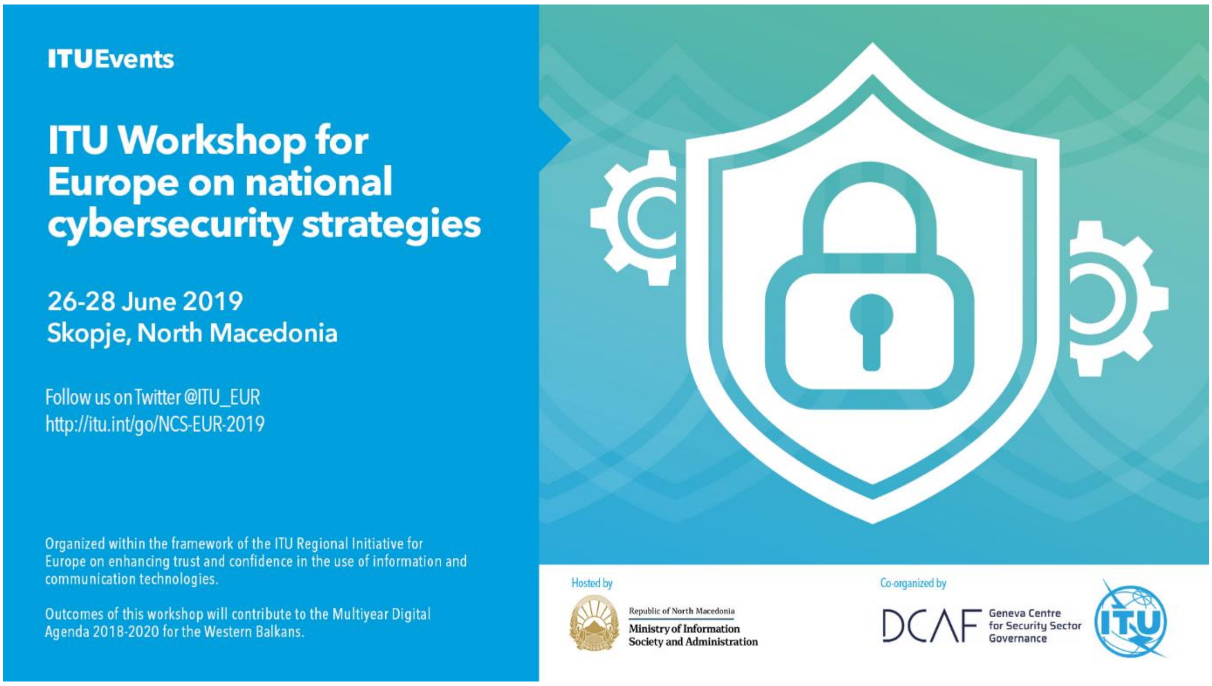


ITUEvents

ITU Workshop for Europe on national cybersecurity strategies

26-28 June 2019
Skopje, North Macedonia

Follow us on Twitter @ITU_EUR
http://itu.int/go/NCS-EUR-2019

Organized within the framework of the ITU Regional Initiative for Europe on enhancing trust and confidence in the use of information and communication technologies.

Outcomes of this workshop will contribute to the Multiyear Digital Agenda 2018-2020 for the Western Balkans.

Hosted by
Republic of North Macedonia
Ministry of Information Society and Administration

Co-organized by
DCAF Geneva Centre for Security Sector Governance
ITU

OUTCOME REPORT

ACKNOWLEDGEMENTS

This report has been produced by International Telecommunication Union (ITU). ITU would like to express their appreciation to the Ministry of Information Society and Administration of North Macedonia for hosting the event and to DCAF and Deloitte for providing inputs for the document.

TABLE OF CONTENT

List of Figures

1. Introduction

ITU Regional Workshop for Europe on "National Cybersecurity Strategies" was organized by the International Telecommunication Union (ITU) at the kind invitation of the Ministry of Information Society and Administration, in collaboration with DCAF. The Workshop took place in Skopje, Republic of North Macedonia, from 26 to 28 June 2019.

The workshop was organized within the framework of the ITU Regional Initiative for Europe on enhancing trust and confidence in the use of information and communication technologies adopted by the ITU World Telecommunication Development Conference 2017 (WTDC-17), that amongst others aims at elaboration, review of national cybersecurity strategies, and regional best practices with case studies. The workshop was supported by DCAF - Geneva Centre for Security Sector Governance and by Deloitte within the scope of the United Kingdom's FCO funded project 'Enhancing Cybersecurity Governance in the Western Balkans'. The workshop also benefited from the presence of the international experts involved in the development of the ITU guide to developing a National Cybersecurity Strategy.

Special attention was dedicated to the Western Balkan countries as a sub region at this workshop being given the ongoing digital integration process and the alignment with the Multi-year Digital Integration Plan 2018-2020. This report contains the main outcomes of the workshop on the way forward for the establishment/enhancement of the National Cybersecurity Strategy of each participating economy.

2. Participation

Representatives of European Ministries, CERTs, private sector, as well as representatives and experts of international organizations and institutions participated in the Workshop. The event was attended by 39 participants representing 10 Member States from ITU Europe region.

Figure 1: Group photo with speakers and participants of the workshop

3. Documentation

The workshop was paperless. 17 training sessions were delivered over the course of three days. Relevant documentation, including the Agenda are can be accessed from the ITU event web page.

4. Opening ceremony

The participants of opening ceremony were welcomed by:

- **H.E. Damjan Manchevski,** Minister of Information Society and Administration of North Macedonia
- **H.E. Ionut Andrei,** State Secretary, Ministry of Communication and Information Society, on the behalf of Romanian Presidency in the Council of European Union, EU
- **Mr. Marco Obiso,** Head of ICT Applications and Cybersecurity Division of International Telecommunication Union, ITU
- **Mr. Milan Sekuloski,** Senior Adviser at the Geneva Centre for Security Sector Governance, DCAF

Remarks by H.E. Damjan Manchevski, Minister of Information Society and Administration of North Macedonia

H.E. Manchevski welcomed all participants. He shared with all the commitment of North Macedonia to facilitating regional and international cooperation, while stressing on the importance of collaborating for a safer cyberspace given the growing number of interconnected IoT devices.

A cybersecurity assessment has been conducted for North Macedonia by the University of Oxford in cooperation with the World Bank. The North Macedonia National Cybersecurity Strategy and Action Plan for 2018-2022 was elaborated in collaboration with International partners including the European Commission. North Macedonia gives prominence to transparency and involvement of all the sector of the society. The public consultation of the National Cybersecurity Strategy was carried out inviting the public and private sector, civil, academia and others to provide comments and suggestions.

A resilient cybersecurity culture needs to be built on an open, safe and secure cyber space. More so, awareness raising, training and education are fundamental elements that are essential in development of a National Cybersecurity Strategy. It is necessary to introduce them not only to ICT professionals, but across all sections of society, ranging from citizens, all the way to the public administration officials. In order to fulfil this vital need in capacity building facilities and opportunities, North Macedonia is establishing **a Regional Cybersecurity Training and Research Centre** in Skopje for Western Balkans public administration officers and academia to take part, be trained, develop research, exchange and share practices in the field of cybersecurity.

H.E. Manchevski expressed confidence that the workshop would allow sharing of ideas and best practices in the field of development of a National Cybersecurity strategy among the economies. He wished all participants successful and fruitful work.

H.E. Ionut Andrei, State Secretary, Ministry of Communication and Information Society, on behalf of Romanian Presidency in the Council of European Union

Mr Andrei, on behalf of the Romanian Presidency in the Council, thanked the organizers and host. He emphasized that, cybersecurity has become a critical element for a better and more efficient society, as our future relies on digitalization in all sectors such as industries, administrations, businesses and citizens. The Romanian Presidency of the EU Council is working on the Digital Agenda to enhance Europe's transformation in advanced technologies. The Romanian Presidency contributed in several projects including the directive on Open Data and Reuse of Public Sector Information to boost EU data economy, the first Digital Europe programme, a tool for investment in ICTs, and on the regulations establishing the European Cybersecurity Competence Centre to support SMEs access to trainings.

A proposal of regulation on E-privacy has been passed in order to combine data protection and confidentiality of electronic communications in technologies. The Romanian Presidency also signed the Quantum Communications Infrastructure Declaration, a statement for Europe as one of the most innovative and safest infrastructure in the world.

Mr. Andrei concluded by highlighting how the Romanian Presidency is strongly promoting the development of digital technologies such as Artificial Intelligence, block-chain, 5G, high performance computing (HPC) and Internet of Things (IoT) according the European framework. He encouraged the audience to continue with their efforts and informed all that the next EU presidency will be held by Finland.

