously, as needed, at all levels of implementation such as capacity building, R&D, awareness creation and in particular for operational incident response. The starting point will be information-sharing. Collaboration will develop naturally once the mutual benefit is identified, given positive encouragement from the national Cybersecurity strategy and recognition from those in authority.

Nevertheless lines of authority and reporting should be clear and unambiguous. To achieve both outcomes, it may be helpful to construct a table of stakeholders that records the individuals who are responsible, accountable, consulted and informed about the major topics of the strategy[2]. It may require some debate to determine this structure. Once finalised, it should be recorded in the strategy document. Appendix 6 offers an example of a RACI table.

4.7 Strategy implementation section

Having set out the high-level objectives and identified the stakeholders, this section should describe how the work is divided into manageable components. The following headings are illustrative and the structure of each country's strategy must reflect the country's needs, existing structures and immediate risk-based priorities for action.

4.7.1 Legal and regulatory framework

The legal and regulatory framework is a foundation to any national Cybersecurity capability, particularly for law enforcement activities, and must remain under continuous review in order to be effective and to reflect the contemporary risks and opportunities arising from the rapid evolution of Cyberspace. In this section, the national Cybersecurity strategy should describe how government will set about achieving this in broad terms, without describing the legislative programme itself, and set targets to:

- Review existing frameworks and develop new ones to remain up-to-date with current technological developments;
- Harmonise existing national laws with Cybersecurity needs;
- Develop and maintain appropriate enforcement mechanisms including cross-border co-operation and mutual assistance;
- While maintaining and protecting privacy and civil liberties of individual.

4.7.2 Capacity Building

Cybersecurity being a new and fast evolving field, national Cybersecurity strategies should address the acquisition of required skills and competencies. It is quite likely that there will be skills shortages in many areas including across all the stakeholders needed even just to develop the national strategy. In view of the range of stakeholders and

[2] Responsible, Accountable, Consulted and Informed: the so-called RACI table. For more on this approach, see http://en.wikipedia.org/wiki/Responsibility_assignment_matrix

institutions involved, a training needs assessment is recommended, including those that are initially ancillary to the Cyber agenda, in order to develop adequate, comprehensive capacity building programmes. Given the fast pace and unpredictable nature of developments in Cyberspace, training needs will require continuing reassessment. Appendix 5 offers some possible approaches.

4.7.3 Awareness

In view of the impact on general public, raising awareness across all sectors and levels of society is a critical component of any Cybersecurity strategy. The awareness campaign should be designed to sit alongside the capacity building activity, providing a simpler message to a much wider audience. The Commonwealth Cybergovernance Model principles emphasise that users have rights and responsibilities, including operating in Cyberspace with an acceptable level of Cyber hygiene. This includes taking proportionate responsibility for their ICT systems and for their behaviour on-line. Appendix 5 describes some of the measures adopted by countries to increase Cybersecurity awareness of citizens.

4.7.4 Local technical capability

A country needs its own technical experts in Cybersecurity in order to advise the government in performing its own work and when placing contracts with other organisations. Research and Development, for example in universities, plays a critical role in developing capacity for Cybersecurity and has been identified as one of the key pillars of a number of Cybersecurity strategies. Cyberspace is developing rapidly and new tools to secure it need to be developed at a correspondingly rapid pace, creating an acute need for R&D in Cybersecurity. Ways of encouraging R&D in Cybersecurity are set out in appendix 5.

4.7.5 Incident response

It is no longer possible to construct the necessary defensive mechanisms to guarantee that there will never be an incident to jeopardise the safety, security and resilience of the country's use of Cyberspace – that is not a viable strategy – therefore, national Cybersecurity strategies must plan for incidents. Those incidents will often require a range of stakeholders to pool their knowledge and skills in order to bring swift remedy yet many of those stakeholders will be commercial rivals in the private sector. Sensitive commercial and personal data may need to be shared in a trusted, proportionate and legally-permitted fashion, encouraged and obliged by national policy, while protecting the interests of the data owners. This may require some government encouragement and endorsement, even light-touch facilitation. Once established, it should operate spontaneously and at the operational pace required to deal with the incident.

