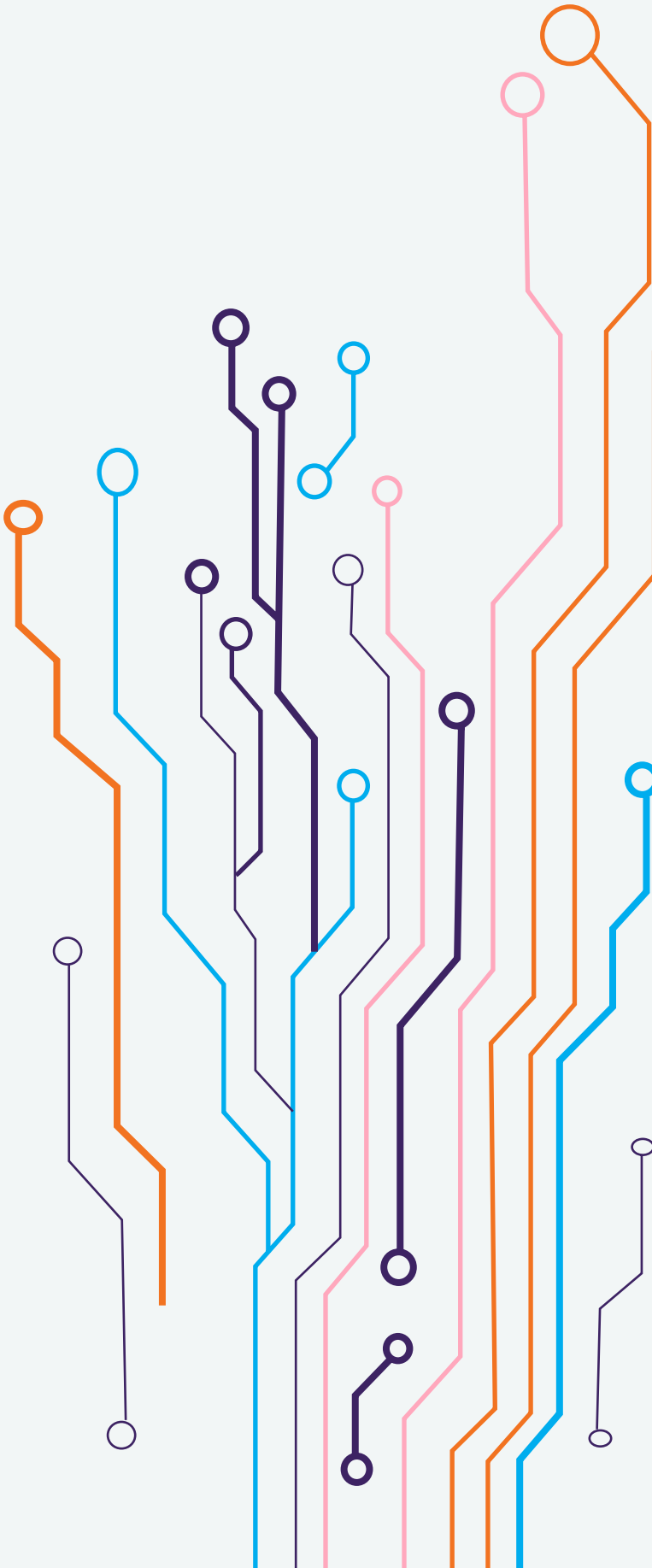
GFCE
Global Forum on Cyber Expertise

THE GLOBAL CYBER CAPACITY BUILDING RESEARCH AGENDA 2021



Foreword

The Global Cyber Capacity Building (CCB) Research Agenda is a new tool developed for and by the GFCE Community. The overarching aim of the Research Agenda is to help the capacity building community design and run more effective projects by identifying knowledge gaps and filling gaps through research.

While the goal for 2020 was to test the first development of the Research Agenda mechanism by running two (2) pilot projects, an opportunity arose to present a draft Research Agenda at the GFCE Annual V-Meeting 2020 on 24 and 25 November. Therefore, between October and November, the GFCE Working Groups and Task Forces, with the support of the Research Committee, identified a total of fifteen (15) research ideas for the draft Research Agenda.

Over half the Community participated in the agenda-setting exercise to determine the prioritization of the research ideas, considering the following questions:

- Is it clear how this research project relates to cyber capacity building?
- Will this research project benefit the GFCE Community and the wider cyber capacity building community?
- Does research like this already exist and is this duplicative of existing efforts?
- How significant is the expected outcome or research output (based on its objectives)?

If you are interested in funding or supporting the GFCE's research efforts, please get in touch with the GFCE Secretariat.

GFCE

Table of Contents

Draft Global CCB Research Agenda 2021 Prioritized List

1) **Developing cyber skills amongst young people**
   What is the presence of digital skills and specifically cyber security skills, in national curricula/extra-curricular activities in 5-23 education?

2) **Training National CSIRTs in low-income countries**
   What are the affordable individual, team, and group training resources, organizational models, and technical tools available to support the development of CSIRTs in low-income countries, and how could a menu of these resources be configured/tailored and applied in an implementation framework to develop and increase the capabilities and maturity of low-income CSIRTs?

3) **Cyber diplomacy gaps analysis**
   What tools exist that, if used, could improve the practice of cyber diplomacy? What are the tools/trainings/support that could, if developed, enhance the delivery of cyber diplomacy?

