THE GLOBAL CYBER CAPACITY BUILDING RESEARCH AGENDA 2022 - 2023

GFCE
Global Forum on Cyber Expertise

Foreword

The Global Cyber Capacity Building (CCB) Research Agenda is a tool designed and developed by the GFCE. 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.

The mechanism was tested through the pilot Research Agenda 2021, with funding allocated to four (4) research projects that were prioritized by the Community. Based on the lessons learned over the past year, the research agenda process has been simplified and refined, and a new draft Research Agenda will be presented at the GFCE Annual V-Meeting on 30 November – 2 December.

Between October and November 2021, the GFCE Working Groups and Task Forces identified a total of **twenty-four (24)** research ideas for the Research Agenda 2022 – 2023. Through a prioritization exercise within the Working Groups, members had the opportunity to vote on the research topic(s) that they felt should be prioritized for funding. When determining which research topic to prioritize, members were invited to consider 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. The GFCE wishes to acknowledge the Research Committee 2020 – 2022 members for their tireless support throughout the process: Amreesh Phokeer, Andrea Calderaro, Carolina Aguerre, Elina Noor, Emmanuella Darkwah, Enrico Calandro (Chair), Klée Aiken, Lia Hernández, Peter Cassidy, Richard Harris.

Disclaimer

GFCE

Table of Contents

Global CCB Research Agenda 2022 – 2023 Prioritized List: Research Topics

[A(i)] Working Group A – Task Force Strategy & Assessments

Impact of national cybersecurity capacity assessments on NCS development and implementation

The main research objective is to understand whether countries consider recommendations put forward by the cybersecurity capacity assessments when developing and implementing national cybersecurity strategy.

[A(ii)] Working Group A – Task Force CBMs/Norms Implementation & Cyberdiplomacy

Understanding the global cyber diplomacy ecosystem

This research focuses on the group of diplomats/government officials working at the intersection of cybersecurity and foreign policy/international relations, looking at how the field has evolved and how much progress there is still to be made.

[B (i)] Working Group B – Task Force Cyber Incident Management

Proactive Cyber Incident Communications and Engagement

This research seeks to understand and describe the impact of more open and proactive approaches to incident communications and information sharing; focusing on approaches, benefits, challenges, and case studies.

[B (ii)] Working Group B – Task Force CIIP

Identifying indicators of CIIP maturity

This study explores how developed countries have implemented CIIP strategies and policies, and what the best practices for implementation and measuring success are.

[C] Working Group C - Cybercrime

Evolution of dark web for criminal activity and its implications on law enforcement

The way the dark web is being used is changing and illegal marketplace platforms are on the rise. The focus of this study is to understand this evolution, and identify patterns and new trends.

[D] Working Group D – Cybersecurity Culture & Skills

Understanding the concept of Cyber Security Culture: What it is and why it matters? How cyber security culture emerges, how it can change and be influenced?

This research will address several key knowledge gaps and promote a broader understanding of how cybersecurity culture can be promoted through cyber capacity building and cyber diplomacy.

Cross-cutting topic & Gender Considerations

Extent of online gender-based violence (OGBV) across the Commonwealth Nations

The main objective of this research is to establish the true extent and scale of the OGBV problem, to inform future policy and campaign work for local Governments and NGOs involved with cyber security.

Global CCB Research Agenda 2022 – 2023 Prioritized List: Elaboration on Research Topics

WG A Task Force Strategy & Assessments:

Impact of national cybersecurity capacity assessments on NCS development and implementation

Research question(s)/objective(s)

The main research objective is to understand whether countries consider recommendations put forward by the cybersecurity capacity assessments when developing and implementing national cybersecurity strategy.

Elaboration

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.