Governments are uniquely placed in terms of national visibility, national responsibility and commercial impartiality to bring representatives from across the public sector, private sector, civil society and academia together in order to share vital, timely information about incidents. Governments are also uniquely placed to establish operational links with neighbouring governments, to share information of common and

mutual interest in a similar manner. Such relationships often develop based on personal trust between individuals, operating with the consent of their parent organisations, within a legal framework.

This can be difficult to achieve without the incentive of an impending crisis. However, it will be too late to start establishing those relationships during a crisis. One approach is to create a network of CERTs (Computer Emergency Response Teams, also referred to as Computer Incident Response Teams) who routinely share information, suitably anonymised where necessary. The FIRST network and the OAS G-8 24/7 Network may offer advice and support in incident response (see appendix 1). The network of CERTs then forms the foundation for a crisis response capability that can then be linked to the country's established crisis management mechanisms, which will already have the vital connections to ministers in order to secure the necessary authority to act in an emergency.

The national Cybersecurity strategy will need to describe how these mechanisms will be established and how they will be exercised to test their continuing effectiveness. Appendix 5 offers an example approach.

4.8 Monitoring and evaluation

This section should set out the Key Performance Indicators by which progress will be measured and the method by which the data will be collected. It will want to identify the nature of reporting required from participating stakeholders and the responsibility for collating the data to achieve transparency in reporting progress against the strategy's objectives. This is a very difficult topic in any delivery activity because the simplest measurements are often about delivery activity but the act of measuring inevitably alters the deliverer's perspective on priorities, sometimes with unintended and perverse consequences. A better, alternative approach is to measure the outcome or end state by posing questions to those stakeholders who are intended to benefit, while accepting that such metrics will be much more subjective.

5. Conclusion and next steps

The CTO believes that every country should have a national Cybersecurity strategy. Modern countries are increasingly dependent on this man-made information space of Cyberspace for many aspects of everyday life. It has become a vital part of our social, economic and governmental activities. This guide offers a starting point to develop a national Cybersecurity Strategy.

We recommend a risk-based approach, framed by principles that reflect the country's culture and the Commonwealth Cybergovernance Principles. Design and delivery of the strategy should include a wide range of stakeholders from across the public and private sectors, across academia and drawn from civil society.

Cyberspace is a global phenomenon and every country's strategy should reflect the complex international supply chain that supports technology of all kinds and of Cyberspace in particular. Further, the strategy should consider its impact beyond its country's borders, regionally and globally.

For many, this work is urgent. Some countries have published their strategies on-line and there are other sources of guidance and support available on-line offering a further helpful resource for an author. The Commonwealth itself is a platform to share expertise, resources and experiences and the CTO's Cybersecurity mini site offers further resources (see appendix 1).

6. Acknowledgements

The CTO is grateful to the International Telecommunication Union (ITU), the Organisation of American States (OAS) and Microsoft for their advice, guidance and support in the compilation of this publication.

Appendix 1 LINKS TO NATIONAL STRATEGIES AND OTHER REFERENCES

No.	Source	Title	URL
1.	Austria	Austria Cyber Security Strategy	https://www.bka.gv.at/DocView.axd?CobId=50999
2.	Australia	Cyber Security Strategy	https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AGCyberSecurityStrategyforwebsite.pdf
3.	Canada	Canada's Cybersecurity Strategy	https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf
4.	France	Information Systems defence and security	http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf
5.	Finland	Finland's Cyber Security Strategy	http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
6.	Germany	Cyber Security Strategy for Germany	http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
7.	India		https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NationalCyberSecurityPolicyINDIA.pdf
8.	Netherlands	National Security Strategy	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf
9.	Spain	National Cyber Security Strategy	https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf
10.	Switzerland	National strategy for the protection of Switzerland against cyber risks.	https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf
11.	Trinidad & Tobago	National Cyber Security Strategy	http://www.nationalsecurity.gov.tt/Portals/0/Pdf%20Files/National_Cyber_Security%20Strategy_Final.pdf