4) **Implementation of the 11 2015 UN GGE norms of responsible state cyber behavior** *What are the most relevant examples of the implementation of responsible State behavior in cyber-space in terms of 2015 UNGGE norms at the national level? What resources are available to support the implementation of the norms at a national level? What additional information can support the implementation of the norms?*

5) **Raising Cybersecurity awareness amongst SMEs**
   How do you maximise impact of SME Cybersecurity awareness through tailoring for the local context?

6) **Comparing effectiveness of cyber capacity building initiatives**
   What determines cyber capacity initiatives' success in preventing malicious cyberattacks?

7) **Impact of national cybersecurity capacity assessments on NCS development and implementation**
   What is the impact of National Cybersecurity Capacity Assessments on NCS Development and implementation?

Draft Global CCB Research Agenda 2021 Prioritized List

8) **Mapping Exercise on Capacity Building for Cyber Norms**
   Understand the extent to which countries have implemented the 11 2015 Norms of Behaviour in Cyberspace.

9) **Identifying indicators of CIIP maturity**
   How have developed countries implemented CIIP strategies and policies, and what are the best practices for implementation and measuring success?

10) **Interplay between cybersecurity and trade**
    What are the cyber norms and capacity building needs emerging from FTAs and multilateral negotiations on digital trade?

11) **Building an Academic Cyber Capacity Building Network**
    What is the feasibility of establishing an academic CCB network in the South East Asia region?

12) **Managing the relationship between national CSIRTs and sectoral CSIRTs**
    This study will focus on the development of a framework on how to manage the relationship between national CSIRTs and sectoral CSIRTs. The aim is to develop a framework that encourages cooperation between both types of CSIRT whilst avoiding overlap in roles and responsibilities.

13) **LATAM countries' efforts on cybercrime legislation**
    What lessons can be learnt from the recent efforts of LATAM countries in developing and adapting procedural and substantive cybercrime legislation?

14) **Identifying important contextual factors that shape and drive different national approaches to CIIP**
    What are the design factors and set of best practices for the development and implementation of CIIP policies and programs around the world given certain key factors?

15) **The role of the private sector in CSIRT capacity building**
    This study will focus on the importance of multi-stakeholder cooperation regarding CSIRT capacity building, more specifically on the role of the private sector.

Working Group A

Cyber Security Policy & Strategy

01	02	03	04
05	06	07	08
09	10	11	12
13	14	15	

Working Group A
Cyber Security Policy & Strategy

03

Task Force CBMs, Norms Implementation and Cyberdiplomacy:

Cyber diplomacy gaps analysis

- *What tools exist that, if used, could improve the practice of cyber diplomacy?*
- *What are the tools/trainings/support that could, if developed, enhance the delivery of cyber diplomacy?*

Knowledge gap

It can be hard for diplomats (especially from smaller and developing countries) to follow and fully contribute to international discussions on cybersecurity because of a lack of information, expertise, or simply available personnel. The discussion requires understanding of international law, technology, as well as foreign affairs.

There is, therefore, an opportunity to help build capacity within the diplomatic community, to help both improve the overall quality of the dialogue and to ensure that countries can fully benefit from the international discussions. The first step in that process need to be a survey of the community engaged in cyber diplomacy a better understand of what tools, training, and support are available (even if they are widely used), and what practice could be drawn from other fields of diplomacy.

04

Task Force CBMs, Norms Implementation and Cyberdiplomacy:

Implementation of the 11 2015 UN GGE norms of responsible state cyber behavior

- *What are the most relevant examples of the implementation of responsible State behavior in cyber-space in terms of 2015 UNGGE norms at the national level?*
- *What resources are available to support the implementation of the norms at a national level?*
- *What additional information can support the implementation of the norms?*

Knowledge gap

The 11 2015 UNGGE norms of responsible state behavior in cyberspace provide an important basis on which states should develop their cybersecurity policies and strategies. However, it has been reported that there is an understanding gap between what the norms say and what they mean in practice. By highlighting concrete real-world examples of where the norms have been implemented with a certain degree of success, there is an opportunity to encourage better understanding and accelerating broad adoption.

Working Group A
Cyber Security Policy & Strategy

06

Task Force Strategy & Assessments:

Comparing effectiveness of cyber capacity building initiatives

What determines cyber capacity initiatives' success in preventing malicious cyberattacks?

Knowledge gap

Governments now rely on a rich body of recommendations and guidelines addressing how to develop cyber capacity building initiatives. However, we have little evidence on what determines effectiveness. This research will fill this gap by providing empirical evidence on the efficiency of cyber capacity building strategies.

07

Task Force Strategy & Assessments:

Impact of national cybersecurity capacity assessments on NCS development and implementation

What is the impact of National Cybersecurity Capacity Assessments on NCS Development and implementation?

Knowledge gap

Currently, little is known on the impact of cybersecurity maturity assessments on cybersecurity development in countries. One of the main objectives of the cybersecurity maturity assessments is to identify evidence-based and informed recommendations to improve the posture of countries in terms of cybersecurity capacity, but we have little evidence on how countries take into account these recommendations.

Working Group A
Cyber Security Policy & Strategy

08

Task Force CBMs, Norms Implementation and Cyberdiplomacy:

Mapping exercise on capacity building for cyber norms

To what extent have countries implemented the 11 2015 norms of Responsible State Behavior in Cyberspace?