Marco Obiso, Head of ICT Applications and Cybersecurity Division, ITU

On behalf of ITU, Mr. Marco Obiso expressed gratitude to the Minister of information Society and Administration of North Macedonia for hosting the workshop. He pointed out the significant growth of cybersecurity needs and especially the increasing need to enhance collaboration in this field, not only through bilateral collaboration, but also a need to focus on multilateral collaboration, partnerships and cooperation. As cybersecurity threats and risks are rapidly evolving, it is important to share and gather knowledge from an outsider perspective thus offering new opportunities and create value chains in the field of cybersecurity. He urged that the workshop should not only limit to 3 days of theoretical presentations, but also focus on participants' contributions, with a specific attention on sharing best practices in the development of a national cybersecurity strategy. The workshop should be help answer questions on how countries can develop and revise their National Cybersecurity Strategy and get a clear understanding on the entire process accompanying the drafting of the strategy.

Milan Sekuloski, Senior Adviser of Geneva Centre for Security Sector Governance, DCAF

On behalf of DCAF, Mr. Milan Sekuloski expressed satisfaction with DCAF's diverse and ever developing cooperation with the Government of North Macedonia, as well as ongoing fruitful cooperation with the ITU. He thanked representatives from all western Balkans economies that have accepted the joint invitation and are actively participating today. Mr Sekuloski explained that DCAF's support for this event is provided within the scope of the project titled 'Enhancing Cybersecurity Governance in the Western Balkans' funded by the UK's Foreign and Commonwealth Office.

DCAF is dedicated to making states and people safer, within the framework of democratic governance, the rule of law and respect for human rights with focus on security sector stakeholders and policies. Due to the importance of digital networks and supporting infrastructures used for the continued functioning of a state, the policies and strategies being developed to protect them are interconnected –either implicitly or explicitly –with national security strategies. DCAF's approach to cybersecurity focuses on supporting good governance initiatives.

Mr. Sekuloski acknowledged that although cybersecurity governance is a fairly new concept, public administration reforms, particularly those reforms related to introduction of strategic management, offer a lot of valuable lessons and experiences that can be used when devising and implementing efficient cybersecurity strategies. He noted that even the EU accession negotiation process itself, may be observed as a strategic management process, with a set of long and short-term goals, performance indicators, key players and resources.

DCAF has worked extensively with various government on introducing strategic management in the security sector: be it national security or sectoral strategies, and has always noted the positive impact strategic management processes had on furthering governance reforms. Mr Sekuloski stressed that he believes that this region has already accumulated significant good and bad strategic management lessons that can undoubtedly be used for the development and implementation of effective cybersecurity strategies. The NCS guide is a valuable tool that help implement those lessons as well as globally acknowledged good practices. In conclusion, Mr. Sekuloski expressed the belief that the workshop will help all the participants in reflecting on their respective experiences and drawing valuable lessons for themselves and others.

5. INTRODUCTORY SESSION

Mr. Orhan Osmani, ITU Cybersecurity Coordinator, outlined the objectives of the event and introducted the NCS guide. He shared a quote from Bruce Schneier that indicates "cybersecurity is a journey, not as a destination."

The introduction emphasized that though cybersecurity may have various definition, the key message is for countries to build confidence and trust in the use of ICTs. ITU's current focus is to help countries to build capacity to tackle challenges faced, and the countries that attended the event acknowledged the importance of having the term cybersecurity defined and harmonized, taking into consideration international standards. Mr. Milan Sekuloski highlighted that sometimes the complexity of a language barrier hinders the establishment of a harmonized the definition on cybersecurity. Furthermore, during the presentation, Mr. Osmani highlighted the global challenges encountered while implementing, monitoring, and evaluating National Cybersecurity Strategies.

It was also, highlighted the need to measure the commitment on cybersecurity, enforce and implement specific processes for the NCS implementation to be effective. These processes include active public awareness, the addition of cybersecurity in primary, secondary, and higher-level educational curricula to develop a cybersecurity culture on the national level. He also mentioned that National Cybersecurity Strategy' priorities should vary from economy to economy, depending on the specific needs, the culture, and the status of ICTs.

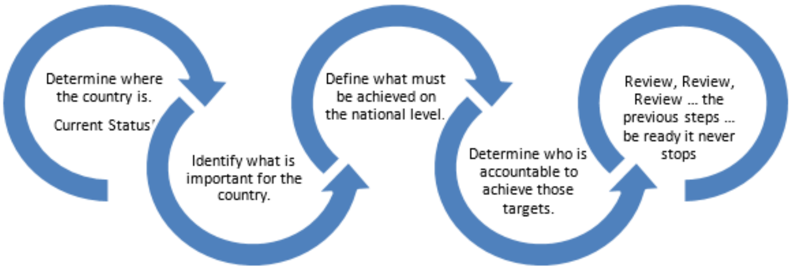

Determine where the country is.
Current Status'
Identify what is important for the country.
Define what must be achieved on the national level.
Determine who is accountable to achieve those targets.
Review, Review, Review ... the previous steps ... be ready it never stops

Figure 2: Key steps in strategy building

For an NCS to be successful, certain factors should be present at all stages. A reliable, transparent, and comprehensive communication among stakeholders involved allows the creation of innovative and creative ways of thinking about the strategy and the future of ICTs development. Moreover, it is essential to take into consideration the local culture and mentalities of the population to be able to raise awareness and develop a clear strategy that includes management of the NCS lifecycle. Based on the several documents referenced by the NCS guide, foreseen challenges within the implementation of a National Cybersecurity Strategy, were highlighted including the ability to:

- State the goals, objectives, and baselines based on risk assessment
- Develop, implement and monitor a clear action plan based on the human and financial resources
- Define the roles and responsibilities, share them through the stakeholders' specific field and enhance coordination and cooperation at the international and national level
- Harmonize the approach between all the countries

Based on an assessment of several National Cybersecurity Strategies of Western Balkan countries conducted by DCAF and ITU, it was noted that some of the Western Balkans economies need to address the following areas for improvement during the development or review of their National Cybersecurity Strategies

- Inclusiveness that is cooperation amongst public and private sectors, academia and civil society, tends to be unclear in most of the revised strategies
- Human rights are not one of the priorities of more than half of the countries reviewed
- Risk management is often missing while developing or revising a strategy

Participants were asked to keep an open mind since the workshop activities are not meant to teach the participants in a restrictive and unique way to draft national cybersecurity strategies but rather provide an understanding and introduce a process as well as concepts to consider during such a process.

6. Setting the Context – Background Papers

In preparation of the workshop, DCAF drafted background papers on each of the normative and strategic frameworks of the Western Balkan economies. As comparative studies based on the ITU Guide to developing National Cybersecurity Strategies, the background papers inspected which of the outlined elements in terms of overarching principles and good practice found in the guide were also transcribed into the existing strategic frameworks in the Western Balkans. By analysing the legislative, strategic and institutional framework(s), DCAF presented a breakdown of adoption of the mentioned overarching principles, namely references to vision, comprehensive approach and tailored priorities, inclusiveness, economic and social prosperity, fundamental human rights, clear leadership, role and resource allocation, the process of drafting the strategic documents as well as existence or aim of establishing a trust environment.

Presenting an overview of the background papers on behalf of DCAF, Ms. Irina Rizmal divided existing approaches into *common*, consisting of principles shared among all Western Balkan economies; *partial*, consisting of principles found in the majority of the document analysed but not all; *individual*, consisting of principles adopted only by a number of strategic documents; and *unique*, as those that are referred to in a number of documents, but from very specific, differing angles.

In terms of common principles, there is expression of a clear vision within the majority of cybersecurity strategies analysed. Even within those that do not explicitly state a clear vision, clear references are made to guiding principles found within the EU NIS Directive[1] and the NATO Cyber Defence Pledge[2]. In general, proclaimed visions span from national security priorities, through capacities, to human rights, public-private partnerships and international cooperation. Additionally, all documents list between five and seven strategic priorities, including generally references to institutional and capacity development, CIIP and risk management as well as awareness raising and partnerships (both public-private and international). Finally, all Western Balkan economies have different sets of policy frameworks in place in addition to cybersecurity legislation and/or strategies. These include existence of Penal Codes that consider cybersecurity notions too, legislation regulating matters pertaining to cybercrime, classified data and privacy, electronic communications, signatures and trade, as well as specific legislative instruments such as Methodologies for CII identification, for example.

[1] 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. *OJ L 194, 19.7.2016*.

[2] Cyber Defence Pledge. 2016. *NATO Press Release (2016) 124*. Available at: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Partially adopted overarching principles contain inclusiveness and references to fundamental human rights. While some of the documents refer to the comprehensive and/or multi-stakeholder working groups that were tasked with developing drafts of the strategic documents, including non-state actors as well as international partners, others have been developed solely by state actors. What is also common is that even in the case where the strategy explicitly states that non-state actors have been included in the drafting process, further elaboration on the type, or the specific actors involved, is still missing. The situation also varies when it comes to referencing fundamental human rights. While some strategies make explicit reference to the broad spectrum of human rights and liberties, listing, among other, freedom of speech and expression, privacy, etc. others either lack any mention of these principles, or focus solely on specific ones, such as privacy for example.

In terms of individual principles, found only in few of the strategies analysed, economic and social prosperity are included whereby the need for a safe digital space for ensuring investments is recognised, but a vision of cybersecurity as a potential driving force for economic and social development is missing. Similarly, references to risk management and resilience are also limited and explicitly mentioned only in a few documents.