No.	Source	Title	URL
12.	Italy	National strategic framework for cyberspace security	http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf
13.	United Kingdom	The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
14.	U.S.A	The National Strategy to Secure Cyberspace	https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
15.	Uganda	National Information Security Strategy	http://www.sicurezzacibernetica.it/en/[Uganda]%20National%20Cyber%20Security%20Strategy%20-%202011%20-%20EN.pdf
16.	ITU	ITU draft Cybersecurity framework	http://groups.itu.int/Default.aspx?tabid=841 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf
17.	ITU	ITU National Cybersecurity Strategy guide	http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
18.	OAS	Inter-American strategy	http://www.oas.org/cyber/documents/resolution.pdf
19.	OECD	Cybersecurity Policy Making At A Turning Point	http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf
20.	SADC	HIPSSA Computercrime and Cybersecurity	http://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf
21.	ENISA	National Cyber Security Strategies	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper
22.	ENISA	National Cyber Security Strategies: Practical Guide on Development and Execution	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Other references for further reading			
1.	Commonwealth	The Commonwealth Charter from which the principles in the Commonwealth Cybergovernance model are derived.	http://thecommonwealth.org/our-charter
2.	CTO	The Commonwealth Cybergovernance model agreed in March 2014	http://www.cto.int/media/pr-re/Commonwealth%20Cybergovernance%20Model.pdf
3.	CTO	The CTO Cybersecurity mini-site maintains an up-to-date list of National Cybersecurity Strategies	http://www.cto.int/priority-areas/cybersecurity/national-cybersecurity-strategies/
4.	CTO	The CTO Cybersecurity mini-site provides a list of other useful links relating to National Cybersecurity Strategies	http://www.cto.int/priority-areas/cybersecurity/web-links-cyber/
5.	First	FIRST brings together computer security incident response teams from government, commercial, and educational organizations, to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing.	http://www.first.org/
6.	GCSCC	Global Cyber Security Capacity Centre's Cyber Security Capability Maturity Model provides a scientific framework to better understand national capacity in Cybersecurity. This is aimed at helping nations to self-assess, to benchmark, better plan national strategies and set priorities and investments for capacity development.	https://www.sbs.ox.ac.uk/cybersecurity-capacity/ See also: http://www.oxfordmartin.ox.ac.uk/cybersecurity/dimensions

7.	Microsoft	A guide: Developing a national strategy for Cybersecurity: foundations for Security, Growth, and Innovation.	http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf
8.	NATO CCDCOE Cooperative Cyber Defence Centre of Excellence	The Tallinn Manual on the International Law Applicable to Cyber Warfare examines how extant international law norms apply to this 'new' form of warfare.	https://www.ccdcoe.org/328.html
9.	OAS	The OAS has compiled and systematized the existing cyber-crime legislation of the OAS Member States.	http://www.oas.org/juridico/english/cyber_nat_leg.htm
10.	OAS	The G-8 24/7 Network for Data Preservation provides points of contact in participating countries that require urgent assistance with investigations involving electronic evidence.	http://www.oas.org/juridico/english/cyber_g8.htm

Appendix 2 RISK MANAGEMENT STANDARDS AND GOOD PRACTICE GUIDES

Note that this table contains a selection of some well known publications but many others exist.

Name of standard	Authority who developed the standard	Comment on the nature of the standard	URL
ISO-31000 (issued 2009)	**ISO** The International Organization for Standardization develops and publishes International Standards**.**	ISO-31000 is the internationally-recognised standard for risk management. It is detailed in its coverage and has to be purchased.	http://www.iso.org/iso/catalogue_detail?csnumber=43170
The IRM's risk management standard (issued 2002)	**IRM** The Institute of Risk Management	This is a easy-to-read 16 page guide that the IRM targets at business professionals. It is free to download and available in 16 languages. It was written to be consistent with ISO vocabulary on risk management.	https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf
The IRM's cyber risk executive summary (issued 2014)	**IRM** The Institute of Risk Management	This is an easy-to-read 18 page free summary of a more detailed document that has to be purchased.	https://www.theirm.org/media/883443/Final_IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf

Appendix 3 INTERNATIONAL STANDARDS AND GOOD PRACTICE GUIDES FOR CYBERSECURITY

Note that this table contains a selection of the better known publications but many others exist.

