GLOBAL AGENDA
ON
CYBER CAPACITY BUILDING

FIRST DRAFT

CONTENTS

1. PREAMBLE

CONTEXT

The world is rapidly transforming through digitalization. Digital networks and cyber systems are entering many aspects of society. Cyberspace brings tremendous changes in the way people work, communicate, travel and live across the globe. Digitization brings great new opportunities to businesses, individuals and governments. Personal and professional lives are infused with digital services which empower many societal functions. Communities across the globe are closer connected than ever before. Cyberspace, digital technology and devices have become the foundation upon which communities and businesses are built.

International communities[1] recognize a strong sense of urgency to develop global cyber capacities to address the (known and unknown) risks to cyberspace. For this reason the Global Forum on Cyber Expertise (GFCE) was launched in 2015 at the Global Conference on Cyber Space (GCCS) in The Hague. The GFCE currently entails 60+ members consisting of governments, industry, non-governmental organizations (NGOs), technical communities and international organizations. In addition, the GFCE has a broad partner network consisting of civil organizations, academia and knowledge institutes.

Cyber capacities range from national policy to daily practice, from international cooperation to local expertise and cooperation, from rapid crisis response to long-term development programming. Building and developing global cyber capacities strengthens global resilience and enables citizens, organizations and nations to take better advantage of cyberspace opportunities.

Because of differences in culture, law, governance and organizational structures, and pace of cyber-development, capacity building efforts will need to be tailored to the needs of nations. Cyber capacity building can make a major step forward, nationally and globally, through better orchestration of existing national and global efforts, and by smarter sharing of resources. Therefore, there is an urgent need for international cooperation as global community. Nations, organizations, and other multilateral and global entities need to act consistently, coherently, coordinated, and collaboratively to ensure a free, open, safe, and secure cyberspace.

OBJECTIVE

The Global Agenda on Cyber Capacity Building (GACCB) has been developed by the GFCE community over the past months through extensive research, consultation and discussion. The GACCB will be presented to the global community at the GCCS2017 on 23-24 November in New Delhi, India.

With the GACCB the GFCE aims to encourage the global community to:

- Strengthen international cooperation;
- Develop a common (global) focus;
- Make more efficient use of available resources;
- Establish a concrete set of ambitions and actions.

[1] e.g. by the Global Conferences on Cyber Space (GCSS 2011,2013,2015), World Summit on Information Security (WSIS(+10) 2003, 2015), United Nations Group of Governmental Experts (UN GGE 2010, 2015) and the Busan Partnership for Effective Development Cooperation (2011).

With the GACCB the GFCE identifies future priorities for cyber capacity building (CCB) and recognizes the need for practical guides, frameworks and practices for CCB. This ambition reaffirms the function of the GFCE as a global knowledge sharing platform, and global coordination mechanism.

This GACCB addresses the sense of urgency and calls for action to jointly strengthen cyber capacities.

PROCESS

The GFCE community takes leadership in developing the GACCB. The Netherlands Organisation for Applied Scientific Research TNO facilitates this process. At every step of this trajectory, the global multi-stakeholder community (national governments, technical community, private companies, international organizations, knowledge partners and civil society) will be invited to provide input and feedback to ensure that the GACCB supports the global ambitions.

The development process of the GACCB:

April – May	• Desk research and analysis:
	  ○ 72 National Cyber Security Strategies
	  ○ International Policy Documents
	  ○ Oxford Portal content

May 31 – June 1	• Annual Meeting GFCE, Brussels – presenting the results of the desk-research. Prioritization of key topics and agenda directions.
June - August	• Request for input and feedback on the GACCB outline document by the GFCE community. • Conference calls on the GACCB with national governments, technical community, private companies, international organizations, knowledge partners and civil society.
September	• Request for feedback of the first draft GACCB. • Review (written input) by GFCE community on first draft. • Workshop GACCB in The Hague/ remote calls on September 26th.
October	• Review (written input) by GFCE community after workshop on first draft GACCB. Request for acceptance of 2nd draft of the GACCB. • Final GFCE draft version of the GACCB (to be shared with the GCCS community) in mid-October.
Mid-October – November 21	• Consultation period with the GCCS community. • GFCE Pre-meeting GCCS, presenting the final version of the GACCB.
November 23-24	• Presentation of the GACCB to the GCCS.