Knowledge gap

The 2015 UN GGE set out 11 Norms of Responsible Behavior in Cyberspace. While norms are essential for cyber stability, there is a lack of good information on the extent to which countries have taken action to implement those norms. At the very least we should seek to understand that from within the GFCE Member countries.

At the same time, there are a range of organizations (including governmental organizations, private companies and non-profits) who offer countries help in that implementation effort. There is currently no comprehensive mapping of that community either. At the very least we should understand the available resources from within the GFCE community.

10

Task Force Strategy & Assessments:

Interplay between cybersecurity and trade

What are the cyber norms and capacity building needs emerging from FTAs and multilateral negotiations on digital trade?

Knowledge gap

On one hand, cybersecurity is regarded as a precondition for the growth of digital trade. Some cybersecurity-related norms are emerging under the umbrella of trade negotiations: several free-trade agreements (FTAs) and the current plurilateral negotiations on e-commerce taking place at the WTO encompass provisions related to cybersecurity. Many of them mention the need for cyber cooperation and capacity building. On the other hand, the introduction of trade restrictions motivated by concerns related to cybersecurity and national security is fragmenting global value chains. This is putting an increasing pressure on the multilateral trading system and on trade negotiators, who do not necessarily have expertise on cyber issues and are frequently not fully aware of existing mechanisms of cyber cooperation outside the trading system. Collaboration is further complicated by the fact that trade negotiations are usually not transparent and not open to the involvement of non-governmental actors.
The research would offer elements to strengthen the whole-of-government and multi-stakeholder approaches to cybersecurity, especially when it comes to promoting the coherence between security and trade objectives.

Working Group B

Cyber Incident Management (CIM) & Critical Information Infrastructure Protection (CIIP)

01	02	03	04
05	06	07	08
09	10	11	12
13	14	15	

Working Group B
CIM and CIIP

02

Task Force Cyber Incident Management:

Training national CSIRTS in low income countries

What are the affordable individual, team, and group training resources, organizational models, and technical tools available to support the development of CSIRTs in low-income countries, and how could a menu of these resources be configured/tailored and applied in an implementation framework to develop and increase the capabilities and maturity of low-income CSIRTs?

Knowledge gap

Technically competent national CSIRTs are needed to address the increasing risks of technology to a nation by increasing society's awareness of cyber risks, providing advice to governments on appropriate risk mitigation policies, responding to incidents, and helping all citizens and businesses to operate more safely in cyberspace. Many low-income countries do not have, and cannot afford to train, equip, and operate viable national CSIRTs that are capable of performing the essential CSIRT services described by the FIRST organization. No compendium of affordable and achievable training, organizational and technical resources, that can be applied under an implementation framework tailored to address a variety of low-income country CSIRT development needs currently exists. Such a product would be a useful guide for developing national CSIRTs and increasing countries' ability to deal with cyber security issues. This product would also strengthen regional CSIRT ecosystems. This research effort should also ensure that this compendium of resources and framework for implementation is tailorable to multiple circumstances and is not a 'one-size-fits-all' solution.

09

Task Force Critical Information Infrastructure Protection:

Identifying indicators of CIIP maturity

How have developed countries implemented CIIP strategies and policies, and what are the best practices for implementation and measuring success?

Knowledge gap

The capacity building community needs to better understand the methodologies for CIIP strategy and policy implementation focusing on the practical aspects of incentivization, investment strategies, organization structures, coordination mechanisms, regulation, public/private partnerships, etc.,

Therefore, the target of this research is to study countries who have already identified and addressed their CIIP to identify indicators.

Working Group B
CIM & CIIP

12

Task Force Cyber Incident Management:

Managing the Relationship between national CSIRTS and sectoral CSIRTs

This study will focus on the development of a framework on how to manage the relationship between national CSIRTs and sectoral CSIRTs. The aim is to develop a framework that encourages cooperation between both types of CSIRT whilst avoiding overlap in roles and responsibilities.

Knowledge gap

Cooperation between national CSIRTs and sectoral CSIRTs is essential. There is existing research on cooperation between national and sectoral CSIRTs, but no formal framework or listing of observed best practices exists that CSIRTs could apply to develop such cooperation.

-

14

Task Force Critical Information Infrastructure Protection:

National approaches to CIIP

What are the design factors and set of best practices for the development and implementation of CIIP policies and programs around the world given certain key factors?

Knowledge gap

Countries and organizations have different approaches to Critical Information Infrastructure Protection (CIIP), starting in how CII is identified to how countries and organizations implement protection measures. There is a need to improve the capacity building community's understanding of the context in which national CIIP policies and strategies are developed and implemented across a representative swath of developed and developing countries to inform the development of CIIP capacity building efforts in nations and areas where they are lacking. This knowledge gap also needs to be filled as a potential foundation for the development of a CIIP maturity scale.

Therefore, the target of this research is to study countries who are still in the process of identifying and addressing their CIIP.

Working Group B
CIM & CIIP

15

Task Force Cyber Incident Management:

Role of the private sector in CSIRT capacity building

This study will focus on the importance of multi-stakeholder cooperation regarding CSIRT capacity building, more specifically on the role of the private sector. The aim of the study is to examine how private sector entities can support CSIRT capacity building.