Name of standard	Authority who developed the standard	Comment on the nature of the standard	URL
ASD Strategies to Mitigate Targeted Cyber Intrusions, previously known as the Top 35 (Revised Feb 2014)	**ASD** The Australian Signals Directorate is part of the Australian government.	ASD claims that least 85% of the targeted cyber intrusions that the ASD responds to could be prevented by following the top 4 mitigation strategies	http://www.asd.gov.au/infosec/top35mitigationstrategies.htm
The BSI IT-Grundschutz (Continuously revised)	**BSI** Bundesamt für Sicherheit in der Informationstechnik (abbreviated BSI - in English: Federal Office for Information Security)	The aim of IT-Grundschutz is to achieve an appropriate security level for all types of information of an organisation. IT-Grundschutz uses a holistic approach to this process. It offers extremely detailed requirements across a range of documents	https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html and https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html
COBIT 5 (Issued April 2012, superseding COBIT 4.1)	**ISACA** A non-profit, global membership association for IT and information systems professionals,	ISACA claims that COBIT 5 is the only business framework for the governance and management of enterprise IT.	http://www.isaca.org/COBIT/
ISF Standard of Good Practice (Revised in 2014 and	**ISF** The Information Security Forum is a not-for-profit organisation that supplies	Updated annually, the Standard of Good Practice for Information Security (the Standard) claims it is the most comprehensive information security standard in the world, providing more coverage	https://www.securityforum.org/

every year)	opinion and guidance on all aspects of information security. It is a leading international authority on information risk management.	of topics than ISO.	
ISO-27000 (Revised in 2014)	**ISO** The International Organization for Standardization develops and publishes International Standards**.**	ISO-27000 is the international standard for Information Security. The ISO 27000 family of standards helps organizations keep information assets secure. ISO 27001 describes an information security management system (ISMS).	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63411
NIST SP800-53 (Revision 4 issued April 2014)	**NIST** US National Institute for Standards and Technology	One of a range of publications in the SP800 series, this describes Security and Privacy Controls for U.S. Federal Information Systems and Organizations.	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
SANS Top 20 Critical Security Controls	The **SANS** Top 20 is now maintained by the Council on CyberSecurity, an independent, global non-profit entity committed to a secure and open Internet.	The Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works".	http://www.sans.org/critical-security-controls
UK 10 Steps to cyber security	**UK Government** This publication is the work of multiple UK government agencies: BIS, CPNI, GCHQ and the Cabinet Office.	This publication is aimed at the senior reader and sets out the most important topics to focus on first. It contains a mixture of technical and non-technical measures.	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

Appendix 4 SAMPLE GLOSSARY

Note that in many cases there is no single, universally-accepted definition. This table provides those in common use, drawing on internationally-recognised sources. Words that are underlined are themselves defined in this glossary.

Word	Definition	Source
Availability	Availability is a property or characteristic. Something is available if it is accessible and usable when an authorized entity demands access.	ISO
Confidentiality	Confidentiality is a characteristic that applies to information. To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes.	ISO
Control	In the context of information security management, a control is any administrative, managerial, technical, or legal method that is used to modify or manage information security risk. Controls can include things like practices, processes, policies, procedures, programs, tools, techniques, technologies, devices, and organizational structures. Controls are sometimes also referred to as safeguards or countermeasures. (See ISO27000 for more detail on this.)	ISO
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment	NIST ITU

Cyberspace	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.	NIST
Documented information	The term documented information refers to information that must be controlled and maintained and its supporting medium. Documented information can be in any format and on any medium and can come from any source. Documented information includes information about the management system and related processes. It also includes all the information that organizations need to operate and all the information that they use to document the results that they achieve (aka records). In short, the term documented information is just a new name for what used to be called documents and records. But this change is significant. In the past, documents and records were to be managed differently. Now the same set of requirements is to be applied to both documents and records.	ISO
Information Security	The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable.	ISO
Integrity	Within the narrow context of information security, the term integrity means to protect the accuracy and completeness of information.	ISO
Resilience	The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning. Also The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.	NIST
Risk	According to ISO 31000, risk is the "effect of uncertainty on objectives" and an effect is a positive or negative deviation from what is expected. (See ISO31000 for more on this.)	ISO