2. GUIDING PRINCIPLES FOR GLOBAL CYBER CAPACITY BUILDING

Based on the *Busan Partnership for Effective Development Cooperation* principles[2], the following guiding principles for CCB have been derived:

1. **Inclusiveness:** Strengthening cyber capacity and expertise is a global responsibility
2. **Ownership**: Partner nations need to take ownership of capacity building priorities.
3. **Sustainability**: Obtaining sustainable impact should be the driving force for cyber capacity building
4. **Partnership**: Cyber Capacity Building requires the participation of all actors
5. **Transparency and shared responsibility**: Transparency and shared responsibility are fundamental values of cyber resilience

Inclusiveness: Strengthening cyber capacity, expertise and resources is a global effort

The global community should work towards a more open and proactive attitude of sharing expertise, information and resources, while recognizing individual interests.

Ownership: Partner nations need to take ownership of capacity building priorities

Nations depend on each other's capacities to mitigate threats, and build a free, open, safe and secure cyberspace to foster a prosperous future. Nations have a due diligence in cyberspace by attaining a base set of cyber capacities (e.g. on National Cyber Security Strategy, Critical Information Infrastructure Protection, National Cyber Security Incident Response Capacity, Cyber Security Awareness, Education and Training, Legal Frameworks, Law Enforcement). It is also a responsibility among nations to call on other nations to develop similar capacities.

Sustainability: Obtaining sustainable impact should be the driving force for cyber capacity building

Cyber capacity building initiatives require a comprehensive approach that includes technical, human, organizational, governmental and legal aspects. This ensures that cyber capacities become well-embedded in their target environment and become sustainable and effective.

Partnership: Cyber Capacity Building requires the participation of all actors

The global community should connect and link national, regional and global cyber as well as non-cyber capacities, regardless of national contexts, priorities or cyber security standing.

Transparency and shared responsibility: Transparency and shared responsibility are fundamental values of cyber resilience

Organizations and citizens of all nations are collectively responsible for a safe and secure cyberspace. Nations have the joint responsibility to advance a culture of cyber security, and promote transparency and shared responsibility

[2] http://www.oecd.org/development/effectiveness/busanpartnership.htm

3. CAPACITIES (THEMES AND TOPICS)

In this chapter, the main capacities for international cooperation are described.

The GACCB is built upon **thematic areas of cyber capacity building** (see figure 1). Each thematic area constitutes an important foundation for national, regional and global cyber security developments. The thematic areas are closely linked and, according to the GFCE community, constitute key focal areas for this agenda.

At the GFCE Annual meeting (31 May 2017) 31 capacities (topics) were given priority by the GFCE community. During the consultation period (July and August) the list of topics was further refined to the current set of 15 cyber capacity building topics. Appendix 1 describes the capacity refinement process.

