Research Paper

International Security Programme

July 2024

The Strategic Approach to Countering Cybercrime (SACC) framework

Helping countries to tackle the growing threat to their economic and national security from cybercrime

Joyce Hakmeh and Jamie Saunders

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Summary

— Cybercrime is a significant global problem that is escalating in frequency and severity, posing a serious threat not just to individuals and corporations, but to prosperity and security around the world. To illustrate the threat, the cost of cybercrime to the global economy is projected to reach $13.8 trillion by 2028. Incidents such as the ransomware attacks against Colonial Pipeline in 2021 and Costa Rica in 2022 have reinforced the need for better responses to cybercrime at both national and international levels.

— This research paper presents a framework for a strategic approach to countering cybercrime (SACC). The SACC framework is designed to aid countries in developing tailored interventions to address their specific cybercrime challenges, identify existing gaps and leverage international best practices and support.

— It is also intended to facilitate structured discussions among policymakers and relevant agencies – e.g. interior, security and information and communications technology ministries – seeking to tackle cybercrime comprehensively and strategically.

— The framework provides an adaptable tool for practitioners addressing the evolving landscape of cybercrime threats, and is designed to allow for ongoing refinement of strategies through regular assessments and adjustments to existing plans.

— The SACC framework comprises five stages: strategy development; establishing enablers; establishing operational capability; tasking and prioritization; and evaluation. Emphasizing the importance of context, it acknowledges the diverse needs of countries in addressing cybercrime and considers factors such as economic conditions, legislative frameworks and the resources available.

— As well as presenting the framework itself, this paper offers three options for its deployment, offering flexibility to accommodate different contexts and preferences. These options include focus group methodology facilitated by independent experts; self-assessment by countries; and simulation exercises framing strategic dilemmas for stakeholders to address.

— During the framework's development, the project team conducted a simulation exercise in Singapore, which explored ASEAN responses to cybercrime, the gaps and successes. The SACC framework has also been deployed by the Oceania Cyber Security Centre (OCSC), using focus group methodology, as part of the cyber maturity assessment for Fiji in February 2024. The framework helped OCSC to enhance data collection and broaden the investigative scope of its assessment.

Introduction

Cybercrime is an escalating global problem in terms of both frequency and severity. The problem poses a growing threat not just to individuals and large corporations, but to countries' economic and national security. Recent statistics have revealed that the global cost of online criminal acts amounted to $8.44 trillion in 2022. That cost is projected to reach $13.82 trillion in 2028.[1]

Over the last decade, the cyberthreat landscape has evolved significantly. The number of actors conducting cyberattacks against critical infrastructure and government agencies is growing.[2] They include both hostile state actors and criminals, with the lines between state and criminal activity becoming increasingly blurred.[3] Today, there are multiple instances of criminal groups working in concert with state actors, and of states either pretending to be criminal actors or turning a blind eye to cybercriminal activity originating from their territories.[4] This complexity is compounded by the proliferation of high-end cyber capabilities – such as ransomware-as-a-service and spyware – that are readily available on commercial and criminal marketplaces.[5]

This continued evolution is changing the perception of the threat, both in government and among the wider public. While previously, financial concerns took precedence, recent cyberattacks have shown the serious impact that cybercrime – and particularly that involving ransomware – can have on national security. For example, the ransomware attack on Colonial Pipeline in 2021 – considered 'one of the most significant attacks on critical national infrastructure in history' – and the series of attacks that led Costa Rica to declare a state of emergency in 2022 both illustrate this impact.[6] Meanwhile, similar attacks elsewhere have paralyzed education and healthcare organizations, as well as other critical services.[7] In June 2024, for example, a ransomware attack against a third-party supplier to multiple hospitals and medical practices in London led to the cancellation of operations and to the declaration of a critical incident emergency.[8] These incidents and others have reinforced the need for better responses at both national and international levels to address emerging threats from cybercrime before they become more damaging for global prosperity and security.

---

1 Fleck, A. (2024), 'Cybercrime Expected To Skyrocket in Coming Years', Statista, 22 February 2024, https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027.
2 UK Parliament (2018), 'Cyber Security of the UK's Critical National Infrastructure: Protecting CNI against cyber-attack: a 'wicked' problem', National Security Strategy Select Committee, 19 November 2018, https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/170805.htm.
3 Todd Lopez, C. (2021), 'In Cyber, Differentiating Between State Actors, Criminals is a Blur', United States Department of Defense DOD News, 14 May 2021, https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur.
4 Merrigan, E. (2019), 'Blurred Lines Between State and Non-State Actors', Council on Foreign Relations Net Politics blog, 5 December 2019, https://www.cfr.org/blog/blurred-lines-between-state-and-non-state-actors.
5 The White House (2023), 'President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security', fact sheet, 27 March 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security.
6 Tidy, J. (2021), 'Colonial hack: How did cyber-attackers shut off pipeline?', BBC News, 10 May 2021, https://www.bbc.co.uk/news/technology-57063636; Associated Press via *Guardian* (2022), 'Costa Rica declares national emergency amid ransomware attacks', 12 May 2022, https://www.theguardian.com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks.
7 BBC News (2021), 'Cyber-attack on Irish health service 'catastrophic'', 20 May 2021, https://www.bbc.co.uk/news/world-europe-57184977.
8 Martin, A. (2024), 'Critical incident declared as ransomware attack disrupts multiple London hospitals', The Record, 4 June 2024, https://therecord.media/london-hospitals-ransomware-attack-critical-incident-declared.

