GFCE CCB Research Agenda
WG C Research Topic Proposals

VOTE FOR PROPOSALS HERE: https://forms.gle/p3MLyeynRLX7iJ4P8

PROPOSAL 1	
Research Topic/Idea	Detecting, Cataloguing and Preventing Cyber Crime
Research question(s) or objective(s)/ outcome(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. The project should aim at the following outcomes: ▪ Come up with a statistical data on the variations of cybercrime within the research stipulated areas. ▪ We should be able to have resources on the various cybercrime statistics and threats vectors that instigate cybercrime. ▪ A platform for monitoring the current threat landscape and its associated threat groups or threat actors. ▪ Use threat intelligence report to build data driven decisions that will reduce the risks posture to critical information sectors. Example, the financial, health and the industrial control systems.
Any additional information or considerations	Focus should be on West Africa, including Liberia & all sectors and neighbouring countries (Guinea, Sierra Leone, and Ivory Coast)

PROPOSAL 2	
Research Topic/Idea	Extent of online gender-based violence (OGBV) across the Commonwealth of Nations
Research question(s) or objective(s)/ outcome(s)	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. The main objective of this research project would therefore be to establish the true extent and scale of the problem which could then help to inform future policy and campaign work for local Governments and NGOs involved with cyber security.
Any additional information or considerations	Focus of the research would be on the Commonwealth of Nations, predominantly in the Caribbean, Pacific and in sub-Saharan Africa. The following organisations have been identified as willing to collaborate on this research: The Oceania Cyber Security Centre, Organisation of American States, Cybersecurity Capacity Centre for Southern African and UN Women.

GFCE CCB Research Agenda
WG C Research Topic Proposals

VOTE FOR PROPOSALS HERE: https://forms.gle/p3MLyeynRLX7iJ4P8

PROPOSAL 3	
Research Topic/Idea	Analysis of the cost of cybercrime
Research question(s) or objective(s)/ outcome(s)	What are the visible and invisible costs of cybercrime to society as a whole? 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.

PROPOSAL 4	
Research Topic/Idea	Evolution of dark web for criminal activity and its implications on law enforcement
Research question(s) or objective(s)/ outcome(s)	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." So it will be really interesting to dig into this and try to understand this evolution, the patterns and new trends. As several capacity building activities revolve around the DarkWeb, this will definitely help better inform those projects and cybercrime efforts more generally.

PROPOSAL 5	
Research Topic/Idea	Building an attribution repository to document all public attribution efforts
Research question(s) or objective(s)/ outcome(s)	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.

GFCE CCB Research Agenda
WG C Research Topic Proposals

VOTE FOR PROPOSALS HERE: https://forms.gle/p3MLyeynRLX7iJ4P8

PROPOSAL 6	
Research Topic/Idea	Understanding the societal harm of ransomware
Research question(s) or objective(s)/ outcome(s)	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.

PROPOSAL 7	
Research Topic/Idea	Cybercrime and emerging technologies with a particular focus on AI
Research question(s) or objective(s)/ outcome(s)	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 endeavours 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. And again, the findings will be very useful in designing and sourcing future cybercrime CB activities. for understanding the societal harms of ransomware, including long-lasting physical, reputational, psychological consequences on targets and victims.

PROPOSAL 8	
Research Topic/Idea	Cybercrime and Cyber Incident Response
Research question(s) or objective(s)/ outcome(s)	The project should aim at the following outcomes: ▪ Design a comprehensive incident response handling guide for institutions of all sizes. ▪ We should be able to have resources on the various cyber security frameworks and policies that influence the cyber security sectors and its implementation. ▪ A platform for monitoring the current threat landscape and its associated threat groups or threat actors. ▪ Use threat intelligence report to build data driven decisions that will reduce the risks posture to critical information sectors. Example, the financial, health and the industrial control systems.
Any additional information or considerations	Industrial Control System (ICS) sector, financial, telecommunication, health and the IoT sectors.

GFCE CCB Research Agenda
WG C Research Topic Proposals

VOTE FOR PROPOSALS HERE: https://forms.gle/p3MLyeynRLX7iJ4P8

PROPOSAL 9	
Research Topic/Idea	Mechanisms for implementing cooperation in the fight against cybercrime in Africa and beyond
Research question(s) or objective(s)/ outcome(s)	Objectives What are the formal and informal tools available to African states for cooperation and collaboration in their efforts to combat cybercrime? What are the tools to be developed for the implementation of a sound and effective cooperation that meets the requirements and threats related to cybercrime on the continent? 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? Problem statement/knowledge gap Cybercrime is one of the scourges that threaten the African continent on a daily basis 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.
Any additional information or considerations	The main beneficiaries of this study will be States, followed by legal entities and individuals likely to be victims of cybercrime. The institutions and cooperation bodies of the continent as well as any other international entity intervening in the continent for the application of the law and also and especially those concerned with the protection and promotion of human rights, will also be beneficiaries.