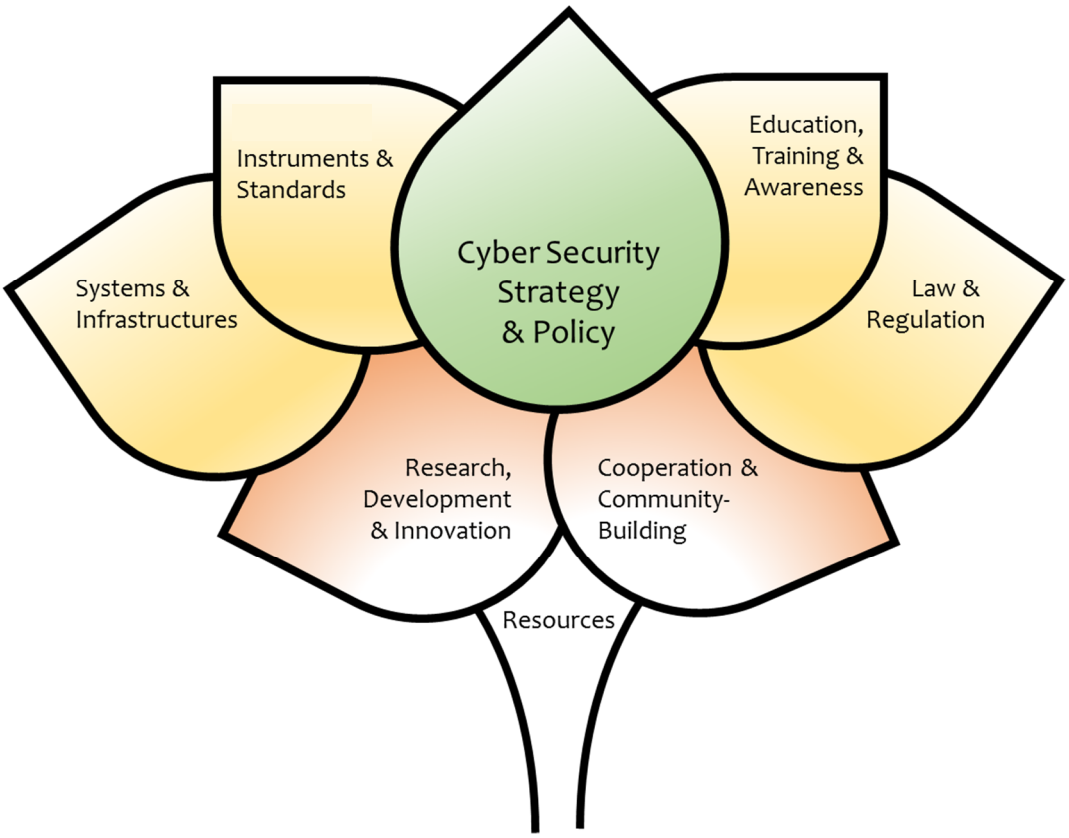
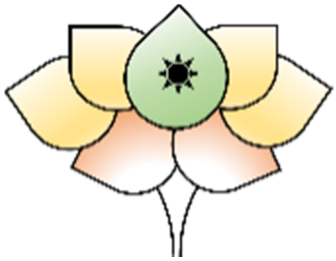


Figure 1: Thematic areas of cyber capacity building

THEME: **CYBER SECURITY STRATEGY & POLICY**



Cyber security and cyber resilience should start from a strongly stated, widely adopted strategy, rooted in a clear set of objectives and guided through effective policies. This holds true for organizations, sectors, nations and the global community, notwithstanding that strategies and policies might differ substantially. The capacity to build and maintain an effective cyber security strategy and policy should be regarded as a core capacity as it lays the foundation for capacity development.

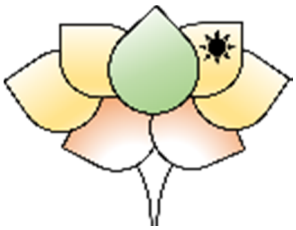
1. National Cyber Security Strategy

The capacity to publish a National Cyber Security Strategy (NCSS) is essential because the document outlines the major cyber security concerns of a nation and formulates action plans to deal with them. A NCSS belongs to the core of any nation's effort to improve cyber security and paves the way for developing other cyber capacity building topics.

2. Benchmarking

Benchmarking the state of national cyber security capacity assists in balancing one's cyber security raising efforts with perceived risk and to identify weaker areas which require additional efforts. Benchmarking can be done at any level of governance, and could be part of a comprehensive national cyber security strategy. Benchmarking should be performed periodically.

THEME: **EDUCATION, TRAINING & AWARENESS**



The capacity to learn is an essential pillar of resilience. Education and training creates a culture of awareness and a body of competence: skilled workers, informed citizens, more secure products and services, and a higher degree of societal awareness of cyber security opportunities, threats and risks.

3. Cyber Security Awareness

Cyber security awareness is the elemental understanding of cyber threats and risks, cyber hygiene, response options and perception of cyber risk in communities. This capacity is about the creation of a culture of cyber security in communities and providing perspectives for action when confronted with cyber risks.

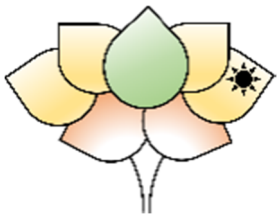
4. Education and Training

Education and Training is a capacity to systematically establish a skilled cyber security workforce, both in the public and private sectors as well as of the population at large that can prevent and respond to cyber security issues. This capacity includes the development of dedicated curricula, teaching and awareness-raising materials, streamlining the applicability of degrees, educators and certification measures. Training refers to knowledge and competences acquired after primary, secondary and higher years of education. Training focuses on specific skills that should be developed, and applied practically in order to improve performance, sustainability, and/or productivity.