Risk management	Risk management refers to a coordinated set of activities, methods, and techniques that organizations use to deal with the risk and uncertainty that influences how well they achieve their objectives.	ISO
Safety	The condition of being protected from or unlikely to cause danger, risk, or injury	OED

Source	Reference	URL
ISO	ISO27000 Plain English Information Security Definitions of 2014	http://www.praxiom.com/iso-27000-definitions.htm#Business_continuity
ITU	International Telecommunication Union definition of Cybersecurity	http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
OED	Oxford English Dictionary	http://www.oxforddictionaries.com/
NIST	NISTIR7298 Revision 2 Glossary of Key Information Security Terms of May 2013	http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Appendix 5 NATIONAL CYBERSECURITY STRATEGY – OUTLINE GUIDE

STRATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
1. Introduction / background This section provides a succinct background of the country's circumstances and the status of its Cybersecurity	• Explain the importance of Cybersecurity to economic and social development. • Describe the use of Cyberspace and the nature of Cybersecurity challenges to justify the need for the Cybersecurity strategy • Explain the relationship to existing national strategies and initiatives.	**Uganda**'s introduction covers: • The definition of information security • The justification for a strategy • Country analysis of current state of information security framework. • Strategy guiding principles • Vision, mission, strategic objectives Note that this example covers the first three sections in this guide.
2. Guiding principles This section identifies the guiding principles for addressing Cybersecurity within which the strategy is designed and delivered.	• Build from the principles of the Commonwealth Cybergovernance model. • Include any relevant national principles. • Describe the approach that guides the design of the objectives goals, vision and objectives. • Consider the suitability of programme and project management methodology that is used by the government.	In addition to the Commonwealth Cybergovernance principles and national principles the following approach is recommended: • Risk-based. Assess risk by identifying threats, vulnerabilities, and consequences, then manage the risk through mitigations, controls, costs, and similar measures. • Outcome-focused. Focus on the desired end state rather than prescribing the means to achieve it, and measure progress towards that end state. • Prioritised. Adopt a graduated approach and focus on what is critical, recognising that the impact of disruption or failure is not uniform among assets or sectors. • Practicable. Optimise for adoption by the largest possible group of critical assets and realistic implementation across the broadest range of critical sectors. • Globally relevant. Integrate international standards to the maximum extent possible, keeping the goal of

STRATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
		harmonization in mind wherever possible.
3. Strategic goals and vision This section defines what success looks like in broad summary terms and reflects the country's priorities. The country's strategic goals, as affected by Cyberspace, should be stated in this section, to link the strategy to the country's broader agenda.	• Make a clear statement of the country's commitment to protecting the use of its Cyberspace • Emphasise the breadth of the use of Cyberspace: covering social and economic activity • Include text that can be quoted as part of the communication with wider stakeholders, e.g. a vision statement.	**Australia**'s vision: "The maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy" Three pillars of the **Australian** strategy: • All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online; • Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers; • The Australian Government ensures its information and communications technologies are secure and resilient." Four pillars of the **UK** strategy: • Tackle cybercrime and be one of the most secure places in the world to do business in cyberspace; • To be more resilient to cyber attacks and better able to protect our interests in cyberspace; • To have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies; • To have the cross-cutting knowledge, skills and capability it needs to underpin all our Cybersecurity objectives.
4. Objectives and priorities – using a risk-based approach. This section links the country's	• How risk management is currently performed, for example for national security. • Key assets and services that are	From Microsoft's guidance, listed in appendix 3: • A clear structure for assessing and managing risk • Understand national threats and major vulnerabilities • Document and review risk acceptance and exceptions

STRATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
strategic goals to the detailed objectives of the strategy. This section describes how risks to those strategic goals arising from Cyberspace require specific and tangible objectives to be set. It also assigns relative priorities.	affected by or supported by Cyberspace, e.g. critical infrastructure. • Cybersecurity maturity of the country and any key weaknesses. • Sources of threat information and of major vulnerabilities. • How granular to make the outcomes and objectives. • How frequently to repeat the risk assessment process.	• Set clear security priorities consistent with the principles • Make national cyber risk assessment an ongoing process
5. Stakeholders This section identifies key participants in the development and delivery of the strategy. Roles and responsibilities should be clearly defined using RACI terminology (see appendix 5). This section will also describe how national and international	• Identify all relevant key stakeholders taking into consideration, country objectives and focus areas • Identify key international stakeholders and partners that could contribute effectively • Draw stakeholders from governmental and non-governmental organizations, civil societies, academia, public and private sectors of the economy. Should include but not limited to software and equipment vendors, owners and operators of CII, law enforcement institutions etc. Steps to encourage collaboration: • Encourage promising national, regional and International	In constructing the list of stakeholders, the following constituencies should be considered: • ministers and other politicians; • government departments concerned with ICT, telecommunications and information security; • private sector organisations that provide ICT services; • government departments whose responsibilities rely upon or who engage with Cyberspace, including: most economic activity, trade, defence, tourism, law enforcement, etc; • providers of the critical national infrastructure whose vital communications are increasingly carried across the internet; • companies across the economy that rely upon Cyberspace, often represented by trade associations; • representatives of civil society, often in the form of groups that reflect broad public opinion and can advise on the best way to achieve outcomes involving the public; • civil society organisations that represent particular parts of society or interest groups and can explain, for example, the needs of the young, of women, of rural communities and of the vulnerable;

STRATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
collaboration will be encouraged between stakeholders. The starting point will be information-sharing.	collaboration schemes by starting with information sharing about common interests. • Establish bilateral and multilateral partnerships with relevant institutions. • Establish inter-governmental collaboration, particularly regional. • Establish Public-Private-Partnerships with stakeholders in Cyberspace (e.g. ISPs, operators of infrastructure network)	• experts who understand how Cyberspace works, from a technical perspective, to ensure that government strategies are practical; • Academia who can advise on R&D, international best practice, emerging issues, etc; • International bodies such as the Commonwealth Telecommunications Organisation • Other countries, particularly regional countries. "Develop strategies and partner with international reputable organizations that will help it build capacity to manage any risk associated with information security arising out of border cyber activity."- **Uganda** "Ensure effective collaboration on cyber security in Europe and worldwide." – **Austria** "Develop an international engagement strategy to clearly define and articulate **Australia**'s national interests and priorities in relation to cyber security and resilience." "Encourage international and regional organizations to support capacity building, for example working with the Commonwealth to promote model legislation on cybercrime, with the ITU to support training on technical standards, with the Council of Europe and the Organisation for Security and Co-operation in Europe (OSCE) to promote freedom of expression online." – **United Kingdom** "Canada will also build on its existing engagement in

STRATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
		cybersecurity discussions at key international fora, such as the United Nations, NATO and the Group of Eight. We are one of the non-European states that have signed the Council of Europe's *Convention on Cybercrime*, and the Government is preparing legislation to permit ratification of this treaty" - **Canada**. "Effective coordinated action to ensure cyber security in Europe and worldwide." – **Germany**
6. Governance and management structure This section describes the establishment of governance and management for the strategy, covering its development and delivery. This must include management of monitoring and improvement.	• Establish a strong leadership role at the highest level to give priority and recognition to the strategy. • Establish suitable multi-stakeholder governance of the strategy to cover all aspects. This should cover all economic sectors, civil society, private and public sectors. • Identify and establish activities required to monitor and validate the strategy's implementation. • Note: the management and monitoring of the strategy's delivery may require a small full-time staff. • Management of crises (covered later) must be considered as part of the governance structure. • Adopt measures to foster institutional and technical collaboration. • Consider creating centres of excellence in cyber security	"The Specialised Cyber Security Committee will support the National Security Council in performing its functions, particularly in assisting the Prime Minister in directing and coordinating the National Security Policy in the field of cyber security." - **Spain** "The Specialised Situation Committee will be convened to manage crisis situations in the field of cyber security ..." - **Spain** "The Specialised Cyber Security Committee and the Specialised Situation Committee will act in a complementary manner, each in its own area of responsibility but under the same strategic and political direction of the National Security Council chaired by the Prime Minister." - **Spain** Establishment of a Trinidad and Tobago Cyber Security Agency (TTCSA) – **Trinidad and Tobago** Establishing a Cyber Security Steering Group; Creating a structure for coordination at operational level; Establishing a Cyber Crisis Management – **Austria** Creation of an Information Security Advisory Group to provide

