GLOBAL AGENDA

FOR

CYBER CAPACITY BUILDING

Putting Principles into Practice

November 21st 2017 Version

GFCE
Global Forum on Cyber Expertise

CONTENTS

1. INTRODUCTION

THE IMPORTANCE OF CYBER CAPACITY BUILDING

The global digital economy has rapidly changed the world. Digital networks are part of many aspects of society – communities across the globe are more interconnected than ever before. Cyberspace creates countless new opportunities for individuals, businesses, and governments but also comes with challenges to existing concepts of governance, security and way of living.

Cyberspace is dynamic and ever evolving, and therefore all stakeholders must be able to adapt and continually improve their capabilities to address the risks that arise. To be better prepared for known and unknown threats in cyberspace, nations, businesses and other stakeholders must work together and invest in ***cyber capacity building (CCB).***[1]

The need for cyber capacity building is a topic important to all stakeholders, regardless of their maturity level. The need for a global agenda stems from:

- A lack of harmonization of efforts across nations and sectors;
- A poor understanding of the causes, impacts and phenomena in cyberspace; and
- A global imbalance in resources, knowledge and expertise.

To overcome these challenges, it is important to find more effective ways to work together, build new partnerships, establish and promote best practices and to provide assistance to each other.

The Global Forum on Cyber Expertise recognizes the urgency to strengthen international cooperation in cyber security, and the development of global cyber capacities.[2] Nations, organizations, and other multi-lateral and global communities need to act consistently, coherently, collaboratively and in a coordinated fashion to ensure an open, free and secure cyberspace – a crucial requirement for a prosperous future.

---

[1] The development and reinforcement of processes, competences, resources and agreements that is necessary for communities, businesses and governments to cope with the rapid changes and challenges of a fast-changing world. Cyber capacity building is global in nature, since the Internet transcends conventional borders.

[2] 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), The Busan Partnership for Effective Development Cooperation (2011).

GUIDING PRINCIPLES FOR CYBER CAPACITY BUILDING

The Fourth High Level Forum on Aid Effectiveness (Busan, Republic of Korea, 29 November to 1 December 2011) articulated a number of principles for effective development cooperation in the *Busan Partnership for Effective Development Cooperation*.[3] The following guiding principles are derived from the Busan outcomes, and adapted to the cyber capacity building context.

1. Inclusive partnerships and shared responsibility: effective cyber capacity building requires cooperation across nations, including various stakeholders, and at different levels

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. Trust, transparency and accountability: transparency and accountability play a key role in establishing trust, which is necessary for effective cooperation

OBJECTIVE

Over the past nine months, the GFCE conducted extensive research, consultations and discussions to develop the GACCB. The global multi-stakeholder community (national governments, technical community, private companies, international organizations, knowledge partners and civil society) provided input and feedback at every step to ensure the GACCB supports global ambitions.

The GACCB encourages the global community to:

- Strengthen international cooperation;
- Develop a common (global) focus;
- Drive a more efficient use of available resources;
- Establish a shared set of ambitions.

The GACCB reaffirms the GFCE's efforts on the prioritization of cyber capacity building and calls for action to jointly strengthen global cyber capacities.

The GACCB is organized into three sections:

1. **Themes and topics**, which state the high-priority goals and topics for cyber capacity building, as identified by the GFCE;
2. An Annex of **Guiding principles**, which define fundamental values GFCE members uphold in cyber capacity building efforts; and
3. An Annex of **Practical guides**: frameworks and practices for cyber capacity building (CCB) derived from GFCE Initiatives.