Knowledge gap

Countries and organizations have different approaches to CSIRT capacity building. It is essential for the process that the private sector is involved, as well as other stakeholders. However, it is not always clear how to involve all relevant stakeholders in CSIRT capacity building activities. In particular private sector organizations are not always brought in early, leading to potential miscommunication once the CSIRT is active.

While it is widely accepted that CSIRT development needs to involve a wide stakeholder community, few practical approaches are available that a CSIRT can pick up to actively engage and work with private sector.

-

Working Group C

Cybercrime

01	02	03	04
05	06	07	08
09	10	11	12
13	14	15	

Working Group C

Cybercrime

11

Building an academic cyber capacity building network

What is the feasibility of establishing an academic CCB network in the South East Asia region?

Knowledge gap

Youth is the future. In order to implement the goals of capacity building and the GFCE in a sustainable way it is essential to involve young people. Given the complexity of cyber issues, this is typically interesting for universities in developing countries.

University partnerships are quite common worldwide, and the research proposal stems from existing informal partnerships established in Thailand, Vietnam, India and Malaysia amongst others. This project examines the feasibility of further aligning and strengthening these partnerships towards a sustainable academic network for cyber capacity building with an emphasis on Southeast Asia.

13

LATAM countries' efforts on cybercrime legislation

What lessons can be learnt from the recent efforts of LATAM countries in developing and adapting procedural and substantive cybercrime legislation?

Knowledge gap

Whilst many Latin American (LATAM) countries have ratified international treaties on cybercrime, few have fully adapted their current legislation to comply with recommendations.

Given these developments, research is needed to look at what challenges LATAM countries are experiencing in adapting their procedural and substantive legislation and what lessons can be learned for other countries in adapting their own legislation; and how are these affected by regional or local context.

Working Group D

Cyber Security Culture & Skills

01	02	03	04
05	06	07	08
09	10	11	12
13	14	15	

Working Group D

Cyber Security Culture & Skills

01

Developing cyber skills amongst young people

What is the presence of digital skills and specifically cyber security skills, in national curricula/extra-curricular activities in 5 – 23 education?

Knowledge gap

Cyber skills are specialist digital skills but in many countries the education system is not fully-equipped to provide students with the necessary digital skills at sufficient depth and scale.

The objective for a number of countries is to fund initiatives that create and develop a sustainable pipeline for cyber security talent both now and in the future to meet the growing global need for individuals to possess cyber skills.

Many countries are working to develop cyber skills amongst young people. However, many countries are not aware of what other countries are doing in this space and are unable to learn from best practice.

05

Raising cybersecurity awareness amongst SMEs

How do you maximize impact of SME cybersecurity awareness through tailoring for the local context?

Knowledge gap

COVID-19 restrictions have accelerated trading SME reliance on digital platforms for trade with little thought to cybersecurity. Good practices do exist to assist SMEs to trade more securely, however, more often than not, people attempt to transplant practices from one context to the next in the hope they will work just as well.

Tailoring resources to the SME community and local context will help ensure the greatest chance of adoption and increasing cyber resilience amongst this significant group. Sharing lessons learned and methodologies used for cyber awareness initiatives in this space will help improve effectiveness of future efforts.

Annex I:
Research idea proposals

This Annex contains fifteen (15) research idea proposals that were submitted for the Draft Global CCB Research Agenda 2021.

Contents

Working Group	WG A, Task Force Strategy & Assessments
Research Topic	**Impact of National Cybersecurity Capacity Assessments on NCS Development and implementation** We propose to assess/understand the impact of national cybersecurity capacity reviews based on the Cybersecurity Capacity Maturity Model for Nations (CMM), and specifically of its Dimension 1 "Cybersecurity and Policy", on national cybersecurity strategy (NCS) development and on the implementation of recommendations from the CMM. The research project would look at a set of countries where the CMM was conducted (from different regions and with different development status) and research whether the recommendations on cybersecurity strategy were taken forward by these countries. The aim is to identify lessons can be learnt both on the effectiveness of the CMM in the identification of evidence-based, informed, and feasible recommendations, and on what additional support/capacity building countries need to effectively implement the recommendations. This research can be conducted on in a comparative way, either by the constellation of regional cybersecurity capacity centers (Global Cybersecurity Capacity Centre (GCSCC), Oceania Cyber Security Centre (OCSC), and Cybersecurity Capacity Centre for Southern Africa (C3SA)) themselves or with the support of an external research organization.
Research Question	What is the impact of National Cybersecurity Capacity Assessments on NCS Development and implementation?
Problem statement/Knowledge gap	Currently, little is known on the impact of cybersecurity maturity assessments on cybersecurity development in countries. One of the main objectives of the cybersecurity maturity assessments is to identify evidence-based and informed recommendations to improve the posture of countries in terms of cybersecurity capacity, but we have little evidence on how countries take into account these recommendations.
Research objectives	The main research objective is to understand whether countries take into account recommendations put forward by the cybersecurity maturity assessments. The secondary objectives are: - Find out how countries prioritize recommendations and what the factors influence the prioritization. - Understand what are the main obstacles to implement cybersecurity maturity assessments' recommendations. - Identify what additional support is needed to implement the recommendations.

Beneficiaries	• Governments would benefit from more clarity how an assessment of cybersecurity capacity and existing gaps can inform and support the NCS process and how it impacts the country's overall cybersecurity posture. • The cybersecurity capacity-building community (beneficiaries, funders and implementers) get a better understanding what needs to be covered by NCS and what works and what doesn't work.