STRATEGY COMPONENTS		ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
			advisory service to information security governance – **Uganda**
7. Implementation This section identifies activities in more detail.		• Define practical actions to be undertaken. • Group actions into categories convenient for their management.	
	7.1 Legal and regulatory Framework This section describes any legislative programme needed to define serious malicious acts in Cyberspace as prohibited criminal acts. It also describes legal, policy and regulatory measures to enable or compel desirable behaviours.	• Review existing criminal codes regarding Cybercrime and amend as necessary to meet global best practice. • Review legislation and consequent regulation concerning protection of the Critical Infrastructure. • Harmonise and develop legislation to facilitate collaboration and information-sharing between institutions. • Provide protection for intellectual property.	Harmonise existing national security laws with Cybersecurity laws to facilitate collaboration and implementation among relevant institutions. Develop/review appropriate mechanisms to enforce cybercrime legislation. Translate policies into legislations, where appropriate, to make them legally binding. Develop regulation necessary for Critical Information Infrastructure Protection (CIIP[3]).
	7.2 Capacity Building This section set out the actions to develop	For people: • Perform training needs analyses for all relevant sectors and institutions. • Design capacity building	• Develop courses to train Cybersecurity experts with special attention on critical sectors, i.e. international standards, legal and regulatory. • Develop recruitment and retention strategies aimed at

[3] Critical Information Infrastructure Protection is explained by many sources including at http://www.oecd.org/sti/ieconomy/ciip.htm

STRATEGY COMPONENTS		ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
	human and institutional capacity to deliver the strategy and continue to develop to deliver the needs to Cybersecurity in the future.	programmes. For institutions: • Perform a needs analysis to identify the skilled staff required. • Develop recruitment and retention strategies to attract the right skills into critical jobs.	ensuring a sufficient level of technical expertise is developed and maintained within government agencies – **Australia** • Provide for acquiring information security officers in Government Ministries, Departments and Agencies – **Uganda** • Integrate Cybersecurity into national education curricula to build basic cyber skills into the country's national workforce, particularly those engineers who design, build and operate ICT systems. • Establish skills and competency based training programs similar to the computer driving license (i.e. a Cybersecurity driving license) to improve the knowledge of general public and their ability to operate in Cyberspace in a responsible, safe and secure manner. • Collaborate with international partners and training providers to meet the training needs of the country as well as participating in regional and international forums; Establish a network of Cybersecurity experts to encourage information and knowledge sharing.
	7.3 Awareness Complementary to the capacity building section, this concerns the means to raise awareness and thereby improve Cyber hygiene among users of Cyberspace, in both the public and private sectors and across civil	• Arrange periodic sensitization activities to increase and maintain awareness (e.g. annual awareness week) • Design educational communication tools (e.g. web-based information, use of social-networks). • Create a culture of responsibility for good Cyber behaviour. • Develop special awareness initiatives for the protection of children and other vulnerable groups when online.	"Promote a national culture of cyber security consistent with United Nations General Assembly Resolutions 57/239 entitled "Creation of a global culture of cyber security"; and 58/199 entitled "Creation of a global culture of cyber security and the protection of critical information infrastructures" – **Trinidad & Tobago** Strengthening a cyber security culture; incorporating cyber security and media competence into all levels of education and training; – **Austria** Establish an effective mechanism of disseminating information security issues for different constituencies – **Uganda**