5. Cyber Security Workforce

The cyber security workforce capacity refers to the readiness of an adequate sized cyber security workforce in a nation. In the forthcoming years a substantial growth of qualified and well-trained personnel is to be expected in order to address the cyber challenges in all layers of society.

THEME: **LAW & REGULATION**



Cyber security and cybercrime challenge traditional laws and regulatory frameworks, partly due to their institutional and geographical crosscutting nature. Therefore, it is crucial to establish effective national and international legal and regulatory frameworks. Moreover, adequate enforcement capacities to cope with cybercrime in all forms are a necessity.

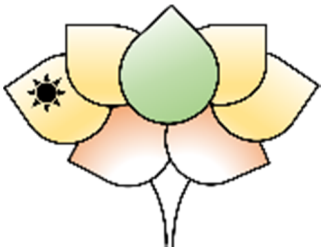
6. Legal Frameworks

Legal frameworks as a capacity for nations and organizations are essential to deal with cyber-related risk and crime issues effectively. Legal frameworks enable and provide new chances for economic development.

7. Law enforcement in cyberspace

Law enforcement in cyberspace is the capacity to adequately enforce law in cyberspace and to raise attention to operational capacity. This capacity includes trained law enforcement officers, cyber forensics, prosecutors and judges who thoroughly understand cyberspace related crimes and their ramifications.

THEME: **SYSTEMS & INFRASTRUCTURES**



This area of capacity development covers the development of systems, infrastructures and agencies that help to improve cyber security. This includes cyber security monitoring and management entities (CSIRTs/CERTs; intelligence agencies), as well as systems in place at infrastructures to uphold cyber security (response mechanisms, fallback options).

8. Computer Security Incident Response Team

The capacity to adequately prevent, detect, respond/mitigate and recover from a cyber incident is operationalized by a Computer Security Incident Response Team CSIRT. [3] This capacity is typically established as one or more CSIRTs with national responsibilities.

9. Critical Information Infrastructure Protection

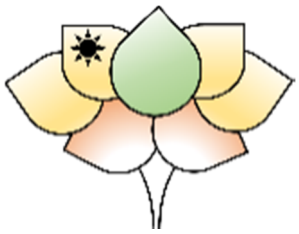
The capacity to define and protect the national critical information infrastructure (CII) helps to pinpoint cyber security-related risk to one's national critical infrastructure (CI), its services and assets; as well as to focus on prevention, incident response and incident recovery efforts.

[3] CSIRT to be replaced by multiple notions, e.g. Computer Emergency Response Team (CERT), Computer Incident Response Capability (CIRC), Cyber Incident Response Team (CIRT), Computer Security Incident Response Capability or Centre (CSIRC), Computer and Network Security Incident Response Team.

10. Cyber Security Exercises

The capacity to regularly perform national cyber security exercises, evaluate them and improve the national cyber security response mechanisms is an essential capacity. The capacity of nations and international organizations to organize joint cyber security exercises. Such exercises would include the participation of cyber security response teams, national critical infrastructure, national and international government agencies and other stakeholders.

THEME: **INSTRUMENTS & STANDARDS**



Instruments and standards form the backbone of cyber security capacity development, and provide agencies, sectors and businesses with the tools to prevent, prepare, respond and recover from cyber security incidents.

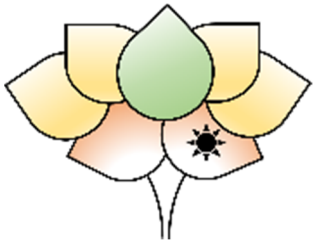
11. Standards

The capacity to develop, mandate and utilize cyber security practices, norms and standards. The focus of this capacity can be international, regional, national or sectorial standardization (e.g. ISO, CEN/CENELEC, BS, and ISA).

12. Record incident data and perform root cause analysis, facts, figures and statistics

This capacity reflects the need to become more mature by getting more grip and understanding of the threat landscape, its origins, history and causal links of (previous) incidents. This improves incident response analysis, evaluation and improvement of the response capacity and eventually the effectiveness of prevention measures.

THEME: **COOPERATION & COMMUNITY BUILDING**



Cooperation and community-building is an important capacity to achieve global cyber resilience. Cyberspace stretches across borders, sectors, systems and communities, and can only be made safe and secure by unity of vision, willingness and effort. The capacity to build communities and collaborations is a key requirement.