WG A Task Force CBMs/Norms Implementation & Cyberdiplomacy:

Understanding the global cyber diplomacy ecosystem

Research question(s)/objective(s)

This research should look at:

- *Estimated no. of officials working in each country at the intersection of cybersecurity and foreign policy/international relations.*
- *The demographic profile of the group (gender, age, academic/professional background, type of government agency, how long in post, etc).*
- *Where do members of the group get their information.*
- *How often do they travel, to where, what conferences?*

Elaboration

The UN Open Ended Working Group and the Ad Hoc Committee on Cybercrime, alongside regional and other multilateral fora have led to a significant increase in the number of diplomats engaging on cyber issues. However, it remains unclear exactly how the field is evolving and how much progress there is still to make. While there is now research on training, there is much less info on the group themselves. This will be crucial to understand what future interventions are required. It would be useful to have this information for all countries, but there is a valid argument to do a regional or 'sub-regional' proof of concept. Ideally the analysis would allow for global comparison.

Global CCB Research Agenda 2022 – 2023 Prioritized List: Elaboration on Research Topics

WG B Task Force Cyber Incident Management:

Proactive cyber incident communications and engagement

Research question(s)/objective(s)

To what extent do proactive information sharing and external communications approaches positively impact technical, reputational, financial, and other aspects of incident response and recovery for stakeholders (e.g. organization/ government/the security community/ other stakeholders)?

What are some case studies that demonstrate the approaches to and value of more proactive communications?

Elaboration

The importance of communication, information sharing, and stakeholder engagement around cyber incidents has become increasingly important as the number, scale, and impact of incidents rise. Proactive communications can raise the profile of an incident or inform malicious actors of impact. However, governments and organizations have increasingly recognized that a more proactive approach to communicating with stakeholders and partners, including the public more often results in better outcomes. For example, sharing technical details within the security community can help prevent further incidents and potentially garner insights/support. More forward communications with the public can also help to contain the spread of an incident; avoid speculative coverage; and build, rather than detract, from confidence and trust in an organization. This project will deliver a more research-based understanding of the value of proactive communications to assist CERT/CSIRTs, governments, organizations, and decision makers better understand the importance of and plan for proactive incident communications.

WG B Task Force Critical Information Infrastructure Protection:

Identifying indicators of CIIP maturity

Research question(s)/objective(s)

This study explores how developed countries have implemented CIIP strategies and policies, and what the best practices for implementation and measuring success are.

Elaboration

Taking into account the work that has been carried out by ITU's Global Cybersecurity Index and the Global Readiness Index, 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.

Global CCB Research Agenda 2022 – 2023 Prioritized List: Elaboration on Research Topics

WG C Cybercrime:

Evolution of dark web for criminal activity and its implications on law enforcement

Research question(s)/objective(s)

Evolution of dark web for criminal activity and its implications on law enforcement

Elaboration

Previous IOCTA reports have highlighted an important change in the way the DarkWeb is being used by cybercriminals stating that the "lifecycle of dark web marketplaces has shortened and there is no clear dominant market that has risen over the past year and criminals have started to use other privacy-focused, decentralized marketplace platforms to sell their illegal goods. Although this is not a new phenomenon, these sorts of platforms have started to increase over the last year." Therefore, it will be beneficial to delve deeper into this to attempt to understand this evolution, the patterns, and new trends. As several capacity building activities revolve around the DarkWeb, this will help better inform those projects and cybercrime efforts more generally.

WG D Cybersecurity Culture & Skills:

Understanding the concept of cybersecurity culture: What it is and why it matters? How cyber security culture emerges, how it can change and be influenced?

Research question(s)/objective(s)

This research will promote a broader understanding of how cybersecurity culture can be advanced through cyber capacity building and cyberdiplomacy.

Elaboration

Existing research on cyber security culture is sparse and focused on the business sector. It has not been translated well into the realm of cyber diplomacy and/or cyber capacity building. Whilst culture is acknowledged as being important in cyber security, there are relatively few holistic analyses of the concept, and a limited understanding of how cyber security culture can be promoted through cyber capacity building and cyber diplomacy. There is also very little research addressing the ingredients of a 'good' or 'bad' cyber security culture? Although this is a normative question, there is a lack of understanding of how behavior, ideas, practices, and processes (the core elements of culture) can lead to cyber breaches and insecurity. Much of the work that has been done is in the private sector and fails to consider either national or regional cultural drivers of cyber insecurity. At the regional level, there are various plans for developing strategic culture but very little work that looks at how international organizations can promote good cyber security culture within their memberships. The proposed research thus fills both a conceptual gap, and an empirical one (through its examination of case studies of where cyber breaches were caused by poor cyber culture). Crucially these questions relate to the GFCE's work: how can cyberdiplomacy and cyber capacity building programs and processes be used to advance and promote good security culture?