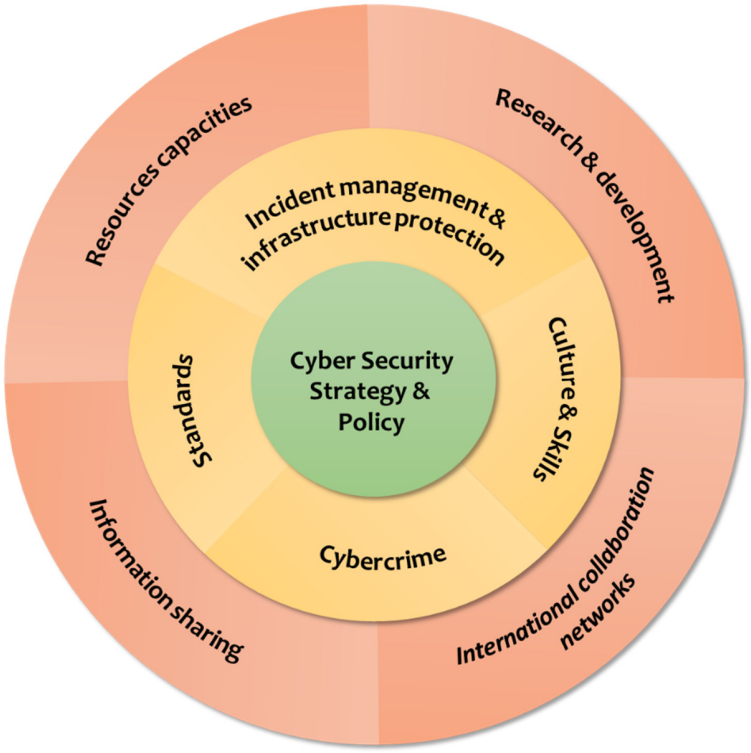
The GACCB reaffirms the function of the GFCE as a global knowledge exchange and coordination platform.

[3] http://www.oecd.org/dac/effectiveness/49650173.pdf

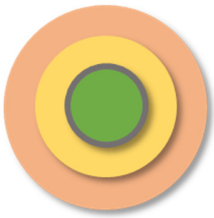
2. CYBER CAPACITY BUILDING THEMES AND TOPICS

The GACCB builds upon **themes of cyber capacity building.** Each theme constitutes an important foundation for national, regional, and global cyber security developments. They are closely related and constitute key foci for cyber capacity building efforts as identified by the GFCE, and are mutually reinforcing.

The diagram below visualizes the themes and topics. 'Cyber Security Policy & Strategy' is positioned at the center of the diagram to represent its central role. The surrounding topics constitute indispensable areas of cyber capacity development. The underlying topics are cross-cutting capacities



THEME: CYBER SECURITY POLICY & STRATEGY



A clearly articulated, widely adopted national cyber security strategy can represent the core of national cyber resilience efforts. Although national approaches may differ, both an effective cyber security strategy and policy, will allow nations to communicate their priorities, set clear goals, define roles and responsibilities, and identify their needs, therefore laying the foundation for continuous capacity development.

1. National Cyber Security Strategies

Seek national policy level commitment to cyber security in order to drive strategic planning, resourcing and implementation. This commonly includes developing and implementing a National Cyber Security Strategy (NCSS).[4] The development and implementation of a comprehensive national cyber security strategy should take into consideration the role of all stakeholders (government authorities, the private sector, civil society, and citizens).

A NCSS can represent the core of any nation's effort to improve cyber security. A NCSS can convey the main cyber security challenges a nation is facing, as well as formulate a vision and priorities to meet these challenges. Concrete actions are often set out in a separate action plan or in the strategy itself. To achieve maximum impact and ownership to the direction and priorities the strategy sets, a NCSS should build upon contributions from the whole of government and multi-stakeholder community (public sector, private sector, technical community, civil society, and other stakeholders). Only in this manner, will it be able to align national priorities, policies, and actions with interests of the multi-stakeholder community, and sets the stage for cyber security and economic development. A NCSS should be evaluated and revised in regular intervals.

The drafting of a NCSS can support a nation identifying and understanding their strengths and priorities, as well as their needs in protecting critical information infrastructure, and other aspects of their online environment. Furthermore, a NCSS can drive transparency both domestically and internationally as it communicates a nation's priorities, existing or developing capacities and approaches that contribute to a secure and resilient cyberspace.

Nations with an established NCSS may share their experiences and practices with other nations. Nations in early phases of NCSS development may actively seek support from other nations and organizations with proven expertise in this field.

[4] Some nations or organizations name this a digital (security) strategy or alike.

2. National Cyber Security assessments

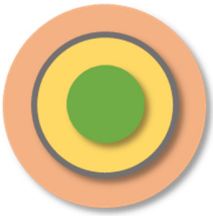
Assess current national practices, threats and vulnerabilities, and develop, implement and evolve over time, as necessary, a comprehensive national cyber security strategy that considers how these issues impact all stakeholders and their role in the process.
National cyber security assessments provide insight into the national level playing field considering cyber security measures, challenges, practices, threats and vulnerabilities. Assessment results may influence national policy writers and political decision makers to plan next steps.