STRATEGY COMPONENTS		ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
	society.	• Encourage service providers to establish consumer alert systems and ensure implementation.	Promote, foster and maintain culture of information security for awareness creation in Government, business and private sectors, civil society and the citizenry. Organize annual events to promote information security. Raise the awareness of citizens, professionals and companies about the importance of Cybersecurity and the responsible use of new technologies and the services of the Information Society
	7.4 Local Technical Capability This section describes how the country will develop its own experts to guide the country's Cybersecurity activities. The research and development capacity of academia, the private sector and government have a central role to play and will be encouraged to work together to tackle Cybersecurity challenges.	• Give Cybersecurity R&D programs an appropriate priority in the national development agenda. • Coordinate national and international R&D activities. • Develop linkages between R&D outcomes and policy development. • Harmonize R&D activities at the national level (e.g. between Private & Public sector) • Invest in academic R&D research where possible. • Recognise intellectual property rights as important for individuals to benefit from the fruits of their labours.	• Strengthen **Austria**'s research in the area of cyber security • Provide targeted funding and support for cyber security research and development activities through a range of programs such as the Research Support for National Security Program; • Develop an annual set of research and development priorities to inform the broader science and innovation community of the priority work required to achieve the **Australian** Government's cyber security policy. • Promote and provide Incentives for Research and Development (R&D) in the area of information security. • Promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development – **Uganda** • Support the application of research, working with the Government Office for Science and others to build innovative cybersecurity solutions, building on our world-leading technical capabilities in support of national security interests and wider economic prosperity; • Identify Centres of Excellence in cyber research to locate existing strengths and providing focused investment to address gaps. First focused investment by March 2012 –

STRATEGY COMPONENTS		ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
			United Kingdom • Promote the training of professionals, give impetus to industrial development and strengthen the research, development and innovation (R&D&I) system in cyber security matters – **Spain**
	7.5 Incident response This section describes the operational structures that will detect and deal with the inevitable Cybersecurity incidents.	• Create a network of CERTs that can handle minor incidents without central intervention. • Establish escalation paths and lines of authority for managing incidents of national significance. • Take active steps to establish trust between key organisations, to share sensitive information. • Exercise the system. • Consider whether feasible to use this network to assess the ability of organisations to resist attacks and their readiness to respond.	"A national Cybersecurity steering group or council with membership drawn from cabinet, national security, and relevant Ministries to ensure coordination at the political level." "A Cybersecurity agency/directorate/centre/focal point/institution to champion operational coordination of all Cybersecurity activities and initiatives nationwide, set up crisis management schemes, collaborate with similar international institutions to keep the country up-to-date with global Cybersecurity trends and advise government on matters relating to Cybersecurity through the relevant ministry(ies). The institution will be primarily responsible for: • Setting up national CERTs that will interface with other sectoral CERTs and international CERTs if feasible and charged with the responsibility of coordinating, managing and reporting cyber incidents, • Conducting Cybersecurity defence exercises to test the nation's Cybersecurity level of readiness and robustness, • Creating an alert system to inform of eminent attacks and trends in Cybersecurity, Developing a minimum set of national Cybersecurity standards and indicators for measuring robustness."
8. Monitoring and evaluation This section describes the method and the KPIs that will		• Measuring progress on delivering the strategy can be difficult because the choice of measurement can alter priorities	"The information technologies used are subject to short innovation cycles. This means that the technical and social aspects of cyberspace will continue to change and bear not only new opportunities, but also new risks. For this reason the

STRATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
be put in place in order to assess progress and provide feedback for governance and management. It should also describe the method for continuous monitoring of the Cyberspace environment.	and this can lead to perverse outcomes. • Assessments are best when performed by the customer, client or beneficiary, not the delivery organisation. • How to monitor the status of key cyberspace assets.	Federal Government will regularly review whether the aims of the Cyber Security Strategy have been achieved under the overall control of the National Cyber Security Council and will adapt the strategies and measures to the given requirements and framework conditions"- **Germany** Establishing a national approach for continuous monitoring of the highest-priority systems in order to respond to a changing threat landscape. – paraphrasing Microsoft advice

Appendix 6 EXAMPLE RACI TABLE

	Minister	Senior official	Junior official	A foreign government	A company
National Strategy	A	R	I	I	I
Selecting a project milestone involving a company	I	A	R	-	C

R = responsible, the person who actually performs the task
A = accountable, the person who must explain if the task is not done: "the buck stops here"
C = consulted, one or more people who may offer a view on the task
I = informed, one or more people who would expect to be told about the task