Finally, in terms of unique approaches, as points for discussion, Ms Rizmal highlighted the notion of resource allocation and trust environment. Namely, although all the documents analysed provide an outline of cybersecurity governance structure, therefore determining the competent institutions and their specific roles, challenges arise when it comes to resource allocation. Provisional resource allocation, as inspected within respective action plans for strategy implementation generally either fail to provide clear indications on the scope of resources needed for specific action implementation, or rely on various donations, projects and external support for implementation. Although obtaining additional resources from external sources is a completely legitimate and practised method of capacity and capability building, leaving the majority of activities dependant on external funding makes the potential for actual implementation questionable and respective action plans possibly ineffective.

The final element of overarching principles discussed by Ms Rizmal is that of a trust environment. Although mentioned by most of the strategic documents, the lens through which this notion is seen significantly varies. Trust environments are seen in the form of establishing citizen trust in government electronic services, trust between partners from both the public and private sector, as well as investment trust in the business climate and potential of the analysed economies. This means that although the principle of trust is there, it is employed differently within the different national contexts. This variation ranges from trust as a tool for ensuring citizens use of government e-services, as a goal in terms of establishing close ties between public and private actors working in the field of cybersecurity, or even as a risk in terms of dissuading potential investors from engaging with the economy at hand, jeopardising therefore economic and social development.

Ms. Rizmal concluded that all Western Balkan economies have certain legislative and strategic frameworks in place or are in the process of developing them. With most of the presented overarching principles adopted within these frameworks, the workshop is to serve as a forum for exchange of experience and practice resulting in discussions on how to develop and/or revise existing frameworks to achieve greater effectiveness in national cybersecurity.

7. Assessment session - Lifecycle of National Cybersecurity Strategy

This session was moderated by Mr. Marco Obiso who introduced the guide for developing a National Cybersecurity Strategy, used as a basic tool for the workshop. The guide has three separate sections that should be read from different perspectives. The first section is called the lifecycle, the second regards the guiding principles that should be followed in all lifecycle including the drafting, and the third is the section that presents the best practices, implementation and monitoring phases.

This session has been dedicated to the first section of the guide, the lifecycle phases through which a country should undertake when developing and revising a National Cybersecurity Strategy.

7.1 Phase 1: Initiation phase

Initiation phase describes the pre-requirement needed before developing a strategy. First, a ***Lead Project Authority*** should be established to lead the development of the Strategy. This could be a pre-existing or newly created public entity, such as law enforcement body, specific ministry or department. This lead project authority should be multi-sectoral and crosscutting. Then, a ***Steering Committee***, a structure overseeing the project, should be identified. It may occur that the Lead Project Authority, in charge of the implementation, and the Steering Committee, in charge of the governance, is the same institution. If organised as such, it is advised to clearly define their roles within the institution. During this phase, ***the stakeholders involved in the project and their roles during the entire process are clarified***. As one of the key steps when developing a strategy, mapping all relevant stakeholders will facilitate the quality of the strategy.

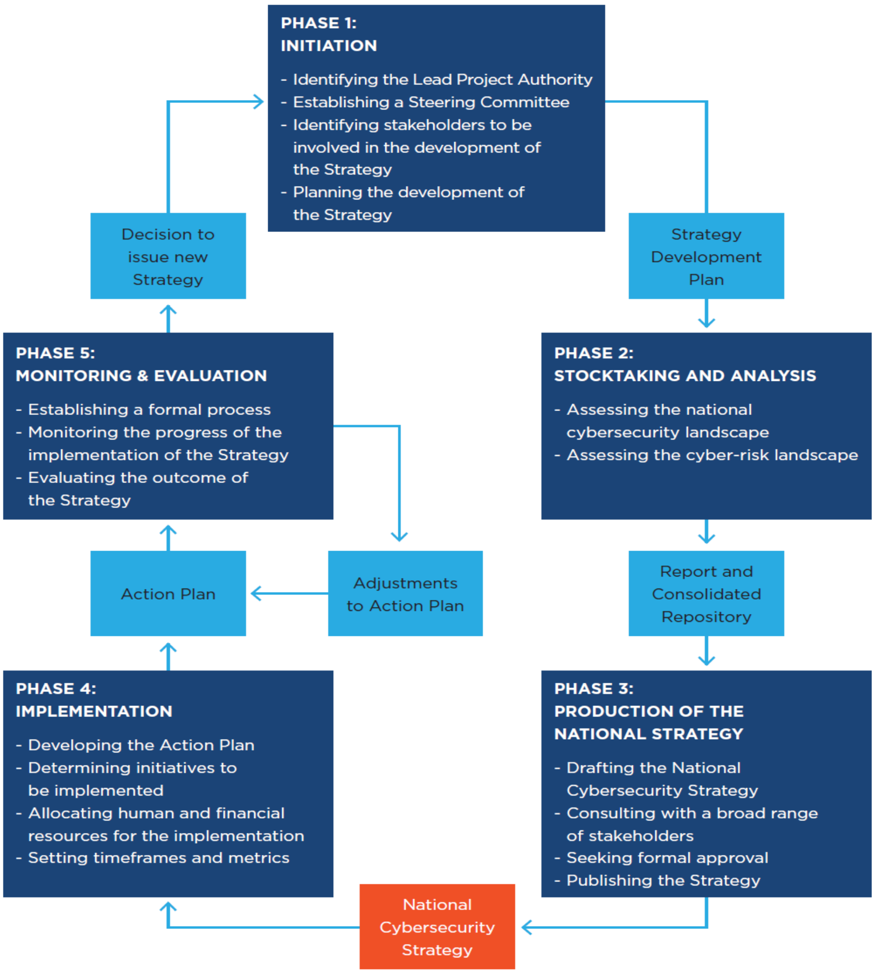

PHASE 1:
INITIATION
- Identifying the Lead Project Authority
- Establishing a Steering Committee
- Identifying stakeholders to be involved in the development of the Strategy
- Planning the development of the Strategy
Strategy Development Plan
PHASE 2:
STOCKTAKING AND ANALYSIS
- Assessing the national cybersecurity landscape
- Assessing the cyber-risk landscape
Report and Consolidated Repository
PHASE 3:
PRODUCTION OF THE NATIONAL STRATEGY
- Drafting the National Cybersecurity Strategy
- Consulting with a broad range of stakeholders
- Seeking formal approval
- Publishing the Strategy
National Cybersecurity Strategy
PHASE 4:
IMPLEMENTATION
- Developing the Action Plan
- Determining initiatives to be implemented
- Allocating human and financial resources for the implementation
- Setting timeframes and metrics
Action Plan
Adjustments to Action Plan
PHASE 5:
MONITORING & EVALUATION
- Establishing a formal process
- Monitoring the progress of the implementation of the Strategy
- Evaluating the outcome of the Strategy
Decision to issue new Strategy

Figure 3: NCS Lifecycle

Analysis

For most of the Western Balkan's economies, a steering committee has already been identified. Their role is to oversee the development of the strategy, its implementation and revision. Most lead project authorities are ministries and private institutions have not been involved in the steering committee. Usually, academia and private sector get involved to comment once the draft strategy is developed. Not all economies have both a steering committee and a lead project authority. For some, working groups have replaced the steering committee where international organisation and national institutions from various field such as law enforcement, prosecutions, government and industry, have been included. The involvement of the international community brings a high value to an economy's knowledge. However, an international organisation should not be considered as a relevant stakeholder during **all** the lifecycle of the strategy. Indeed, before developing a National Cybersecurity Strategy, it is necessary to understand what has been done worldwide and be aware of international standards and best practices. This investigation should be made during the stocktaking and analysis phase and during each revision process. However, a NCS is a national project and should be developed accordingly to the specific needs of the economy, with regards to aspects including their cybersecurity culture, the state of ICT industry, cybersecurity curricula's, ICT and IoT presence and use. The international organisation can be involved for advising and contributing to the overall process, but the lead project authority should be a state stakeholder. There is need for an umbrella that would lead the National Cybersecurity Strategy and coordinate the process with all the stakeholders involved. The Swedish model and their way of handling cybersecurity, which is decentralized and where each institution has specific roles and shared responsibilities has been presented as a best practice.

7.2 Phase 2: Stocktaking and analysis phase

This phase is mainly dedicated to the economy's analysis. The objective is to understand and have a deep knowledge of the past, actual and future cybersecurity situation as well as to evaluate the cybersecurity landscape in the economy. Stocktaking is fundamental before drafting the strategy, even if it might not be seen as a priority. It is imperative to collect data to ***understand the cybersecurity status*** of the economy and the global situation while assessing the cyber-risks landscape. In the past, cybersecurity actions were developed with the objective of finding solutions for preparedness and to fight threats. Today, cybersecurity development should be considered according to the ***risk*** being managed. Economies need to find the right balance between the likelihood and impact of a threat which is measured by the risk level. For instance, investing resources on protecting an economy with an averagely developed secured digital infrastructure against highly complex and rare malware is not worthwhile if the government has not invested in raising awareness and providing training in society against social engineering cybercrime.