Reoccurring national cyber capacity assessments help mitigate identified risks with actions, and identifies areas for improvement, as cyber security evolves. Risk management needs to be at the core of any national approach. In a national cyber capacity assessment, stakeholders may weigh their state of cyber security against an established national or international baseline. Outcomes may provide insight into a stakeholder's capacity to withstand and cope cyber-attacks and to ensure business continuity. National capacity assessments may help track CCB activities in a standardized and harmonized way, and assure that continuous progress is made.

Stakeholders with experience in the implementation of a NCSS and capacity assessments may share practices, and provide support to nations that are in earlier phases of development. The global stakeholder community should develop and promote practices that allow nations to assess their capacities.

THEME: INCIDENT MANAGEMENT & INFRASTRUCTURE PROTECTION

CCB on incident management and infrastructure protection aims to improve capacities that allow nations to respond to and recover from cyber incidents in a timely and efficient manner. Monitoring, response and mitigation capacities enhances infrastructures continuity and can improve communication and cooperation between national and international entities and stakeholders. In turn these activities can support the overall cyber resilience of cyberspace much beyond a particular nation.



3. National Computer Security Incident Response

Develop national incident response systems prevent, detect, deter, respond to and recover from cyber incidents. This system commonly includes one or more Computer Security Incident Response Teams (CSIRTs) with national responsibilities.

On a technical level, national CSIRTs preferably are well-connected with international communities. The global community may encourage nations to establish a national Computer Security Incident Response team capacity (CSIRT[5]).

On the policy level, nations should identify the capacities that are needed to ensure that incidents are reported to responsible entities, and that these parties are provided with sufficient information for effective decision making.

Nations and multilateral organizations with established national CSIRTs may mature their operations and broaden and strengthen their national and international information exchange of technical indicators and mitigation advices. National Cyber Security Centers may enable and encourage regional and sectorial initiatives to collectively strengthen cyber security-related ecosystems.

4. Incident capture and analytics

Improving the ability to document cyber security incidents and perform analysis on root causes and effects bolsters security in cyberspace.

Comprehensive incident documentation and analysis yields a deep insight into key drivers of incidents and the effectiveness of counter-measures. Enhancing a nations understanding of the threat landscape, its origins, history and causal links with (previous) incidents can improve existing prevention, response and mitigation procedures.

Global information sharing on practices and subject-matter expertise (e.g. the ability to document cyber security incidents, log relevant data, support by sharing existing methodologies and tools, perform analysis on root causes and effects) contributes to the development of more evidence-based cyber security strategies and the alignment of (inter)national response.

5. Cyber Security Exercises

Develop, test and exercise emergency response plans and procedures, domestically and internationally, to ensure that government and non-government collaborators can build trust, prepare for, coordinate effectively and handle crises.

Public and private stakeholders may develop, facilitate, and participate in cyber security exercises. Cyber security exercises can help train and test realistic scenarios on crisis management processes and structures, contingency plans, and communications with all relevant stakeholders on a national, international, regional or local level. All exercises should be evaluated, and recommendations followed up.

[5] The term CSIRT is used as placeholder for many related response capacities such as 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.

The capacity to regularly perform national cyber security exercises may require the participation of cyber security response teams (CSIRTs), national critical infrastructure, private sector, and other national and international (government) agencies/stakeholders. The capacity to organize joint cyber security exercises help to: (1) support and strengthen national CSIRTs in their coordination role, (2) enhance awareness, (3) tests information sharing mechanisms, and (4) brings CII operators in closer connection with the public sector.

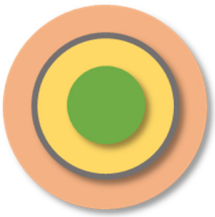
6. Critical Information Infrastructure Protection

Identify and protect national critical information infrastructure sectors.

Raising awareness on the importance of critical information infrastructure protection for governmental and non-governmental stakeholders is important. A NCSS may include a strategy for critical information infrastructure protection (CIIP). Key elements of such a strategy may include the identification of critical information infrastructure (CII) and the organizational structure and processes related to CIIP. The identification and protection of national CII raises the level of resilience against cyber security-related risk.

CIIP is often a joint responsibility of public and private entities, because much of a nation's CII is owned by private companies. Stakeholders with CIIP experience may bring good practices forward to other nations starting with CIIP. Nations with cross-border CII should approach CIIP collaboratively.