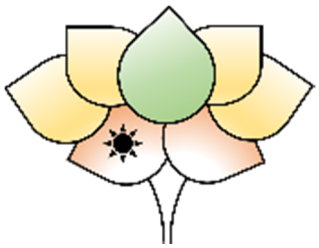
13. International collaboration networks

There are many established and emerging international networks in the field of cyber security. These networks address cyberspace security issues, and may have a strategic/tactical character, or a more practical operational character. These networks are important vehicles to discuss views, exchange experiences, agree on standards, harmonize approaches and build mutual trust and understanding. Nations and international organizations need to capitalize on these networks, and invest in making these networks an essential asset in their cyber security capacity building efforts. Increasing participation in these networks will help nations be more informed and more capable to deal with cyber security challenges.

14. Reinforce information sharing across national and international partners

Information sharing is the backbone of cyber capacity building. The capacity to engage in the timely sharing of reliable, actionable cyber security-related information is crucial in mitigating cyber security threats. Sharing may concern threats, vulnerabilities, incidents, and responses at strategic, tactical and operational/technical levels, and across the whole incident response cycle.[4] The objective is to enhance defenses, limit damage, increase situational awareness and broaden learning supported by mutual trust.

THEME: **RESEARCH, DEVELOPMENT & INNOVATION**



Capacities to organize, implement and exploit research, development and innovation in the field of cyber security and related fields. Such capacities will often leverage upon - and be embedded in - existing research, development and innovation infrastructures.

15. Research, Development and Innovation for cyber security

Research, Development and Innovation (RD&I) in cyber security capacity provides policy, resources and incentives to further cyber security RD&I. The specific capacity provides strategic direction for research, development and innovation in cyber security, and enables the effective and efficient valorization of results.

[4] Pro-act – prevent – prepare – detect – respond – recover – aftermath

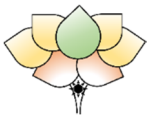
4. AMBITIONS AND ACTIONS – WORK IN PROGRESS CCB COMMUNITY

The GACCB identifies a set of ambitions and actions to strengthen the global endeavors on CCB. Over the past few months, numerous ambitions and GFCE needs were identified per capacity. These are presented in the table below. The next step in the GACCB process is to translate these ambitions into concrete actions.

The table consists of four columns:

- Topics (capacities);
- Ambitions;
- GFCE identified needs;
- Actions [5]

One outcome of the consultation round was the set of GFCE identified needs:



- Knowledge and information sharing through international cooperation / portal / shared database
- Good Practices / Common tool sets
- Pool of expertise / implementation experts
- Funding

These resource capacities are described in appendix 3.

The ambitions and the GFCE identified needs give direction to the GFCE and GCCS communities to translate these into actions. These two columns should be further refined in consultation with the GFCE community. The 'actions' column is still empty and will be filled in by the communities in the months towards the GCCS2017, (e.g. work in progress)

[5] Appendix 2 contains examples of current activities per topic.

THEME: **CYBER SECURITY STRATEGY & POLICY**

Topic	Ambitions	GFCE identified needs	Actions
1. National Cyber Security Strategy (NCSS)	• Nations have a comprehensive NCSS in place.	• Insight into which actors and/or nations are supporting others in establishing NCSSs.	
2. Benchmarking	• Nations and other stakeholders have obtained insight into the state of their cyber security postures by the use of benchmarking. • Collaborative development of an international metrics methodology.	• Standards for data collection and tools.	

THEME: **EDUCATION, TRAINING & AWARENESS**

Topic	Ambitions	GFCE identified needs	Actions
3. Cyber Security Awareness	• Nations and other stakeholders are collaboratively aware of cyberspace's potential, its risks and the needs for cyber secure behavior.	• Combining and developing a knowledge repository on good practices for awareness campaigns. • Expertise for performing awareness campaigns nationally. • Funding of cyber security awareness campaigns.	
4. Education and Training	• Basic cyber security skills education and training across age groups and employment categories supported or initiated by the government. • Good practices, tools, and materials for cyber security education programs are produced, available and disseminated worldwide.	• Expertise, knowledge sharing, and development of tools and material. • Funding.	