Analysis

With regards to risk aspect, a lack of legal and regulatory framework was highlighted, in particular regarding the Critical Information Infrastructure. Within governments, several distinct cybersecurity strategies are developed in some economies. An NCS does not have to be the only policy regarding the field of cybersecurity. In strong economies, the private sector develops sectoral cybersecurity strategies to protect against cyber risks. However, when various cybersecurity strategies exist, they should be developed in line with national guidelines in order to avoid conflicting guidelines. As such, having an overall National Cybersecurity Strategy considered as the umbrella would harmonise the economy's strategies.

It was noted that most of economies do not include the Ministry of Foreign Affairs (MFA) in the development of their NCS. Even if not directly involved in cybersecurity, MFA are key stakeholders. Cybercrime does not impact only the national level, but crosses borders as well. Cyber incidents can have an effect on state relations not solely in instances of crime but also suspected state-sponsored cyber-attacks or cyber espionage. This is why cyber diplomacy is becoming significant in MFAs across Europe and wider. While the entire process should be led at the national level, involving international stakeholders and building the basis according to the international context and recommendations is highly advised.

Oxford's representative, Mr. Andraz Kastelic**,** added that the Global Cybersecurity Index 2018 (GCI) as well as the Cybersecurity Capacity Maturity Model for Nations' (CMM), assessments can help better understand the state of cybersecurity in economies in this phase of NCS development lifecycle.

7.3 Phase 3: Production of the National Cybersecurity Strategy

During this phase, economies are drafting their strategies according to previous phases' results. As noted several times, drafting the strategy is not always seen as an important priority step. It happens that elements not directly included in the draft, even if planned during the previous phases, may not be picked up during the implementation phase. Also, the written document is highly important as it allows society to understand what the government is focusing on in the field of cybersecurity in a transparent and assuring manner. Once the draft is complete, it should go through approval and comments from all the relevant stakeholders selected during the first phase. Usually, this step is done through an online public consultation. Comments received from civil society, academia, and public as well as the private sector shall then be taken into account, and the draft should be reviewed. Subsequently, a final NCS document seeking formal approval has to be given by the highest level of government and the final strategy should be published online and be accessible to everyone.

Analysis

Most of the economies already have a strategy in place, but not necessarily publicised and not having undergone public consultation. Few are already working or soon to commence work on a revised (second version) of their strategy. As all government decisions go through a public consultation, it should also be the case for the NCS. Ministries, Telecommunications operators and services, secret services and all governmental institutions have a role to play. In some economies, it is noted that under the umbrella of Government, a working group is created which includes academic and private sectors, and is tasked to review the National Cybersecurity Strategy draft and give inputs. The general process to publish the NCS is as follows: After drafting the strategy, the working group goes through an expert review. Then, the competent ministry approves the comments (through a council session) and a public consultation is set up after which the government gives the final approval. Some countries even publish the reviewed document along with the National Cybersecurity Strategy. It is important that the experts involved in the review of the document have the appropriate skills and roles defined. The main objective of a public consultation is to open the document for comments and inclusion of stakeholders' views, the value is gained when the government considers comments received and adapt its strategy accordingly.

7.4 Phase 4: Implementation: Define the Action Plan and implement it

This session underlined that more than 50-60% of the action plans are considered as a draft and the objectives cannot be attained. For an action plan to be efficient, the objectives of each action need to be thought and selected in line with the available human and financial resources. Sometimes this phase becomes controversial as economies have ambitious objectives but resources are missing. In some cases, the actions may not be clear enough and attribution for implementation may involve several stakeholders with diluted accountability and lack of coordination.

ITU shared their point of view on the importance of having an **implementable impactful action plan**. While it may not be possible to share financial/human resources allocations and certain sensitive actions in a public document, such sections may be omitted in a version shared with the population. It was noted that the publicly available United Kingdom National Cybersecurity Strategy has included resources allocation.

Analysis

More than half of the Western Balkans countries have NCS related action plans. The main issues mentioned are the lack of resources to implement those actions and the inappropriate allocation of resources needed, because the existing Action Plans list projects as 'funded' for a significant number of activities. Issues not always appear from a lack of resources, but often they fail at allocating and securing them.

7.5 Phase 5: Monitoring and evaluation

Analysis

Implementation phase and monitoring are understood and considered by economies. For most of them, the implementation is expected to be governed by legislation aligned with cybersecurity law. It may happen that due to a lack of trust from the society, implementation is slowed down and takes more time than expected. Thus a trustful environment is highly important.

7.6 Session Conclusion

The lead project authority, the Steering Committee and all stakeholders should carefully abide to their roles and responsibilities. There should be an attention to involve MFA as activities in cyberspace are not border limited and clear-cut, and in addition to protect the economy against external threats and risks and vice versa. In addition, the international community should not be considered as a relevant stakeholder during the entire lifecycle. In case the Lead Project Authority and the Steering Committee are the same institution, an attention should be put on clearly defining roles within the institution.

In the second phase, a deep analysis on the economy's current situation in relation to cybersecurity and a stocktaking phase that will allow gathering the appropriate experts and stakeholder's needs must be conducted to understand what will be the actionable objectives that the economy can deploy before producing the strategy.

During the production of the strategy, there is a special need to correctly conduct the online public consultation and the following steps such as taking into account the outsiders' comments (public/private institutions, academia, society etc.) and review the draft strategy accordingly. In addition, NCS must reflect the political, social and economic posture of the economy assessed during the second phase. The mismatch and lack of human and financial resources will always impede on effective implementation of the NCS action plan. It is imperative to identify synergies with existing actions and the ones proposed in the NCS action plan to optimise the use of resources.

8. HANDS-ON EXERCISE: ESTABLISH A GOVERNANCE STRUCTURE TO DEVELOP & MAINTAIN THE NCS

Participants put into three teams and asked to answer a series of questions as detailed below.

Q1: Identify the main constructs/structures/mechanisms that you consider indispensable for an effective production/ revision of a strategy

One of the main constraints that should be raised is to provide ***more public awareness*** in cybersecurity. Also, ***one authority*** should coordinate the tasks and oversee the work of all other institutions involved. To produce an effective National Cybersecurity Strategy, all relevant stakeholders should be included i n the process with the creation of ***a working group of all relevant stakeholders***. This would include individual partners such as the law enforcement authority, the military and the judiciary, the latter being a key partner for the development of a legal framework. This working group should advance the discussions on how the strategy should be structured and have some ***round table discussions***. The majority of the participants agreed that a working group is a key element in the production and revision of the strategy. However, the government should lead the project. In the literature, some economies have a Cyber defence strategy for law enforcement and military, separate from a National Cybersecurity Strategy.

Q2: Lead Project Authority: List the entities that you consider necessary to be part of it

The Steering Committee should include several entities such as ***ministries***, especially MFA, the ***military***, ***the private sector, academia, telecommunications industry players including ISP providers***. But the highest level of government, the lead project authority should be coordinating with all those stakeholders. While all aforementioned stakeholders should indeed be involved in the process, their role and responsibilities, need to be clearly defined and communicated.

Q3: Stocktaking and analysis: Provide the main aspects that must be taken into account for the production / revision of a NCS.

For an effective National Cybersecurity Strategy, the assessment should include the analysis of the global situation of the economy. The following focus areas and topics should be approached. First, the strategy should address the Critical Information Infrastructure's protection. The existing policies should be known and a revision should be planned every 1 or 2 years. An action plan is important, but as mentioned by the ITU team, it needs to be realistic. In that sense, it should be actionable without being too optimistic. During the assessment phases, several frameworks should be analysed, in particular the existing legal and regulatory framework. A cybersecurity maturity assessment, the existing national and international standards, the telecommunication situation and position in the economy, the educational opportunities in ICTs can be highly valuable to understand the needs and the cybersecurity level of the country. Finally, all national initiatives not driven by the government are valuable when drafting the strategy. For example, to be aware if there is any academia and/or business existing initiatives, regulations, policies, strategies, standards. In other words, a local market analysis should be done.

Q4: Production phase: Provide a short visual on how you envisage the relationship and interaction with relevant stakeholders (private sector, civil society, academia among others) during the production and revision phase.

The relationship and interaction between the stakeholders will take many and various forms. Notably, the academic sector would bring theories for new approaches and private sector new IT solutions. The leading authority should organize round table discussions either separately (various small groups) or one general group that would then be divided in several working groups. After the roundtable discussions, a first document should be drafted and shared for remarks and recommendations with all stakeholders and international partners.

Analysis

Awareness of the available resources is extremely important. It was stressed that an action plan must contain clear objectives, in which the needed financial and human resources are carefully considered and clearly defined. It is important to clearly define who is monitoring and who is operationalising.

9. Hands-on exercise: NCS implementation & Establishment of an action plan

The NCS lifecycle is made of different steps, among which the Implementation phase is of particular relevance. In fact, a structured approach to implementation, supported by adequate human and financial resources, is critical to the success of a strategy and needs to be considered as part of its development. The implementation cannot be the sole responsibility of a single authority. It requires engagement and coordination of a range of different stakeholders across the government, as well as support from civil society and the private sector.