THEME: CYBERCRIME



The transnational nature of cyberspace illustrates the need for more effective laws and regulatory frameworks. Cybercrime and computer security laws and regulations enable law enforcement as well as technical and judiciary communities to effectively investigate and deter cyber threats. The objective is a safer and more secure cyberspace in which national and international stakeholders are protected from cybercrime and other cyber security threats, supporting overall trust in the system and enabling societies to take advantage of the economic opportunities afforded by ICT.

7. Legal Frameworks

Enact and enforce a comprehensive set of laws, guidelines, policies and programmes relating to cybercrime in line with existing international standards that allow for effective international cooperation, such as the Budapest Convention on Cybercrime..

The global community should actively disseminate practices and experiences on maintaining, modernizing and harmonizing legal and regulatory frameworks to effectively deter cyber risk and enable chances for economic development. This requires leveraging expertise from government, academia, non-profit

organizations and the private sector to identify and agree upon base-line criminal and procedural law and regulations.

Nations in a region or the same language-group could form judicial expert groups. These groups may utilize internationally recognized best practices such as the Budapest Convention on Cybercrime in combination with regional or multilateral principles, conventions and directives in developing a national and/or regional legal and regulatory cyber security or computer security framework.

8. Law enforcement in cyberspace

Modernize and strengthen criminal justice systems to deal with cybercrime and crimes involving electronic evidence, including the effective prevention, detection, investigation, prosecution and adjudication of such crimes in all their forms.

Given the transnational nature of cybercrime, law enforcement agencies strongly depend on international cooperation to operate successfully. Key mechanisms include efficient mutual legal assistance as well as a strong operational capacity. Trained law enforcement officers, cyber forensics tooling and expertise, and well-trained public prosecutors and judges can bolster the capability and capacities to effectively administer justice in relation to digital crimes.

Nations and international organizations can contribute to the expansion and strengthening of mutual legal assistance initiatives and schemes (e.g. the Harare scheme, Budapest Convention on Cybercrime). They should coordinate international cooperation on developing standards for training of law enforcement and justice systems capable of deterring, investigating and prosecuting cybercrime.

THEME: CYBER SECURITY CULTURE & SKILLS

Cyber security education and training programs can generate skilled workforces, informed citizens, more secure products and services, and a higher degree of societal awareness. In turn, they can foster economic and social development and address the critical questions of a gap in a cybersecurity workforce experienced across the world.

9. Cyber Security Awareness

Promote comprehensive awareness across stakeholders of cyber-related threats and empower the population with the knowledge, skills and sense of shared responsibility to practice safe and informed behaviours in the use of ICTs.

Cyber security awareness raising can promote foundational understandings of cyber threats and risk, cyber hygiene, and other appropriate response options. It informs citizens about best practices and proactive measures when confronted with cyber risks.

Nations should promote cyber awareness of cyber-related threats among the public, companies and government employees. To streamline and facilitate national cyber security awareness campaigns a

worldwide repository (or repositories) should be developed for good practices, expertise and materials. Such a repository can help increase in the number and quality of national cyber security awareness campaigns. Repositories such as these should be maintained and updated to reflect new technological developments, tools, resources and insights.

10. Education and Training

Leverage expertise from all stakeholders to generate a workforce with the cyber security skills employers require.

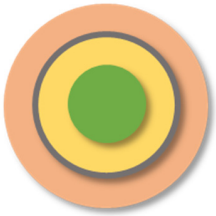
There is a substantial and growing need to develop a skilled cyber security workforce to increase a nation's readiness to respond to threats and adapt to changes in technology. Nations should leverage expertise from government, academia, non-profit organizations and the private sector to generate (e.g. to define, train, certify and position) a workforce with the cyber security skills employers need. The global community should aim to provide best practices, tools, and materials for cyber security programs.

Cyber security education can be improved by the development of dedicated cyber security curricula, education- and awareness-raising materials, streamlining the applicability of degrees, and mutual recognition of certifications. While developing this capacity, attention should be paid to regional differences and the basic competencies and skills that are required but not often included in formal training.

Training refers to knowledge and competences acquired after primary, secondary and higher education. Training focuses on achieving and maintaining specific skills that should be developed, and applied practically to improve performance, sustainability, and/or productivity. Shared training and education materials are preferably licensed through Creative Commons, to facilitate translation and adaption to the local need of nations.