Working Group	WG A, Task Force Strategy & Assessments
Research Topic	The interplay between cybersecurity and trade
Research Question	What are the cyber norms and capacity building needs emerging from FTAs and multilateral negotiations on digital trade?
Problem statement/Knowledge gap	Cybersecurity needs a whole-of-government approach. This is becoming particularly clear with the increasing interplay between cybersecurity and trade. On the one hand, cybersecurity is regarded as a precondition for the growth of digital trade. Some cybersecurity-related norms are emerging under the umbrella of trade negotiations: several free-trade agreements (FTAs) and the current plurilateral negotiations on e-commerce taking place at the WTO encompass provisions related to cybersecurity. Many of them mention the need for cyber cooperation and capacity building. On the other hand, the introduction of trade restrictions motivated by concerns related to cybersecurity and national security is fragmenting global value chains. This is putting an increasing pressure on the multilateral trading system and on trade negotiators, who do not necessarily have expertise on cyber issues and are frequently not fully aware of existing mechanisms of cyber cooperation outside the trading system. Collaboration is further complicated by the fact that trade negotiations are usually not transparent and not open to the involvement of non-governmental actors. The research would offer elements to strengthen the whole-of-government and multi-stakeholder approaches to cybersecurity, especially when it comes to promoting the coherence between security and trade objectives.
Research objectives	Objective: • To investigate cybersecurity-related provisions being included in FTAs and in multilateral negotiations on digital trade and identify emerging trends and norms. Secondary objectives: • To unpack the provisions related to cooperation and capacity building, identifying the specific cyber capacity-building needs of trade actors. • To identify current and potential tensions between promoting security and digital trade objectives that are emerging from cybersecurity-related provisions. • To identify actors and organizations outside the trade environment that could potentially contribute to trade discussions if mechanisms of dialogue are established between the trade and cyber communities.

Beneficiaries	• Cybersecurity actors would benefit from more clarity about how trade norms (approved or under discussion) could potentially impact security. • The cyber capacity-building community would be more aware of CB needs emerging from the intersection between trade and cyber issues. • Trade negotiators and practitioners.

Working Group	WG A, Task Force Strategy & Assessments
Research Topic	**Comparing effectiveness of cyber capacity building**
Research Question	What determines cyber capacity initiatives' success in preventing malicious cyberattacks?
Problem statement/Knowledge gap	Governments now rely on a rich body of recommendations and guidelines addressing how to develop cyber capacity building initiatives. However, we have little evidence on what determines effectiveness. This research will fill this gap by providing empirical evidence on the efficiency of cyber capacity building strategies.
Research objectives	Primary Objectives - Provide empirical evidence of what determines effective cyber capacity building initiatives Secondary Objectives - Compare cyber capacity building implementation globally - Identify best practices and lessons learned that can be exported to other contexts
Beneficiaries	This research will support the work of the Task Force in informing key stakeholders from government, industry and civil society responsible for the implementation of national cybersecurity strategy where to invest their efforts.

Working Group	WG A, Task Force CBMs, Norms Implementation and Cyber Diplomacy
Research Topic	Supporting the implementation of the 11 2015 UN GGE norms of responsible state cyber behavior by publishing a consolidated guide containing examples of where the norms have been implemented in practice*
Research question(s)	Primary question 1) What are the most relevant examples of the implementation of responsible State behavior in cyber-space in terms of 2015 UNGGE norms at the national level? Secondary question 2) What resources are available to support the implementation of the norms at a national level? 3) What additional information can support the implementation of the norms?
Existing work/literature on the topic	UNODA (2017). Civil Society and Disarmament: 2017. https://www.un.org/disarmament/publications/civilsociety/civil-society-and-disarmament-2017/ ASPI (2020). UN Cyber Norms, an explainer. https://www.aspi.org.au/cybernorms IGF BPF Cybersecurity
Problem statement/Knowledge gap	The 11 2015 UNGGE norms of responsible state behavior in cyberspace provide an important basis on which states should develop their cybersecurity policies and strategies. However, it has been reported that there is an understanding gap between what the norms say and what they mean in practice. By highlighting concrete real world examples of where the norms have been implemented with a certain degree of success, there is an opportunity to encourage better understanding and accelerating broad adoption.
Scope of Research and limitations	The project should identify and showcase two to three practical examples of each of the norms in the form of short vignettes/case studies. Examples should be drawn from as wide a geographical spread as possible. The project should also identify and collect resources to help countries implement each of the norms. Additional information may be provided if needed by States to assist them in the implementation of the norms.
Research objectives	Provide a consolidated guide to norms implementation that can be provided to national governments to support implementation of the 11 2015 UNGGE norms of responsible state behavior in cyberspace.
Beneficiaries	This research will support the work of governments (including those participating in the GGE/OEWG discussions, as well as the Task Force in understanding future work in this area.

* This research idea has been chosen as a pilot project and funding has been allocated.