The implementation phase is usually underpinned by an action plan, which comprises a set of actions which are initiatives to be implemented in order to reach the goals of the strategy. The drafting of an action plan should serve as a mechanism to bring the relevant stakeholders together to agree on objectives and outcomes, as well as to coordinate efforts and pool resources.

The exercise aims at practising the implementation capacity of the participants related to a National Cybersecurity Strategy. During the exercise, participants were divided in three groups and asked to work on two action items – active defence and protecting Government- by relying on an NCS. They were provided with a National Cybersecurity Strategy and a short description of the action item with relative objectives, and were asked to elaborate on the following:

- Approach/Implementation lines
- Responsibilities
- Performance Indicators

Once the Action Items had been drawn up, each group was asked to present its outcomes followed by a roundtable discussion.

	GROUP 1	***GROUP 2***	***GROUP 3***
Brief Description	Principle of implementing security measures to strengthen a network or system to make it more robust against attack		
Objectives	• Make the country a much harder target • Defeat the vast majority of high-volume/low-sophistication malware activity • Evolve and increase the scope and scale of Government's capabilities to disrupt serious state sponsored and cyber-criminal threats • Secure internet and telecommunications traffic • Harden the critical infrastructure and citizen-facing services against cyber threats; • Disrupt the business model of attackers of every type		
Approach/ Implementation lines	• Development of laws on cybersecurity and Critical Infrastructure • Promote Capacity Building in Risk Management • Establishment of sectoral CERTs and collaboration with Government CERT • Establish Academic Program on Cybersecurity • Conduct awareness campaigns	• Cooperation among Private and Public sector (including Internet Service Providers) • Investments in Government sector and Critical Infrastructure • Implementation of security mechanism • Increase education and Training • Conduct awareness campaigns	• Increase cybersecurity in all pillars • Implementation of National CERTs/Governmental CERT • Increase general capabilities • Establish cybersecurity centres • Monitor National traffic

			• Develop standards on Critical Infrastructures
Responsibilities	National Cybersecurity Centre	• National Cybersecurity Centre • Intelligence • Academia • Ministry of Defence	• Government • Citizens
Performance Indicators	• Decrease of malware	• Increase of Memorandum of Understanding (MOU) • Increase of the budget devolved • Increase of percentage of malware blocked • Less Internet traffic vulnerabilities • Increase of skills and capabilities	• Capability Maturity Model • Global Cybersecurity Index

Figure 4: Exercise result on Active Defence action item

Active Cyber Defence (ACD) is the principle of implementing security measures to strengthen a network or system to make it more robust against attack. In a commercial context, Active Cyber Defence normally refers to cybersecurity analysts developing an understanding of the threats to their networks, and then devising and implementing measures to proactively combat, or defend, against those threats. In the context of this strategy, the Government has chosen to apply the same principle on a larger scale: the Government will use its unique expertise, capabilities and influence to bring about a step-change in national cybersecurity to respond to cyber threats. The 'network' we are attempting to defend is the entire country cyberspace.

The activities proposed represent a defensive action plan to respond to cyber threats at a macro level. If we compare the three approaches adopted by the groups, it is clear that there are numerous traits in common and some differences. In general, all approaches focus on the protection of critical assets and governmental structures. Private public partnerships are encouraged, both at high level and at the level of cooperation between CERTs. The participants recognized also the need to structure education and training programs on the topic, by involving also the Academia.

Other possible approaches could leverage on the need to put controls in place in order to secure the routing of internet traffic, and to set standards for example on the email verification system. The standards should develop in the public sector and then be translated into the industry context. Moreover, the promotion of security best practices and the establishment of control systems could play a fundamental role in increasing the general awareness and securing internet and telecommunications traffic. Furthermore, in order to protect citizens from being targeted in cyber-attacks, the law enforcement channels could also be actively involved.

	GROUP 1	***GROUP 2***	***GROUP 3***
Brief Description	The Government's systems underpin the functioning of our society. The modernisation of public sector services will continue to be the cornerstone of the country's Digital Strategy. To retain the trust of citizens in online public sector services and systems, data held by government must be protected and all branches of government must implement appropriate levels of cyber security		
Objectives	• Citizens use government online services with confidence: they trust that their sensitive information is safe and, in turn, understand their responsibility to submit their sensitive information online in a secure manner; • The Government will set and adhere to the most appropriate cyber security standards, to ensure that all branches of government understand and meet their obligations to secure their networks, data and services • The Government's critical assets, induding those at the highest classification, are protected from cyber attacks		
Approach/ Implementation lines	• Harmonize and implement international and regional policies in trust services • Establish frameworks and policies to secure Networks, data and services • Create secure Networks for Institutions with Critical Assets	• Baseline of security measures • Auditing • Training & education for Institutions • Identify Critical Information Infrastructures (CII) • Development CII protection plan with criticality levels • Auditing and simplification for ensuring compliance with protection plan	• Setting of standards • Cooperation between Private sector and Government • Expanding Intelligence • CERTs, CII, NCS, CPNI • Raising awareness in all the society
Responsibilities	• National Cybersecurity Centre • Governmental CERT	• National Cybersecurity Center • Institution • Academia	• Cybersecurity Authority • Other entities (MoD, MoE, Government)
Performance Indicators	• Implementation of Regulations and policies • Creation of secure networks	• Reduction of the number of incidents • Reduction of time of unavailability of essential services • Reduction of the number of compliance issues reported	• Increase in the number of services offered • Implementation of standards • Number of awareness campaigns

Figure 5: Exercise results on Protecting Government action item

Usually Governments, devolved Administrations and the wider public sector hold large quantities of sensitive data. They deliver essential services to the public and operate networks that are critical to national security and resilience. The Government's systems underpin the functioning of our society. The modernisation of public sector services rely more and more on digital systems and ICTs. To retain the trust of citizens in online public sector services and systems, data held by government must be protected and all branches of government must implement appropriate levels of cyber security in the face of continuous attempts by hostile actors to gain access to government and public sector networks and data.

All the three approaches put emphasis on the need to develop and implement specific policies, standards and security measures for the public sector. Moreover, since Governments usually deal with very sensitive communications, the three groups recognized the importance of creating secure networks at Governmental levels (Institutions, CERTs, Ministries, Agencies, etc.). In fact, in order to be protected from cyberattacks, Governments' networks should be highly complex and in many cases should incorporate legacy systems, as well as some commercially available software, which is no longer supported by the vendor. Moreover, highest classification networks should be improved in order to better protect classified information. The overall Public Sector should improve its cyber resilience and aim at becoming not only "Digital by default", but especially "Secure by default". To reach this objective, it is fundamental to increase awareness in government workers at all levels and to frame clear cybersecurity risk management processes. Moreover, establishing programmes of incident exercises and regular testing could help to increase the overall response capacity.

It is important to stress that there is no right approach with regards to drafting an Action Plan or more specifically in identifying Action Items. The Action Plan, developed in accordance with the principle of clear leadership, roles and resource allocation should support the effective implementation of the Strategy. Its development is almost as important as the Plan itself. The process should serve as a mechanism to bring the relevant stakeholders together to agree on objectives and outcomes, as well as coordinate efforts and pool resources.

The National Cybersecurity Strategy highlights the government's objectives and the outcomes they wish to realise across the different focus areas identified. In the Action Plan, the specific initiatives within each focus area that will help meet those objectives have to be identified. Examples could include organising cybersecurity exercises establishing security baselines for critical infrastructures, or setting an incident reporting framework, amongst others. The timeline and effort needed for the implementation of these initiatives should be prioritised in accordance with their criticality to ensure that limited resources are appropriately leveraged.

10. HANDS-ON EXERCISE: HOW TO MONITOR IMPLEMENTATION, UNDERSTANDING GAPS AND APPLY CORRECTIVE MEASURES

With regard to the previous assessment session, participants were divided into three working groups and asked to answer a series of questions, focusing on the role and capacity of competent authorities in monitoring the implementation of the National Cybersecurity Strategy (NCSS). The working groups were tasked to try applying the Plan-Do-Check-Act (PDCA) model on the national strategy implementation monitoring process. These included questions including:

Plan: Does the strategy or action plan make it clear which institution/entity is in charge for monitoring the strategy implementation? If yes, who is it? Does the institution/entity have the legal authority to request information and propose actions related to strategy implementation? Is it based on law, sub-law, government's decision or mix/something else? To what extent is the legal mandate applicable to the private sector? Does it have monitoring procedures? Are these written down? Where? Are there some good practices that may complement or even compensate for the lack of legally prescribed authority? Are there some bad practices that may hamper the strategy implementation? Could they be mitigated? How? Does the institution/entity which oversees monitoring have the allocated resources to engage in monitoring? Enough competent personnel for monitoring activities? Is there a budget for monitoring activities? How much autonomy does the monitoring institution/entity have in devising and executing its budget? Is there training for monitoring and evaluation training available to the staff of the institution/entity?