Global CCB Research Agenda 2022 – 2023 Prioritized List: Elaboration on Research Topics

Cross-cutting topic & Gender considerations:

Extent of online gender-based violence (OGBV) across the Commonwealth Nations

Research question(s)/objective(s)

The main objective of this research is to establish the true extent and scale of the OGBV problem, to inform future policy and campaign work for local Governments and NGOs involved with cyber security.

Elaboration

OGBV is a highly sensitive and significant problem within Commonwealth countries as identified over the last three years, however there is currently a lack of data and meaningful research on this issue in countries with developing economies. Focus of the research would be on the Commonwealth of Nations, predominantly in the Caribbean, Pacific and in sub-Saharan Africa.

The following organizations have been identified as willing to collaborate on this research: Get Safe Online, The Oceania Cyber Security Centre (OCSC), Organization of American States (OAS), Cybersecurity Capacity Centre for Southern African (C3SA) and UN Women.

Global CCB Research Agenda 2022 – 2023

Annex: Other Research Topics Proposed

Each Working Group identified at least three (3) knowledge gaps/research topics for the Global CCB Research Agenda 2022 – 2023 cycle. This annex outlines the other research topics that were proposed by the Working Groups and received at least one (1) vote during the prioritization exercise.

The research topics are listed below and elaborated on the next page.

- Understanding the cybersecurity capacity needs of African countries to develop and/or update National Cybersecurity Strategies (NCS)
- Understanding the evolution of National Cybersecurity Strategies
- Mapping exercise on capacity building for cyber norms
- Regional CSIRTs and advancing incident response coordination and cybersecurity capacity building
- Managing the relationship between national CSIRTS and sectoral CSIRTs
- Role of the private sector in CSIRT capacity building
- National approaches to CIIP
- Analysis of the cost of cybercrime
- Mechanisms for implementing cooperation in the fight against cybercrime in Africa and beyond
- Cyber attribution repository of public attribution efforts
- Understanding the societal harm of ransomware
- Cybercrime and emerging technologies (focus on AI)
- Cybercrime and cyber incident response
- Detecting, cataloguing, and preventing cybercrime
- Raising cybersecurity awareness amongst SMEs
- Cyber capacity building initiatives on awareness

Global CCB Research Agenda 2022 – 2023

Topics proposed by Working Group A

Task Force Strategy & Assessments:

Understanding the cybersecurity capacity needs of African countries to develop and/or update National Cybersecurity Strategies (NCS)

Research question(s)/objective(s)

What is the status of NCS in African countries? Which NCSs exist, how were they drafted, and how did they evolve? What challenges do countries face in the drafting and implementation phase? Are there any specific factors (from CMM) impacting the NCS?

What are the cybersecurity capacity needs of African countries to develop and/or update NCS? At which stage is support (such as expert advice/funding) most critical and what kind of support is most crucial?

Elaboration

The research aims at better understanding the challenges and requirements for NCS development and implementation in Africa, also considering the different priorities of the African communities and potential of regional integration. The results of the study inform the ways of support that the GFCE can provide to its members from the African continent as outlined in the Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle. The study is also expected to contribute to the GFCE Support Package and to the knowledge modules and development of the GFCE-AU Initiative.

Task Force Strategy & Assessments:

Understanding the evolution of National Cybersecurity Strategies

Research question(s)/objective(s)

An analysis of:

- How the content of national cybersecurity strategies has evolved over time.

- What has changed between a countries' old and updated strategy (i.e. to what extent is learning taking place).

- How the content of national cybersecurity strategies compares to accepted 'best practice'.

- How the strategies are tailored to circumstances in a country vs use generic formulations.

- The extent to which strategies are leveraging/addressing the latest state of available technology.

Elaboration

Since the earliest days of cyber capacity building, having a national cybersecurity strategy has been perceived to be foundational. However, far less attention has been given to the content of these strategies. This is despite the fact that the field has evolved significantly, that threats have shifted, and technologies have matured and given rise to new technologies. It is therefore recommended that the GFCE support an analysis of how strategies have evolved over time and what that tells us about the state of the field.