Topic	Ambitions	GFCE identified needs	Actions
5. Cyber Security Workforce	• Workforce development of essential cyber security skills. • Curricula and certifications are developed and harmonized globally.	• Coordinated workforce development. • Adequate cyber-related curricula in colleges/universities. • Accredited training organizations. • Resources (funding, skilled workforce).	

THEME: **LAW & REGULATION**

Topic	Ambitions	GFCE identified needs	Actions
6. Legal Frameworks	• Nations have specific criminal and procedural legal frameworks to respond to cybercrime challenges, e.g. signing, ratifying and implementing the Budapest Convention on cybercrime. • The national legal framework enables the successful use of cyberspace, its developments and new services.	• Pooling of expertise.	
7. Law enforcement in cyberspace	• Nations have well-trained and effective law enforcement, judges etc. on cybercrime issues. • Nations have established higher level of international anti-cybercrime cooperation, e.g. with INTERPOL, EC3, CEPOL and a point of contact available 24/7.	• Skilled workforce. • Pooling of expertise. • Adequate cyber related curricula in colleges/universities within the region. • Funding.	

THEME: **SYSTEMS & INFRASTRUCTURES**

Topic	Ambitions	GFCE identified needs	Actions
8. Computer Security Incident Response Team (CSIRT)	• Nations have a CSIRT with national responsibility in place. • Nations with a CSIRT with national responsibility work on maturing their operations and their international relations.	• Training and educating local technical expertise. • Good practices. • Increased standardization between CSIRT communities. • Community building. • Funding.	
9. Cyber Security Exercises	• Nations and other stakeholders participate in international exercises, with realistic scenarios that test crisis management, contingency plans, and communications.	• Leadership. • Basic national cyber security training packages. • Resources (workforce, budget).	
10. Critical Information Infrastructure Protection (CIIP)	• Nations are aware of the importance of CIIP, have developed a strategy for CIIP, identified CII operators, and have (let) created protection plans. • Nations with cross-border CII, approach CIIP multilaterally.	• Good practices. • Funding.	

THEME: **INSTRUMENTS & STANDARDS**

Topic	Ambitions	GFCE identified needs	Actions
11. Standards	• Nations should consider applying a recognized cyber security standards scheme (or develop an equivalent national standard). • Industry and other organizations adhere to standards.	• Awareness of the benefits of a cyber security standards scheme. • Cyber security by design in products and services.	.
12. Record incident data and perform	• Nations and other stakeholders record cyber security breaches and	• Good practices, methodologies and tools.	-

Topic	Ambitions	GFCE identified needs	Actions
root cause analysis, facts, figures and statistics	their effects as well as perform analyze root causes with the aim to improve products and services.		

THEME: **COOPERATION AND COMMUNITY BUILDING**

Topic	Ambition	GFCE identified needs	Actions
13. International collaboration networks	• Overcome regional silos in cyber capacity building. • A continuously updated knowledge base on existing efforts at a small set of collaborating internationally accepted clearing houses. • Use of Confidence Building Measures by nations, to foster collaboration and the development of trust in terms of cyber security.	• Knowledge and information exchange. • Trust building.	
14. Reinforce information sharing across national and international partners	• Develop theories and concepts of Trusted Information Sharing and encourage its practice (e.g. in many trusted information sharing groups within and across critical sectors and across borders).	• Methodology development and implementation.	

THEME: **RESEARCH, DEVELOPMENT AND INNOVATION**

Topic	Ambitions	GFCE identified needs	Actions
15. Research, Development and Innovation for cyber security	• Development of an international research and development agenda and network for cyber security.	• Clustering of knowledge and research expertise.	

APPENDIX 1 | CAPACITY (TOPIC) REFINEMENT PROCESS

During the GFCE Annual meeting (31 May – 01 June 2017) the GFCE members started the process towards a Global Agenda on Cyber Capacity Building (GACCB). Through extensive desk research (National Cyber Security Strategies, International Policy Document, Oxford Portal) numerous topics were identified out of which 31 topics were prioritized. The number of topics was further refined during the consultation period between July and August. The following table reflects the changes with regard to the CCB capacities (topics).