Working Group	WG A, Task Force CBMs, Norms Implementation and Cyber Diplomacy
Research Topic	Cyber diplomacy gaps analysis
Research Question	What tools exist that, if used, could improve the practice of cyber diplomacy? What are the tools/trainings/support that could, if developed, could enhance the delivery of cyber diplomacy?
Problem statement/Knowledge gap	Cyber diplomacy – the practice of diplomacy in support of better cybersecurity in the international system is a new and evolving area of practice. The challenges of cybersecurity are universal, and it is increasingly a topic of discussion and action in various international fora. Nevertheless, it can be hard for diplomats (especially from smaller and poorer countries) to follow and fully contribute to those engagements because of lack of information, expertise, or simply available personnel. The discussion requires understanding of international law, technology, as well as foreign affairs. There is, therefore, an opportunity to help build capacity within the diplomatic community, to help both improve the overall quality of the dialogue and to ensure that countries can fully benefit from the international discussions. The first step in that process need to be a survey of the community engaged in cyber diplomacy a better understand of what tools, training, and support are available (even if they are widely used), and what practice could be drawn from other fields of diplomacy.
Research objectives	Primary objective: • To identify what tool and support are available to support the practice of cyber diplomacy and how widely they are used. • To identify where it would be possible to make existing tools and support more widely available. • To identify, based on best practice in other diplomatic communities or other relevant communities of practice, what tools and services could be made available. Secondary objective: • To identify – where possible – what level of additional resource could make a significant difference to the challenge of creating a knowledgeable and well-informed community of diplomats focused on cyber issues.
Beneficiaries	This research will support the work of the Task Force in understanding what future activity it should do in this area.

Working Group	WG A Task Force CBMs, Norms Implementation and Cyber Diplomacy
Research Topic	Capacity Building for Cyber Norms Mapping Exercise
Research Question	To understand the extent to which countries have implemented the 11 2015 Norms of Behavior in Cyberspace.
Problem statement/Knowledge gap	The 2015 UN GGE set out 11 Norms of Responsible Behavior in Cyberspace. While norms are essential for cyber stability, there is a lack of good information on the extent to which countries have taken action to implement those norms. At the very least we should seek to understand that from within the GFCE Member countries. At the same time, there are a range of organizations (including governmental organizations, private companies and non-profits) who offer countries help in that implementation effort. There is currently no comprehensive mapping of that community either. At the very least we should understand the available resources from within the GFCE community.
Research objectives	Objective: • To identify through a mapping exercise of the implementation of the 2015 GGE cyber norms among the GFCE Member countries. • To identify through a mapping exercise the available resources to support the implementation of cyber norms from within the GFCE community. Secondary objective: • To the extent practical, to identify examples of best practice in the implementation of the 2015 GGE cyber norms from outside GFCE Member countries. • To the extent practical, to identify examples of highly impactful resources to support the implementation of cyber norms from outside the GFCE community.
Beneficiaries	This research will support the work of the Task in understanding what future activity it should do in this area.

Working Group	WG B, Task Force CIM (Cyber Incident Management)
Research Idea	Research is needed to identify a menu of practical, feasible and affordable individual, team, and group training options that increase the maturity and capabilities of national CSIRTs in low- income countries*
Research question(s)	Primary Research Question: What are the affordable individual, team, and group training resources, organizational models, and technical tools available to support the development of CSIRTs in low-income countries, and how could a menu of these resources be configured/tailored and applied in an implementation framework to develop and increase the capabilities and maturity of low-income CSIRTs? Secondary Research Question: What are sound approaches for creating CSIRT training programs for low-income CSIRT individuals and teams that leverage existing best practice cyber security training and education models that identify required skills, knowledge, and abilities, and how can low-income CSIRTs best create personnel pipelines that supporting hiring, training and retaining qualified CSIRT.
Problem statement/Knowledge gap	Many low-income countries seek greater economic, social, and governance development by leveraging ICT capabilities. These capabilities provide significant benefits, but also increase risks to the nation that may stymie development goals, increase national security threats through cyberspace, and threaten the privacy of citizens. Technically competent national CSIRTs are needed to address the increasing risks of technology to a nation by increasing society's awareness of cyber risks, providing advice to governments on appropriate risk mitigation policies, responding to incidents, and helping all citizens and businesses to operate more safely in cyberspace. Many low-income countries do not have, and cannot afford to train, equip, and operate viable national CSIRTs that are capable of performing the essential CSIRT services described by the FIRST organization (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1). No compendium of affordable and achievable training, organizational and technical resources, that can be applied under an implementation framework tailored to address a variety of low-income country CSIRT development needs currently exists. Such a product would be a useful guide for developing national CSIRTs and increasing countries' ability to deal with cyber security issues. This product would also strengthen regional CSIRT ecosystems. This research effort should also ensure that this compendium of resources and framework for implementation is tailorable to multiple circumstances and is not a 'one-size-fits-all' solution.
Research objectives	To provide low-income countries with a practical, affordable, flexible, and achievable workforce training and development methods including a menu of resources mapped to CSIRT organizational, technical, and operational service requirements.

* This research idea has been chosen as a pilot project and funding has been allocated.