Do: What monitoring practices are there when it comes to the monitoring of the implementation of the cybersecurity strategy? Is there a reporting mechanism set up for strategy implementation monitoring with clear timeframes, levels of hierarchy and obligations (& possible sanctions?)? For the overall strategy implementation? Per some specific stakeholders and processes? Which ones (please list them)

Check: Does the cybersecurity strategy or the action plan have clearly defined success indicators? Are the indicators/to what extent/ SMART (Specific, Measurable, Actionable, Realistic, Timed)? What are the key challenges in making the indicators more relevant and useful?

Act: Are implementation monitoring reports being made for the cybersecurity strategy? Do these reports also contain recommendations, along with an overview of the implementation process? Are the monitoring reports followed up? If yes, by whom? Is some type of a mid-term review and adaptation of the Strategy/Action Plan envisaged? If not, should there be one? How would it be best set-up? If yes, at what stage of strategy implementation?

The group discussions, moderated by Mr. Milan Sekuloski resulted in the following joint conclusions:

There are competent institutions defined in all economies. One of the main issues raised by the group regards the legal framework, for instance, **limited legal mandates** when it comes to private sector. For that, Cybersecurity laws has been proposed as possible tools to strengthen the legal mandates. Also, Periodical monitoring procedures has been defined and agreed as a necessary process. However, the competent institutions rarely have a specific person, department/division overseeing Monitoring and Evaluation. Indeed, greater capacities and resources dedicated to Monitoring and Evaluation are needed. As part of monitoring and evaluation, an **annual Action Plan** has been defined as enabling quicker adaptation of strategy implementation as it offers regular reviews. From the multi-stakeholders approach, role of international partners as external actors is seen as potential generators of pressure for implementation. With all the economies involved aiming for EU and/or NATO memberships, international partners pose as an oversight mechanism on developments in the field, setting standards for those who want to join the club. Additionally, in economies where political will is weaker than needed for developing comprehensive national cybersecurity mechanisms, interest of international partners in the subject matter may provide an additional soft push for greater focus on the side of policymakers. However, indicators need to be discussed among all relevant stakeholders in multi/cross-sector forums (tech and policy) in order to standardise language and ensure lines of action are plausible and understandable for all the stakeholders involved. This to be done together with external actors in order to have an outside view (e.g. international partners can foster the development of SMART indicators).

11.ASSESSMENT SESSION – OVERARCHING PRINCIPLES

For this session, some of the guiding principles that are commonly used while developing a NCS were presented. These principles can be seen as the umbrella that accompanies the whole process, as there is no unique way of including them in the process. Sometimes those principles are described as separate paragraphs in the text and sometimes they are implicitly present in the way the overall strategy is drafted. The NCS guide presents nine principles. On the other hand, not all of them appear in each economies. The principles should be chosen depending on how the economy is positioning itself, its status and cybersecurity situation and culture. The principles presented here are:

Vision is a presentation of the priorities and orientation of the whole society. The vision is recommended to be clearly written in the strategy as it gives the reader an understanding of the overall situation and priorities of the country such as **what is at stake and why the Strategy is needed** (context), **what it is to be accomplished** (objectives), as well as what it is about and **who it impacts** (scope). Not having a vision risks to convey the wrong message.

Comprehensive approach and tailored priorities: This principle presents an overall cyber posture of the economy. This should result of a previous country's specific context analysis. This analysis should help detailing economies' priorities and how they interrelate, potentially complementing or competing with each other, in line with the objectives, the implementation timeline and the resources available.

Inclusiveness can be understood as twofold; first on the fact an economy should include relevant stakeholders for ***building*** the strategy. However, including other stakeholders does not mean that government shares the control. On the contrary, dedicating work to specialised stakeholders shows a clever control. A government that involves specialists bringing resources and knowledge conveys an inclusive and efficient way of governance. The other aspect of inclusiveness is to not consider the objectives of the strategy to be only dedicated to a specific sector or population (e.g. public sector or academia). The strategy should be ***dedicated to the overall population***, taking into account the protection of the youth, the elderly, the children, workers, non-workers, persons with disabilities, etc. To sum up, it should be at the service for the whole population.

Enhancing **Economic and Social Prosperity** and considering the country's broader socio-economic objectives should be one of the principle the Strategy should be aligned with.

Fundamental human rights: ITU, being a UN organisation, is presenting this principle from UN perspective. And from where ITU stands, fundamental human rights should be thought as a priority in the development of the strategy and should recognize that the population have rights. It means that the cybersecurity should also protect people from their rights online such as data protection, privacy of communication, avoiding practice of unlawful surveillance, interception of communications or practice of arbitrary.

Risk management and resilience: the Strategy should encourage the all public and private institutions, especially ICT Industry, to prioritise their cybersecurity investments and to proactively manage risks, understand the needs and the risk probabilities. Focusing on risk management and encouraging recovery plans and business-continuity measures would enhance stakeholders' resiliency.

By possessing the **appropriate set of policy instrument**, a strategy should possess the appropriate framework (legal and regulatory). This should be the basis on which the strategy will take its foundations. For instance, having a cybercrime law on which the basis of the strategy could take the starting point. However, it should also be the endpoint, meaning that the law should be revised according the strategy and it should help understand what needs to be regulated or not. Some economies might think that too much regulation can affect efficiency, and rightly so. Indeed, there needs to be a balance between soft regulation (OFCOM) and strong regulation.

Clear leadership and resources allocation: In this principle, the Lead Project Authority and the stakeholders involved should think on clearly defining their tasks, the timeframe, and the human and financial resources needed to achieve all the objectives.

Trust environment means that, while progressing on the draft and implementation of the strategy, the economy should be aware and make efforts on getting the whole society to secure in their cyberspace. For that, the strategy must enable policies, processes and actions at the national level in order to render secure critical services. E-governance, e-commerce and digital financial transactions are items that can be implemented to get the citizens and corporations' confidence.

Analysis

From the discussions, the following priorities have been highlighted: Some economies mentioned to be inclusive as various stakeholders and the population are involved during all the development of the strategy. Their vision surrounds the idea of having a safe cyberspace for all and their strategies are population oriented (towards the protection of the population, engaged in having a safe and secure cyberspace, highlighting the online human right, etc.). Also, vision has been highlighted as a priority, focusing on the goals to be achieved. Sometimes, focus areas or details about the legal framework and the set of existing policies are briefly defined as part of the vision.

Mr. Adel Abusara of OSCE mission to Serbia highlighted that inclusiveness is promoted and recommended by international organisations. Public-Private Partnerships (PPPs) as an organisational measure must be aligned with a clear leadership, in order to be able to work with a clear assignment of tasks and responsibilities. However, having that principle on the draft strategy is not enough. The question each economy should ask is **"are the principles implemented and reflected by the actions taken?"** Inclusiveness is a principle that cannot be applied in every context; indeed, to implement it, the stakeholders need to trust each other, the public sector should trust private companies and industries and vice versa. Applying the concept of inclusiveness when the relationship is in distrust and the interactions are only agreed upon on surface is not sufficient for developing an efficient cybersecurity strategy. With regard to inclusiveness, the importance of academia has been emphasized. Finally, particular attention was given to how the inclusion of various stakeholders should be built on the long term. In addition, the number of stakeholders does not need to be important to be efficient. The quality of the relationships is more central than the quantity, and it is advised that this number should not be higher than 15-20 institutions to build confidence, trust and a strong community.

12. Hands-on exercise – Overarching principles

In this session, teams were asked to develop two of those nine principles by answering the three following questions:

- ***Context***: Why does my economy need this principle?
- ***Objective***: What is to be accomplished?
- ***Scope***: Who will it impact?

Principle 1 applied: Vision

"Ensuring safe environment of cyberspace by minimising and preventing cyber threats and cooperation with national and international partners."

Why does my economy need a vision?

In an economy's vision, several focus areas can be raised, such as the achievement of stable operations of ICT systems, increase capacities to fight against cybercrime and reduce/prevent cyber threats. A vision can also highlight the priority in cooperation, the laws and policies. When an economy is population-oriented, it can define the priority to ensure a safe cyber space. The vision is an important element to understand the landscape of the economy and understand the whole strategy.

What is to be accomplished in the vision?

In order to achieve stable operations of the ICT system and reduce or prevent threats, the specific objectives could be to protect critical information infrastructure, enhance cyber defence and cybersecurity capacities. When the overall context is about cooperation, the objective could be to engage in cooperation and collaboration between non-governmental organisations, public and private sector as well with other national and international partners. When the vision's priority is population-oriented, the overall objective could be the institutional and capacity building development.

Who the vision will impact?

In general, the vision should impact the whole society, but specific objectives could address specific needs, so target a specific population. In that case, the vision should describe briefly the targeted population such as governmental institutions, citizens, private sector, CSOs, professional associations, international partners.

Principle 2 applied: Human Rights

"We want to ensure protection of basic human rights in balancing security and privacy."

Why does my economy need to integrate the Fundamental Human Rights?