July 2017	**September 2017**
Cyber Security Strategy & Policy • National Cyber Security Strategy • Future cyber security threats • Benchmarking • Adapt policy to new cyber risk	Cyber Security Strategy & Policy • National Cyber Security Strategy • Benchmarking *National Cyber Security Strategy & Policy and benchmarking are prioritized by the community.*
Education, Training & Awareness • Education and training • Cyber security awareness • Cyber security workforce • National cyber security exercises • International cyber security exercises • Culture of Cyber Security	Education, Training & Awareness • Education and training • Cyber security awareness • Cyber security workforce *National and international exercises are grouped within theme 'Systems and Infrastructures'.*
Law & Regulation • National & Int'l organizational legal frameworks • Law enforcement in cyberspace • Criminal law and Criminal Procedure Law • Data protection	Law & Regulation • Legal frameworks • Law enforcement in cyberspace *Legal frameworks and law enforcement in cyberspace are prioritized by the community.*
Systems & Infrastructures • Critical Information Infrastructure Protection • Computer Emergency Response / Cyber Security Incident Response	Systems & Infrastructures • Computer Security Incident Response Team (CSIRT) • Cyber Security Exercises • Critical Information Infrastructure Protection *Cyber Security Exercises are added as priority within this theme.*
Instruments & Standards • National Emergency response • Early warning/ Threat Intelligence gathering and sharing • Sharing Good Practices • (Inter)national cyber security standards	Instruments & Standards • Cyber security standards • Record incident data, root cause analyses, fact and figures, and statistics *July 17 topics are grouped into 'cyber security standards' and 'Record incident data, root cause*

July 2017	**September 2017**
• International Emergency Response • Incident data, root cause analyses, fact and figures, and statistics • Cybersecurity self-check / health check • Coordinated Vulnerability Disclosure (CVD)	*analyses, fact and figures, and statistics'.*
Cooperation and community building • International collaboration networks • Confidence Building Measures • Cyber diplomacy • Information sharing	Cooperation and community building • International collaboration networks • Reinforce information sharing across national and international partners *July 17 topics are grouped into 'international collaboration networks' and 'reinforce information sharing across national and international partners'.*
Research, Development & Innovation • Cyber security-by-design • RD&I in cyber security • Cryptographic protection	Research, Development & Innovation • RD&I for cyber security *Cyber Security-by-Design and Cryptographic protection is part of RD&I for cyber security.*

APPENDIX 2 | EXAMPLES OF CURRENT ACTIVITIES

The following list provides an overview of current example activities per capacity (topic). Regional and global activities and initiatives are presented. The list is not exhaustive. These examples will be side-to-side with new activities and initiatives in due time.

Themes/topics	**Examples of current activities**
Cyber security strategy & policy	
1. National cyber security strategy (NCSS)	ITU National Cyber Security Strategy (NCS) Toolkit (forthcoming)
2. Benchmarking	Capacity Maturity Model (GCSCC). ITU Cyber Readiness Index. ITU Global Cybersecurity Index. Cyber Green Initiative.
Education, training & awareness	
3. Cyber security awareness	STOP.THINK.CONNECT. Japan-ASEAN information Security Policy meeting.
4. Education and Training	National Initiative for Cybersecurity Education (NICE)
5. Cyber security workforce	Training of trainers by experts on cybercrime and electronic evidence. Cyber-legislation workshop for ECOWAS Member States in collaboration with the Council of Europe
Law & regulation	
6. Legal frameworks	
7. Law enforcement in cyberspace	Training of trainers by experts on cybercrime and electronic evidence. Cyber-legislation workshop for ECOWAS Member States in collaboration with the Council of Europe.
Systems & infrastructures	
8. Computer security incident response team	ITU's multi-stakeholder efforts to aggregate publications and resources. ITU's National CIRT Programme. CSIRT Maturity Toolkit. Memorandum on CSIRTs