Global CCB Research Agenda 2022 – 2023

Topics proposed by Working Group A

Task Force CBMs/Norms Implementation and Cyberdiplomacy:

Mapping exercise on capacity building for cyber norms

Research question(s)/objective(s)

To what extent have GFCE member countries implemented the 11 2015 norms of Responsible State Behavior in Cyberspace? What resources within the GFCE Community are available to support the implementation of cyber norms?

Elaboration

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. This research will support the work of the Task Force in understanding what future activity it should do in this area.

Global CCB Research Agenda 2022 – 2023

Topics proposed by Working Group B

Task Force Cyber Incident Management:

Regional CSIRTs and advancing incident response coordination and cybersecurity capacity building

Research question(s)/objective(s)

How have regional CSIRTs (and equivalent organizations) been effective in advancing regional response coordination and advancing the capacities of national CSIRTs? Should (and can) regional CSIRTs be formed to harness other regional and national cyber security capabilities as well as establish a more organized network of regional incident response and capacity building efforts globally?

Elaboration

This research will explore the effectiveness and feasibility of regional CSIRTs in advancing incident response coordination and cybersecurity capacity building. This research will also support the GFCE as it focuses on its regional approach.

Task Force Cyber Incident Management:

Managing the relationship between national CSIRTS and sectoral CSIRTs

Research question(s)/objective(s)

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.

Elaboration

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.

Global CCB Research Agenda 2022 – 2023

Topics proposed by Working Group B

Task Force Cyber Incident Management:

Role of the private sector in CSIRT capacity building

Research question(s)/objective(s)

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.

Elaboration

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.

Task Force Critical Information Infrastructure Protection:

National approaches to CIIP

Research question(s)/objective(s)

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?

Elaboration

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.

Global CCB Research Agenda 2022 – 2023

Topics proposed by Working Group B

Task Force Critical Information Infrastructure Protection:

Strengthening countries internet infrastructure

Research question(s)/objective(s)

How can countries establish a resilient internet infrastructure? What are the best strategies, policies and good practices for securing national internet infrastructure?

Elaboration

There are already ongoing efforts by the global community to contribute to securing countries internet infrastructure. This can be seen through multiple initiatives, such as the IITU-T sector documents and recommendations, CyberGreen and Global Cyber Alliance, FIRST, among others.

Global CCB Research Agenda 2022 – 2023

Topics proposed by Working Group C

Analysis of the cost of cybercrime

Research question(s)/objective(s)

What are the visible and invisible costs of cybercrime to society as a whole?

Elaboration

A comprehensive analysis of the cost of cybercrime, including societal and individual impact, is both timely and much needed. In parallel with the UN Third Committee process to design a global convention on cybercrime, an evidence-led analysis that shifts the focus from visible financial losses to invisible costs and long-term impact on society would shed light on what is truly at stake in combating the misuse of ICTs for criminal purposes.

Mechanisms for implementing cooperation in the fight against cybercrime in Africa and beyond

Research question(s)/objective(s)

What are the formal and informal tools available to African states for cooperation and collaboration in their efforts to combat cybercrime? With a view to maintaining and improving this regional and international cooperation, how can the institutional and legislative framework of the African Union Member States be harmonized? How to implement joint operations by African States' investigation units against cybercrime networks?

Elaboration

Cybercrime is one of the scourges that threaten the African continent daily with inestimable material and moral damage. The identification and prosecution of cyber offenders is a major challenge for African countries. The disparity of legislative texts, as well as the lack of necessary technical infrastructure and qualified human resources, make the continent a field of predilection for cyber criminals. Indeed, there is a huge gap between the annual rate of cybercrime and the response of states in terms of repression. Because of its virtual, transnational nature and the anonymity of its perpetrators, the challenges posed by cybercrime can only be met with the combined efforts of all State and non-State actors. This necessarily calls for effective and sustained regional and international cooperation among law enforcement authorities and cooperation agencies, as well as public and private companies. At the tactical and operational levels, the lack of joint operations by investigative units from several countries.