The need to integrate human rights in a National Cybersecurity Strategy must be centred around the economies' core values and basic human rights such as the individual liberties, democracy and the need for a transparent government. In addition, values related to the online environment such as the right to web accessibility for everyone at any time, the protection of personal data and the right to privacy (in line with the European Standards) were raised.

What is to be accomplished in including the Fundamental Human Rights?

The implementation of fundamental human rights while developing the strategy offers a reliable and safe cyberspace for the population, the protection of freedom of expression, and data and information protection. Some elements to be accomplished can be more specific, such as protecting sensitive citizens' data and secure the secrecy, the authenticity, offering a cyberspace that respects privacy rights, or raising awareness on the methods that can be adopted by the industries and citizens to better protect their personal data online and restrain information sharing. In this regard, there is a specific need to assess what is the right balance between being too protective of the population's privacy and the need of security control (such as legal interception of communication or internet access without interference).

Who it will impact to integrate the Fundamental Human Rights?

Protecting human rights is a principle that concerns all society and web users including vulnerable groups such as people with disabilities, youths, children, elderly, workers, non-workers, minorities but also all type of institutions such as public institutions, start-ups, businesses, foundations, etc.

13.HANDS-ON EXERCISE: REFLECTING THE GOOD PRACTICES INTO THE NCS TEXT

The NCS Guide introduces a set of Good Practices to use as a reference for developing an NCS. These Good Practices are grouped into focus areas, such as overarching themes, and have to be tailored to the specific national context by considering a series of factors (including maturity level, geopolitical context). Economies should identify and follow the Good Practices that support their own objectives and priorities in line with the vision defined in their Strategy. The exercise consists in comparing a focus area "Capability and capacity building and awareness raising" of three National Cybersecurity Strategies namely USA, Singapore and UK, in order to identify Good practices and possible areas for improvement. The participants divided into groups undertook the exercise and presented the main outcomes followed by a roundtable discussion. The main discussion elements are presented below:

Singapore Good Practices

Establish a professional workforce: Singapore put efforts on raising awareness and capacity building in the field of Cybersecurity. They have implemented University curriculum, scholarship and sponsorship programmes and defined clear cybersecurity career path. In addition, they offer up-skill and re-skill opportunities and adopted international certification schemes.

Extend Singapore's cybersecurity advantage through strong local companies: Singapore is facilitating the growth of local companies in the field of cybersecurity by attracting and anchoring advanced capabilities, supporting cybersecurity start-ups and developing market opportunities in cybersecurity.

Innovate to accelerate the industry's growth: Singapore, as a well advanced country in cybersecurity invested in the creation of new Research and Development facilities and programmes and in implementing new local partnership between government institutions, academia and industries.

UK Good Practices

Embed cybersecurity programs into the curriculum: United Kingdom has embedded cybersecurity programs into the universities curriculum.

Training professionals in the workforce: The country offers training programs for workforces and established a "skill advisory group" formed of government, employers, professional bodies, skills bodies, education providers and academia, which will strengthen the coherence between these key sectors.

Stimulating growth in the cybersecurity sector: The growth of cybersecurity sector is stimulated by the establishment of two innovation centres that drives the development of cutting-edge cyber products and dynamic new cybersecurity companies. These centres will sit at the heart of a programme of initiatives to give start-ups the support they need to get their first customers and attract further investment. Moreover, UK allocates a proportion of the £165m Defence and Cyber Innovation Fund to support innovative procurement in defence and security.

Promoting cybersecurity science and technology: Finally, the country is promoting cybersecurity science and technology through innovative and flexible funding models for research and the commercialisation of research. The Government will continue in providing funding and support to the Academic Centres of Excellence, Research Institutes and Centres for Doctoral Training.

USA Good Practices

Foster a vibrant and resilient Digital Economy: The United States, in their effort to foster a vibrant and resilient Digital Economy, adopted and secured their technological marketplace by improving awareness and advising a certain transparency to cybersecurity providers. Innovation is considered as one of their priorities and the country updated the cybersecurity standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem. These standards and practices should be outcome-oriented and based on sound technological principles rather than point-in-time company specifications. In addition, the country invests in Next Generation Infrastructure by following closely the evolution, such as 5G security. As one of the GCA pillar, priority is put in cooperation. United States have made great efforts on strengthening and creating new international partnership to foster an open industry/globalisation driven by international standards.

Foster and Protect US integrity: To foster and protect US integrity, the country revised its foreign investments through the review of Federal Communications Commission referrals for telecommunications licenses that promotes the protection of intellectual property rights and sensitive emerging technologies. By creating American brands, the country maintains an investor-friendly climate.

Develop a superior cybersecurity marketplace: Finally, the discussion mentioned the country's development of a superior cybersecurity market place in building domestic talent pipeline, promoting the development of robust cybersecurity workforce and enhancing the workforce by promoting financial compensation and unique training.

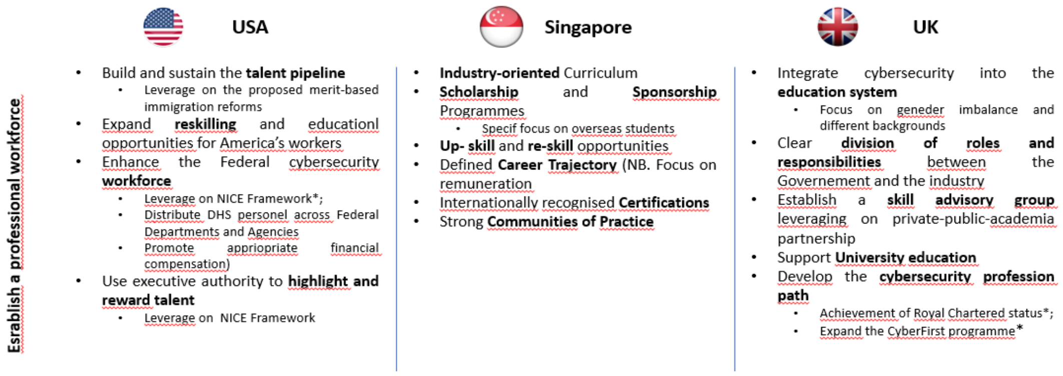
Analysis

Technology and policy considerations risk to dominate cybersecurity discussions, overlooking the fundamental human element at its core, therefore it is important to focus on capability, capacity building and awareness raising. In fact, this Focus Area addresses the challenges related to advancing cybersecurity capacity-building and awareness-raising among government entities, citizens, businesses and other organisations – crucial to enabling a country's digital economy. Good practices considered in this section include the establishment of dedicated cybersecurity curricula and awareness-raising programmes, expansion of training schemes and workforce-development programmes, adoption of international certification schemes, and promotion of innovation and research and development (R&D) clusters. The strategies presented in the exercise have many common features and some distinctive elements deriving from the different contexts to which they belong. These strategies have been chosen as a reference in order to present the approaches of three States, which have a good cyber maturity level and belong to different geographical areas. Therefore, these are not to be understood as the best examples of Strategy.

The Singapore strategy is well structured in areas of intervention and punctual actions. The objectives are developed along three streams: establishing a professional workforce, investing in cybersecurity advantage through strong local companies and innovating and accelerating the growth of the cybersecurity industry. The proposed initiatives are balanced between an interest in the growth and development of the internal market and the attraction of investments and know-how from third countries, as well as the outsourcing of industry and the development of market opportunities at the international level.

The group that analysed the UK Strategy noticed that, apart from paying particular attention to educational programmes and training at all levels, the Strategy focuses particularly on innovation and investments in research and development. The Strategy promotes partnerships between Industry, Academia and Government in all areas related to cybersecurity, from the creation of a "Skill Advisory Group" to identify the skills necessary for the profession, to finance the creation of centres of excellence and facilities.

From the presentation of the US Strategy an approach much more oriented to the promotion and protection of the cyber advantage and the digital economy of the country emerged. The United States is oriented to investing in innovation and mechanisms to protect their technological marketplace. In this regard, the interest in attracting third-party investors is balanced by the need for protection and guarantees.