THEME: CYBER SECURITY STANDARDS

Cyber security standards developed through an international multistakeholder process can provide government bodies, sectors and businesses with an established, documented set of practices and a common approach to manage cyber security.



11. Standards

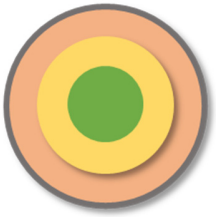
Promote and implement effective cyber security standards and best practices for government and private sector, in line with existing internationally recognised best practices

The promotion and implementation of international standards helps enhance security and stability in cyberspace. The use of standards (1) facilitates the sharing of well-established documented body of knowledge and experiences, (2) enhances cooperation, mutual understanding, and information exchange, and (3) helps to create dialogue on different national and institutional approaches.

The global community should work towards establishment and adoption of international standards that respect fundamental differences among stakeholders, as well as highlight commonalities and agreements. The focus of this capacity can be international, regional, or sectorial and should be the result of a collective effort by all relevant stakeholders and benefit from sharing of online tools and good practice experiences.

CROSSCUTTING CAPACITIES

This theme concerns cross-cutting capacities that strengthen the organization and implementation of cyber capacity building.



International collaboration networks can assist nations in exchanging experiences, harmonizing efforts and building mutual trust amongst stakeholders. Moreover, international collaboration networks may help to bring down regional and sectorial silos and reduce the learning curve for many nations whose populations is now gaining access to the internet. There are many established and emerging international networks that address cyberspace issues, with varying formats and purpose.

Information sharing can enhance cyber security defenses and responses, limit damage resulting from a certain cyber incident, increase situational awareness and transparency, and foster mutual trust. The global community should therefore recognize the need to (a) collaboratively build effective information sharing channels, (b) share good practices, (c) develop theories and concepts for trusted information sharing between various stakeholders and communities, and (d) promote the development of supporting tools.

Research and development (R&D) in cyber security serves as an engine for innovation and a thriving and prosperous digital economy**.** Investment in and strategic focus on R&D can (a) reduce cyber security risks in products and services; (b) improve the efficiency of incident response teams and mechanisms; and (c) enhance incident investigations (e.g. forensics) and prosecution capabilities.

Focussing on ***resource capacities*** is critical in national, regional and global contexts. Cyber capacity building in the end requires man-hours, expertise and materials, which translates into costs. The capacity to manage and request funding are activities that strengthen cyber capacity building globally. In addition, a dedicated pool of experts is needed at both local, regional and global levels. Making use of available expertise in a way that is sensible to national culture, organizational structure and the nation's needs, increases efficiency, speeds-up cyber capacity building in nations, and reduces the need to 'reinvent the wheel'.

3. NEXT STEPS

The GACCB aims to provide guidance to the GFCE community and other actors on how to engage in international cyber capacity building efforts. The GACCB identifies key themes and associated topics for capacity building, and includes a non-exhaustive list of good practices.

The GFCE will draft an action plan for the implementation of the GACCB, with specific attention paid to:

- Securing funding – as funding is scarce, investments need to be efficient, effective and sustainable
- Improving knowledge and information sharing – since the ability to share information in an efficient and timely manner is important for enhancing global cyber capacity building.
- Sharing good (or best) practices – since they reflect proven techniques, methods, or processes.
- Building a pool of expertise – since making use of available expertise speeds up cyber capacity building and reduces the need to 'reinvent wheels'.

At the 2018 GFCE annual meeting, the GFCE community will present an action plan on the implementation of the GACCB. The subsequent GCCS will be used to take stock on the progress that has been made on the implementation of the GACCB.

The GFCE Secretariat will have a coordinating, facilitating and monitoring role in this process.

ANNEX 1: GUIDING PRINCIPLES FOR GLOBAL CYBER CAPACITY BUILDING

The Fourth High Level Forum on Aid Effectiveness (Busan, Republic of Korea, 29 November to 1 December 2011) articulated a number of principles for effective development cooperation in the *Busan Partnership for Effective Development Cooperation*.[6] The following guiding principles for global cyber capacity building are derived from the Busan outcomes, and adapted to the cyber capacity building context.