Global CCB Research Agenda 2022 – 2023

Topics proposed by Working Group C

Cyber attribution repository of public attribution efforts

Research question(s)/objective(s)
To build an attribution repository to document all public attribution efforts.

Elaboration
Information about public attribution efforts is scattered across various stakeholders (public and private) and platforms. Bringing this information together on one platform would be a strong asset for policymakers, victims of cyberattacks and researchers, helping to build expertise around this understudied aspect of cybersecurity.

Understanding the societal harm of ransomware

Research question(s)/objective(s)
To develop a framework for understanding the societal harm of ransomware.

Elaboration
Ransomware causes a wide range of direct harms to targets, but also to society as a whole. When attacks target critical infrastructure or essential services, their (temporary) disruption has long-term consequences on society's functioning and can undermine the trust in legitimate processes. We are currently missing a framework for understanding the societal harms of ransomware, including long-lasting physical, reputational, psychological consequences on targets and victims.

Global CCB Research Agenda 2022 – 2023

Topics proposed by Working Group C

Cybercrime and emerging technologies (focus on AI)

Research question(s)/objective(s)

To understand how emerging technologies such as AI is being leveraged to conduct cybercrime and fight cybercrime, and what the latest developments are.

Elaboration

Some experts believe that the nature of AI – specifically, its applicability to 'big data' – is more suited to defensive operations rather than offensive ones. As things stand, those trying to use AI to boost cybersecurity seem to have the edge over those seeking to use such technology in the pursuit of criminal endeavors or other assaults on the integrity of networked systems. This however might change. It would be good to get a piece of research looking at the latest developments on that front, how is AI being used to fight cybercrime but also conduct criminal activity. The findings will be very useful in designing and sourcing future cybercrime capacity building activities. for understanding the societal harms of ransomware, including long-lasting physical, reputational, psychological consequences on targets and victims.

Cybercrime and cyber incident response

Research question(s)/objective(s)

To develop a comprehensive incident response handling guide for institutions of all sizes.

Elaboration

The project should include a comprehensive mapping of resources available on the various cybersecurity frameworks and policies that influence the cybersecurity sector.

Global CCB Research Agenda 2022 – 2023

Topics proposed by Working Group C

Detecting, cataloguing, and preventing cybercrime

Research question(s)/objective(s)

The primary objective of this research topic will be to detect, catalogue and prevent emerging cybercrime a nation cyberspace. A second objective would be to look at the various mechanisms, techniques or processes that can be used to restore or bring a system back to its normal operating state after a major security incident or breach.

Elaboration

The project should deliver statistical data on the variations of cybercrime within the research stipulated areas, explore the various cybercrime statistics and threats vectors that instigate cybercrime. The study will explore the current threat landscape and its associated threat groups or threat actors. Threat intelligence reports could be used to build data driven decisions that will reduce the risks posture to critical information sectors (e.g. financial, health, telecommunication, internet of things, and industrial control system)

Global CCB Research Agenda 2022 – 2023

Topics proposed by Working Group D

Raising cybersecurity awareness amongst SMEs

Research question(s)/objective(s)

This study explores how organizations maximize impact of SME Cybersecurity awareness for the local context. For example, by mapping existing cybersecurity awareness activities focused on SMEs (through a comprehensive survey and analysis), distil key messages across the initiatives. Also, looking at how the local context is defined and how this influences the delivery of awareness-raising messages.

Elaboration

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. 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.

Cyber capacity building initiatives on awareness

Research question(s)/objective(s)

The major goal of this research project is to understand how countries are implementing or conducting cyber security capacity building initiatives related to raising cyber awareness in the global/local context.

Elaboration

This project would focus on Liberia and the West Africa region. By the end of this project, the following deliverables would also be achieved:

- Building a national, regional and continental cyber security simulation and training center that will be used to host conferences, seminars, trainings, cybersecurity simulations and etc.
- The Center will also be used to host offices for the GFCE community across Africa that includes guesthouse, offices for national, regional and international cyber security organizations. This will reduce the huge rental costs for venue intended for training, seminars and other capacity building initiatives that could potentially span over weeks.