Esrablish a professional workforce

USA

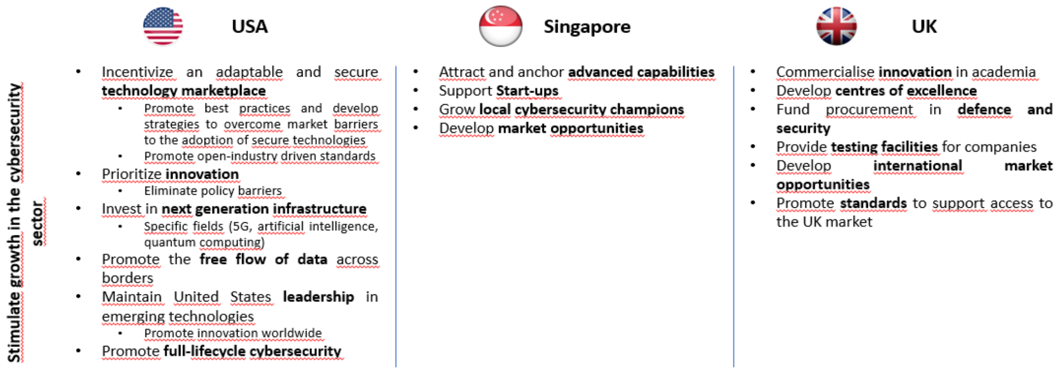
- Build and sustain the **talent pipeline**
  - Leverage on the proposed merit-based immigration reforms
- Expand **reskilling** and educationl opportunities for America's workers
- Enhance the Federal cybersecurity **workforce**
  - Leverage on NICE Framework*;
  - Distribute DHS personel across Federal Departments and Agencies
  - Promote appriopriate financial compensation)
- Use executive authority to **highlight and reward talent**
  - Leverage on NICE Framework

Singapore

- **Industry-oriented** Curriculum
- **Scholarship** and **Sponsorship** Programmes
  - Specif focus on overseas students
- **Up- skill** and **re-skill** opportunities
- Defined **Career Trajectory** (NB. Focus on remuneration
- Internationally recognised **Certifications**
- Strong **Communities of Practice**

UK

- Integrate cybersecurity into the **education system**
  - Focus on geneder imbalance and different backgrounds
- Clear **division of roles and responsibilities** between the Governement and the industry
- Establish a **skill advisory group** leveraging on private-public-academia partnership
- Support **University education**
- Develop the **cybersecurity profession path**
  - Achievement of Royal Chartered status*;
  - Expand the CyberFirst programme*



Stimulate growth in the cybersecurity sector

USA

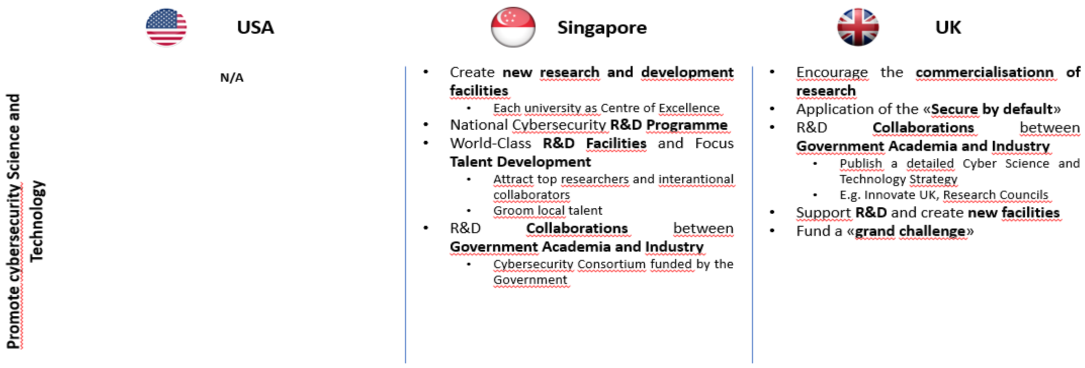
- Incentivize an adaptable and secure **technology marketplace**
  - Promote best practices and develop strategies to overcome market barriers to the adoption of secure technologies
  - Promote open-industry driven standards
- Prioritize **innovation**
  - Eliminate policy barriers
- Invest in **next generation infrastructure**
  - Specific fields (5G, artificial intelligence, quantum computing)
- Promote the **free flow of data** across borders
- Maintain United States **leadership** in emerging technologies
  - Promote innovation worldwide
- Promote **full-lifecycle cybersecurity**

Singapore

- Attract and anchor **advanced capabilities**
- Support **Start-ups**
- Grow **local cybersecurity champions**
- Develop **market opportunities**

UK

- Commercialise **innovation** in academia
- Develop **centres of excellence**
- Fund procurement in **defence and security**
- Provide **testing facilities** for companies
- Develop **international market opportunities**
- Promote **standards** to support access to the UK market



	USA	Singapore	UK
Promote cybersecurity Science and Technology	N/A	- Create **new research and development facilities** - Each university as Centre of Excellence - National Cybersecurity **R&D Programme** - World-Class **R&D Facilities** and Focus **Talent Development** - Attract top researchers and interantional collaborators - Groom local talent - R&D **Collaborations** between **Government Academia and Industry** - Cybersecurity Consortium funded by the Government	- Encourage the **commercialisationn of research** - Application of the «**Secure by default**» - R&D **Collaborations** between **Government Academia and Industry** - Publish a detailed Cyber Science and Technology Strategy - E.g. Innovate UK, Research Councils - Support **R&D** and create **new facilities** - Fund a «**grand challenge**»

Figure 6: Exercise result on Good Practices

The benchmark of the strategies highlights how various activities can be grouped into three different streams: establishment of a professional workforce, stimulating growth in the cybersecurity sector and promoting cybersecurity Science and Technology as depicted in figure 4 above.

14.HANDS-ON EXERCISE: OPEN QUESTIONS ABOUT GOOD PRACTICES

The goal of the exercise was to stimulate the analysis capabilities of the groups, in order to evaluate pros and cons for each approach related to a Good Practice – Focus Area. In particular, the participants, were put in two groups. Each group were given four questions: two related to "Critical Infrastructure services and essential services" and two related to "International Cooperation". At first, the groups answered the questions related to "Critical Infrastructure services and essential services" and discussed about the results with Deloitte facilitators, supported by a benchmark of US, Singapore and UK National Cybersecurity Strategies focused on the same theme, implemented by facilitators themselves. Then, the groups answered the other questions related to "International Cooperation" and discussed about the results with Deloitte facilitators, also supported by a benchmark of US, Singapore and UK National Cybersecurity Strategies focused on the same theme, implemented by facilitators themselves. The exercise questions were:

Critical Infrastructure services and essential services:

1. What elements are necessary in a strategy to ensure Critical Infrastructure protection?

2. How to achieve an effective collaboration between Critical Infrastructures?

International Cooperation:

1. Which level of international cooperation (regional, international) do you consider more effective?

2. How to achieve an effective International Cooperation?

Related to the topic "Critical Infrastructure services and essential services", the first group recognised the need to establish and formalize strategic partnerships with owners of Critical Infrastructures and exchanging of information and expertise between them. From a technical point of view, the group also pointed out the opportunity of technical security measures implementation and procedures development.

The second group, instead, focused its attention on the need for an unambiguous definition of the concept of "Critical Infrastructures", because there are multiple definitions, which could create confusion, especially in the identification phase of the critical actors. Moreover, once the category has been defined, the need to survey all critical infrastructure assets and essential services providers has been highlighted. Finally, the second group reiterated the opportunity of Information and knowledge sharing between Critical Infrastructures.

Regarding the topic "International Cooperation", the first group noted the importance of cooperation both at regional and international level, specifying, however, that regional cooperation is a prerequisite of international cooperation. As a best example of cooperation, a specific reference was made to the need to collaborate with international institutions such as EU, NATO and ITU. The second group, has noted particular advantages in regional cooperation because it seems easier to carry on joint projects with "neighbours" who share several common features. As last point, the importance of developing workshops and table top exercises within the international community has been recognized, as well as the opportunity to establish partnerships between countries that share common goals within their respective National Cybersecurity Strategies.

Analysis

Analysing the various approaches identified within US, Singapore and UK strategies and used by the groups for the good practices and focus areas implementation, it should be noted that there is no wrong or correct approach because each approach is connected with the strategic needs of each country. For this reason, to guarantee national security, some countries might consider some priority actions while other countries would consider a different action as more relevant to their strategic needs. In particular, it was interesting to observe the involvement of the participants in trying to reason as a regional area, recognizing the opportunity for joint action between countries.

Critical Infrastructure and essential services is a pillar of Cybersecurity. It was also interesting how both groups highlighted the importance of information and knowledge sharing between stakeholders and introduced the concept "country ecosystems". In fact, from the point of view of national security, within cyber environment where the threat is hybrid and not perimeter, individual national actors must think as part of an ecosystem rather than individually.

Referring to International Cooperation, both groups considered the two levels of cooperation, regional and international. The first group identified regional cooperation as a prerequisite for international cooperation, a natural evolution of a regional cooperation based on common objectives. The second one focused on the ease of a regional cooperation to promote joint actions with neighbouring countries with common cultures and experiences. In addition, the value of international cooperation has been considered as an effective method for a solid development of common interests.

The results produced by the groups were interesting as despite the limited time, both groups, with different approaches and considerations, identified some of the main aspects that form a National Cybersecurity Strategy. It emerged that awareness of the cyber environment can't be managed exclusively at national level but needs a constant comparison with the other countries.

15.WORKSHOP CONCLUSION

This workshop provided an insight to all participants on how to use the NCS guide to assess the current situation in their respective countries, to apply the analytical tools embedded in the approach and perspectives explained in the guide to reach a better understanding on what needs to be done to improve the current NCS situation, to renew the action plan and to ensure sustainable effective implementation.

Trainers as well as participants agreed that a follow-up exercise at sub-regional and even at national levels would be highly beneficial to continue the work initiated in the last two days for all countries represented in the workshop to make full use of the NCS guide and bring their National Cybersecurity Strategies to a level where these can be benchmarked, can be successfully implemented, monitored and further improved.