Working Group	Working Group B Task Force CIM, Cyber Incident Management
Research Topic	Framework on how to manage the relationship between national CSIRTs and sectoral CSIRTs
Research Question	This study will focus on the development of a framework on how to manage the relationship between national CSIRTs and sectoral CSIRTs. The aim is to develop a framework that encourages cooperation between both types of CSIRT whilst avoiding overlap in roles and responsibilities.
Problem statement/Knowledge gap	Cooperation between national CSIRTs and sectoral CSIRTs is essential. There is existing research on cooperation between national and sectoral CSIRTs, but no formal framework or listing of observed best practices exists that CSIRTs could apply to develop such cooperation.
Research objectives	Objective: • To produce a framework, including best practices and proposed approaches, to encourages cooperation and provide pathways to improve information sharing and collaboration between national CSIRTs and sectoral CSIRTs whilst mitigating potential bottlenecks and overlap in roles and responsibilities.
Beneficiaries	This research will support the work of the Task Force CIM's members in their CSIRT capacity building efforts on how to encourage cooperation between national and sectoral CSIRTs and that they can use in their CSIRT capacity building activities. In particular, the framework can be used by partner states in CSIRT capacity building projects to ensure national CSIRTs are part of an effective CSIRT network within the state.

Working Group	Working Group B Task Force CIM, Cyber Incident Management
Research Topic	The role of the private sector in CSIRT capacity building
Research Question	This study will focus on the importance of multi-stakeholder cooperation regarding CSIRT capacity building, more specifically on the role of the private sector. The aim of the study is to examine how private sector entities can support CSIRT capacity building.
Problem statement/Knowledge gap	Countries and organizations have different approaches to CSIRT capacity building. It is essential for the process that the private sector is involved, as well as other stakeholders. However, it is not always clear how to involve all relevant stakeholders in CSIRT capacity building activities. In particular private sector organizations are not always brought in early, leading to potential miscommunication once the CSIRT is active. While it is widely accepted that CSIRT development needs to involve a wide stakeholder community, few practical approaches are available that a CSIRT can pick up to actively engage and work with private sector.
Research objectives	Objective: To produce a study that • Identifies and catalogues existing private sector capacity building activities, capabilities, and venues. • Provides recommendations on the feasibility and potential approaches toward increasing the private sector in CSIRT capacity building activities focusing on the potential best practices and unique capabilities they have contributed toward capacity building, as well as identifying potential capacity building needs the private sector may be best suited to meet.
Beneficiaries	This research will support the work of the Task Force CIM's members in their CSIRT capacity building efforts on how to increase private sector involvement. In particular, the outcome of this research will lead to CSIRTs being better able to partner with their private sector counterparts, and leverage their expertise as they grow their capacity.

Working Group	WG B, Task Force CIIP (Critical Information Infrastructure Protection)
Research Topic	Identifying important contextual factors that shape and drive different national approaches to CIIP
Research Question	A foundational study of the different aspects of how nations develop and implement CIIP policies and programs around the world to address the question of what are the design factors and set of best practices for the development and implementation of CIIP policies and programs given certain key factors. This study will identify key national factors (constitutions and national policies, culture, governance and strategies, economic system, risk/security profiles, geography and cross-border shared infrastructure, etc.) that shape those policies and approaches to identify commonalities and differences in key contextual factors.
Problem statement/Knowledge gap	Countries and organizations have different approaches to Critical Information Infrastructure Protection (CIIP), starting in how CII is identified to how countries and organizations implement protection measures. There is a need to improve the capacity building community's understanding of the context in which national CIIP policies and strategies are developed and implemented across a representative swath of developed and developing countries to inform the development of CIIP capacity building efforts in nations and areas where they are lacking. This knowledge gap also needs to be filled as a potential foundation for the development of a CIIP maturity scale. Therefore, the target of this research is to study countries who are still in the process of identifying and addressing their CIIP.
Research objectives	To produce a report that identifies the key factors that shape the development and implementation of national CIIP policies and strategies, identifying best practices if possible, and informing the development of capacity building tools and material that supports the efforts of nations seeking to implement a CIIP effort.
Beneficiaries	This research will support the work of the Task Force CIIP in their research efforts that will support creating maturity model derived on the context from this study as well as from another proposed study on identifying indicators of CIIP maturity by identifying methodologies. Therefore, the beneficiaries of this research as well as the other research linked to this Task Force is aimed at countries who have only just started identifying their CII, as well could support countries who are revising their CIIP and are looking to learn from other approaches.

Working Group	WG B, Task Force CIIP (Critical Information Infrastructure Protection)
Research Topic	Identifying indicators of CIIP maturity
Research Question	An initial study that identifies probable indicators of CIIP maturity by identifying how developed countries have implemented CIIP strategies and policies to identify best practices for implementation and measuring success.
Problem statement/Knowledge gap	The capacity building community needs to better understand the methodologies for CIIP strategy and policy implementation focusing on the practical aspects of incentivization, investment strategies, organization structures, coordination mechanisms, regulation, public/private partnerships, etc., Therefore, the target of this research is to study countries who have already identified and addressed their CIIP to identify indicators.
Research objectives	Objective: • To inform capacity building efforts in CIIP by identifying potential indicators are of CIIP maturity through an assessment of implementation methodologies that countries have developed to address CIIP, best practices, and measurements of success.
Beneficiaries	This research will support the work of the Task Force CIIP in their research efforts that will support the follow-on creation of a CIIP maturity model and assessment process derived on the context from this study as well as from another proposed study on identifying different approaches to CIIP around the world by identifying factors as culture, governance, etc. Therefore, the beneficiaries of this research as well as the other research linked to this Task Force is aimed at countries that have only just started identifying their CII, as well could support countries who are revising their CIIP and are looking to learn from other approaches. Additionally, this study will inform the development of capacity building approaches, materials, and designs that could assist immature CIIP efforts become more mature.