Themes/topics	Examples of current activities
9. Critical information infrastructure protection (CIIP)	GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection 2016, 2017. Memorandum on Critical Information Infrastructure Protection.
10. Cyber security exercises	International exercises organized by regions (e.g. APCERT, Nordic CERTs) and collaborations (e.g. NATO, multi-nation, European Governmental CERTs, International Watch and Warning Network IWWN).
Procedures, instruments & standards	
11. Standards	Activities by committees of national and international standardization organizations.
12. Record incident data and perform root cause analysis, facts, figures and statistics	
Cooperation and Community-Building	
13. International collaboration networks	GLACY+ project. GFCE/Oxford portal with initiatives. ITU's actions for knowledge sharing & mutual assistance. Japan actively provides information on its fundamental viewpoint and shares it with many countries through various international fora, such as the UN and bilateral cyber security dialogues. OCSE initiatives, e.g. implementation of OSCE CBMs agreed in 2013 and 2016; Cooperation with other regional organizations such as OAS, AU, ASEAN to promote implementation.
14. Reinforce information sharing across national and international partners	FIRST's promotion of the Traffic Light Protocol. On-going discussion of IE/ISAC models. Attempts to automate the practices. Cybersecurity Good Practices on Sharing Cyber Security Information.
Research, development and Innovation	
15. Research, Development and Innovation for cyber security	

APPENDIX 3 | GFCE IDENTIFIED NEEDS

The GFCE identified needs are the result of repeated statements by the GFCE community and other stakeholders involved in developing the GACCB. The understanding of the GFCE identified needs is an important step in the translation from ambitions to actions.

- **Knowledge and information sharing through international cooperation / portal / shared database**

International cooperation and exchanging information on cyber capacity building has many advantages for stakeholders in the field of cyber capacity building:

1. Learning from the successes and mistakes of others when developing cyber capacities reduces the risk of making the same errors. As a result, capacity building will be accomplished faster and with fewer resources.
2. International collaboration helps to build trust and sustainable networks.
3. Nations offering knowledge and information to other nations benefit when the latter become more cyber safe and secure faster.

The community expressed the need to have a trusted, reviewed and authoritative portal, database or repository containing state of the art information about current CCB initiatives, efforts, baselines, financial streams, recipient (organizations, regions, and nations), donors (industry, nations, NGOs, intergovernmental organizations, regional organizations etc.).

- **Good Practices / Common tool sets**

A good (or best) practice is an agreement that standardizes or prescribes a most efficient and effective way to accomplish a desired outcome. Good practices are usually published in the form of a document or toolkit which reflects on a proven technique, method, or process. Good practices may be converted to (inter)national standards[6].

The GFCE community and other stakeholders involved in developing the GACCB expressed the need to have good practices available which makes duplication of efforts efficient and reduces the risk of making avoidable errors. A set of GFCE good practice documents supporting CCB is in the process of being developed. The community asked for more coordinated mechanism to collaboratively develop good practices. Another need expressed is expert translation of existing material into major languages to support more nations. Good practices are preferably licensed rights free or through creative commons to allow translation and tuning to the local need of nations.

A special type of good practices is the availability of practical tool sets that support cyber capacity building. Tool sets may be developed as part of multistakeholder initiatives. A requirement is that stakeholders should be able to locate such tool sets, e.g. through a common portal. Global initiatives which develop a tool set should consider flexibility, allowing an easy adaption of the tool to other languages.

- **Pool of expertise/ experts**

Local, national and regional cyber capacity building stakeholders need dedicated pools of human expertise at regional and global levels. The expertise pool should be available and dedicated to enable local practitioners

[6] The ISO/IEC 27001:2014 and ISO/IEC 27002:2014 standards are examples of standards for information security which became well-accepted and supported international standards.

to duplicate and embed expertise. Making use of available expertise and help by experts which are sensible to national culture, organizational structures and the nation's needs, increases efficiency, speeds up cyber capacity building in nations, and reduces the need to 'reinvent wheels'.

On certain cyber security topics, the pool of globally available experts is limited. Building such capacity in nations may take exceptionally long. Nations have expressed the need for support by internationally recognized experts to develop teaching materials and to teach the next echelon, which in turn can teach and develop the needed qualified workforce in nations. The teaching materials can be study books and materials, recorded lessons, and Massive Open Online Courses. Such materials are preferably licensed through creative commons to allow translation and tuning to the local need of nations.

The pooling of experts, mentioned above, is an intermediate step in the development of this capacity.

- **Funding**

CCB in the end requires man-hours, and materials, which translates into costs. The capacity to manage and request, to allocate, and to apply for funding are activities the community needs to understand. As this resource is scarce, investments need to be efficient, effective and sustainable. International collaboration, regional and global initiatives, as well as sharing of information, good practices, and lessons learned may enhance such efficiency in cyber capacity building globally.