1. Inclusive partnerships and shared responsibility: effective cyber capacity building requires cooperation across nations, including various stakeholders, and at different levels

Due to the complex and fast-developing nature of cyber challenges, strengthening cyber capacity, expertise, and resources is a global effort. It must include all nations, regardless of their level of development, and all relevant stakeholders, at various levels, across and within nations. Inclusive partnerships must be based on openness, trust, and mutual respect and learning, recognising the different and complementary roles of actors. The high level of cyber interconnectedness means that organisations and citizens of all nations are collectively responsible for a safe and secure cyberspace.

2. Ownership: partner nations need to take ownership of capacity building priorities

Each nation needs to determine its own capacity building priorities, based on country-specific situations and needs. For a development process to be effective and sustainable, it must be owned and led by the appropriate entity, whether this is the national government, a specific institution, or a local organization.

3. Sustainability: obtaining sustainable impact should be the driving force for cyber capacity building

Cyber capacity building initiatives require a comprehensive and systematic approach that includes multiple levels and dimensions (technical, human, organizational, governmental, and legal aspects). Capacity building activities should recognise and build on existing capacities, and focus on soft capacities as well as hard capacities. These approaches will help ensure that cyber capacities get embedded in their target environment and are effective, and sustainable.

4. Trust, transparency and accountability: transparency and accountability help establish trust, which is necessary for effective cooperation

Trust is a necessary component for effective cooperation; and cooperation is essential for global cyber capacity building (Principle 1). However, trust may be difficult to establish when securing cyberspace involves sharing sensitive data and disclosing vulnerabilities. Trust can be built through transparency and accountability. The global community should work towards a safe environment for sharing expertise, resources, and unique achievements and innovations, while recognising individual interests.

[6] http://www.oecd.org/dac/effectiveness/49650173.pdf

ANNEX 2: REFERENCE TO PRACTICES

A practice is an agreement that standardises or prescribes an 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.[7] The GFCE community expressed the need to have good practices available which make duplication of efforts efficient and reduces the risk of making avoidable errors.

This table refers to already developed GFCE good practice documents supporting cyber capacity building.

CCB Topic	Good Practices
1. National Cyber Security Strategy[8]	
2. National Capacity Assessments	Assess national cybersecurity capacity using the maturity model #MaturityModel
	Cybercrime and cyber security trends in Africa (Report, 2016)
3. National Computer Security Incident Response	Global Good Practices: National Computer Security Incident Response Teams (CSIRTs)
	Best Practices for Establishing a National CSIRT (Guidebook, 2016)
4. Incident capture and analytics	Establish a clearinghouse for gathering systemic risk conditions data in global networks #ClearingHouse
	Produce and present trusted metrics about systemic risk conditions #Healthmetrics
	Assist with cyber-risk mitigation and keep score of successes #ScoreKeeping
5. Cyber Security Exercises[9]	
6. Critical Information Infrastructure Protection	Global Good Practices: Critical Information Infrastructure Protection (CIIP)
	The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers
	Companion Document to the GFCE-MERIDIAN Good Practices Guide on CIIP
7. Legal Frameworks	Global Good Practices: Coordinated Vulnerability Disclosure (CVD)
	Stimulate local ownership of capacity development programmes

[7] 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.

[8] In the process of becoming a GFCE initiative

[9] In the process of becoming a GFCE initiative

8. Law enforcement in cyberspace	through National Project Teams #NationalTeam
	Enhance capacity building outreach through regional hubs #RegionalHubs
	Free available decryption tools for some of the existing ransomware families
	Prevention Advice: How to prevent a ransomware attack?
9. Cyber Security Awareness	Align national campaigns #Campaign
	Focus awareness-building through a cybersecurity Awareness Month #Month
	Cybersecurity Awareness Campaign Toolkit (Toolkit, 2015)
10. Education and Training[10]	
11. Standards	Global Good Practices: Internet infrastructures
	Establish a national multistakeholder platform to promote standards #MSPlatform
	Create a website for testing standards-compliance #TestingTool

The GFCE website (www.thegfce.com) contains two portals with valuable information regarding cyber capacity building:

- The Cybersecurity Capacity Portal. This portal gives a global overview of cyber capacity building initiatives (https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/gfce)
- The GFCE cyber monitor. This monitor gives an overview of valuable cyber security information per nation (https://dwh.hcss.nl/apps/gfce_cyber_monitor/)

[10] In the process of becoming a GFCE initiative