Working Group	WG C Cybercrime
Research Topic	Building an Academic Cyber Capacity Building Network
Research Question	What is the feasibility of establishing an academic CCB network in the South East Asia region?
Problem statement/Knowledge gap	Youth is the future. In order to implement the goals of capacity building and the GFCE in a sustainable way it is essential to involve young people. Given the complexity of cyber issues, this is typically interesting for universities in developing countries. University partnerships are quite common worldwide and the research proposal stems from existing informal partnerships established in Thailand, Vietnam, India and Malaysia amongst others. This project examines the feasibility of further aligning and strengthening these partnerships towards a sustainable academic network for cyber capacity building with an emphasis on Southeast Asia.
Research objectives	The objective is to actively engage universities and academic institutions in developing countries on state-of-the-art cybercrime and capacity building topics, conducting explorative research to assess the feasibility of establishing an academic network on such topics in South East Asia. An assessment will identify how to make the network operational. In the exploration phase, various topics are discussed, such as, but not limited to, cybercrime. During the exploration, an initial plan for outreach activities will be developed and willingness to participate in the activities within a current informal academic network in South East Asia (especially Myanmar, Vietnam, Thailand and Malaysia).the feasibility of these phases will be tested and further streamlined into a realistic action plan for at least two years. In the next phase, the intention is that as a result of the network activities within those universities, research projects will be started on various cybersecurity topics such as Critical Infrastructures (Information) Protection, CSIRT, Cybercrime and Emergent Technologies. As a result, in-depth expertise is developed and established in these countries, where their research projects can be carried out. The output will be presented in a yearly report, including reporting of progress, opportunities and insights within the relevant GFCE Working Groups. Report that presents the findings based on at least 15 interviews with universities. This report should identify: • Interest to join the network • Relations with the national government

	• Topics of interest from university perspective from short term small student projects up till BSc or MSc graduation projects • Topics of interest from GFCE Working Group C perspective • Recommendations on how this academic network can contribute to GFCE Objectives
Beneficiaries	Academic institutions and universities in South East Asia region

Working Group	WG C Cybercrime
Research Topic	LATAM countries efforts on cybercrime legislation
Research Question	What lessons can be taken from recent efforts of LATAM countries in developing and adapting procedural and substantive cybercrime legislation?
Problem statement/Knowledge gap	Whilst many Latin American (LATAM) countries have ratified international treaties on cybercrime, few have fully adapted their current legislation to comply with recommendations. Given these developments, research is needed to look at what challenges LATAM countries are experiencing in adapting their procedural and substantive legislation and what lessons can be learned for other countries in adapting their own legislation; and how are these affected by regional or local context.

Working Group	WG D Cyber Security Culture & Skills
Research Topic	Raising Cybersecurity awareness amongst SMEs
Research Question	How do organizations maximize impact of SME Cybersecurity awareness for the local context?
Problem statement/Knowledge gap	COVID-19 restrictions have accelerated trading SME reliance on digital platforms for trade with little thought to cybersecurity. Good practices do exist to assist SMEs to trade more securely, however, more often than not, people attempt to transplant practices from one context to the next in the hope they will work just as well. Tailoring resources to the SME community and local context will help ensure the greatest chance of adoption and increasing cyber resilience amongst this significant group. Sharing lessons learned and methodologies used for cyber awareness initiatives in this space will help improve effectiveness of future efforts.
Research objectives	Mapping existing cybersecurity awareness activities focused on SMEs (through a comprehensive survey and analysis), distil key messages across the initiatives. Also, we want to know how the local context is defined by different organizations that are delivering awareness raising activities and gather case-studies on how the messages have been delivered based on their local context.
Beneficiaries	This research will support the work of Working Group D and its members. In addition, the findings will assist Cyber awareness implementers to leverage global experience to develop more effective initiatives. Ultimately SME's will benefit through more accessible and locally relevant cybersecurity guidance and advice. The findings will enable us to begin to understand the different contexts organizations find themselves in and how they go about change. As organizations offer up what they deem a successful initiative we will also begin to get a picture of what people see as success.

Working Group	WG D Cyber Security Culture & Skills
Research Topic	Developing cyber skills amongst young people
Research Question	What is the presence of digital skills and specifically cyber security skills, in national curricula/extracurricular activities in 5-23 education?
Problem statement/Knowledge gap	Cyber skills are specialist digital skills but in many countries the education system is not fully-equipped to provide students with the necessary digital skills at sufficient depth and scale. The objective for a number of countries is to fund initiatives that create and develop a sustainable pipeline for cyber security talent both now and in the future to meet the growing global need for individuals to possess cyber skills. Many countries are working to develop cyber skills amongst young people. However, many countries are not aware of what other countries are doing in this space and are unable to learn from best practice.
Research objectives	The primary objective of this research project is to understand how countries are developing a sustainable talent pipeline of cyber security professionals, from school age. The secondary objective of this proposal is to engage with as many countries as possible to understand what they are doing in this space.
Beneficiaries	The working group will be interested and will benefit from understanding best practice and transferable measures which can be taken in their countries. The wider forum will also be interested and will benefit from understanding best practice and transferable measures which can be taken in their countries as countries interested in this topic extend outside of the working group.