In discussing cybercrime, and the strategic approach to countering it, this research paper refers to both 'pure' cybercrimes (or 'cyber-dependent' crimes) and 'cyber-enabled' crimes. (See Box 1 for definitions of these terms.)

Box 1. Defining cybercrime

There is no universally agreed definition of cybercrime. Some countries define it narrowly by including 'cyber-dependent' crimes – sometimes referred to as 'pure' cybercrimes. These are crimes that were not possible before the advent of digital technologies, such as hacking, denial-of-service attacks and ransomware. Cybercrime also includes 'cyber-enabled' crimes, which are traditional crimes such as child sexual exploitation and fraud that have been transformed in scale and impact due to digital technologies.

In addition to the above, some countries consider as 'cyber-enabled' crimes a number of content-related offences like insulting or defaming religion or religious values, threatening publics morals and publishing fake news. Several countries that take such an approach have adopted cybercrime laws that lack precision in their provisions, leading to those laws being often used to prosecute a broad range of online conduct, censoring online speech and infringing on human rights.[9]

More countries are beginning to recognize the need for greater coherence in their response to malicious cyber activity, especially among law enforcement, national security and intelligence services. As a former UK attorney-general outlined in a 2022 speech, ascertaining whether a cyberattack is perpetrated by a state actor or a criminal group when it first happens is difficult.[10] This problem calls for cross-disciplinary and cross-governmental efforts to address a wide range of threats, whether those threats are politically or criminally motivated.

As the global threat of cybercrime continues to escalate and grow in complexity, both within and across borders, the need for a collaborative and strategic response is clear. Countering cybercrime effectively requires a unified effort, with relevant stakeholders joining forces to assess the scale and nature of the cybercrimes they face, establish priorities, identify the optimal mix of interventions, evaluate the impact of adopted strategies and adapt responses accordingly. By adopting such a comprehensive approach, countries can develop tailored processes for tackling cybercrime suited to their individual contexts. Such an approach will also enable the implementation of scalable interventions that are effective in reducing the impact of cybercrime on both economies and societies at large.

The case for a strategic approach can, of course, be made for any kind of anti-crime measure. But cybercrime has unique characteristics that make this proposal particularly relevant. For example, cybercrimes are generally conducted from

9 Human Rights Watch (2021), 'Abuse of Cybercrime Measures Taints UN Talks', 5 May 2021, https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks.
10 UK Attorney General's Office (2022), 'International Law in Future Frontiers: Speech, Rt Hon Suella Braverman KC MP, Attorney-General, Royal Institute of International Affairs, London, UK', 19 May 2022, https://www.gov.uk/government/speeches/international-law-in-future-frontiers.

a distance and tend to be simultaneously directed against multiple victims, who are often located in different jurisdictions. As such, cybercrime breaks the 'crime triangle' of offender, victim and location that underpins much of crime-fighting orthodoxy.[11] Cybercrime requires a greater level of collaboration and coordination between different stakeholders, including local and national components of the criminal justice system, other public authorities, international partners, the private sector and civil society.

Countering cybercrime also requires skills that are often in short supply, even in developed countries. Despite measures like the creation of central specialist units and targeted professional training schemes, keeping up with the latest cyber capabilities is still a challenge. Demand for these skills usually outstrips supply and the cybercrime landscape is constantly evolving. Other factors, such as limited knowledge, experience, capabilities and resources, often hamper attempts to fight cybercrime.

A strategic approach to cybercrime can help overcome these challenges and allow countries to develop bespoke interventions that suit their specific circumstances. Such an approach can help stakeholders identify and agree on national-level priorities, and to assess the required capacities, capabilities and resources to address those priorities. It can also help promote unity of purpose among the various stakeholders, and enable them to measure the overall effectiveness of the interventions and adjust where necessary.

This research paper proposes a new structure for developing a strategic approach – in the form of the Strategic Approach to Countering Cybercrime (SACC) framework. The SACC framework is intended to initiate a structured conversation among policymakers on how to tackle cybercrime comprehensively and strategically. It aims to assist countries in developing a set of interventions that address their specific needs and priorities, identify gaps in any current or existing plans, and benefit from established good practice and practical support available from the international community. The framework is detailed in Chapter 2 and consists of five stages covering the full cybercrime-response life cycle: strategy development; establishing the enablers; establishing operational capability; tasking and prioritization; and evaluation.

Chapter 3 then explores the potential applications of the SACC framework, offering three options as examples – focus group methodology, self-assessment and simulation exercises – and providing insights into their deployment across various scenarios and contexts.

11 Cohen, L. E. and Felson, M. (1979), 'Social Change and Crime Rate Trends: A Routine Activity Approach', *American Sociological Review*, 44(4), pp. 588–608, https://doi.org/10.2307/2094589.

Developing the Strategic Approach to Countering Cybercrime (SACC) framework

The importance of a context-specific approach

Although general guidance is available to help countries develop cybercrime strategies and responses, the specific needs and circumstances of individual countries will naturally vary.[12] The impacts of cybercrime on individuals and businesses depend on economic and social factors, such as a country's level of digitization. Furthermore, the transnational nature of cybercrime means that some countries suffer disproportionately from being targeted by cybercriminals from outside their jurisdictions, while others might be home to criminals whose victims are located elsewhere. The distinction may impact the level of priority that any one country might apply to countering cybercrime relative to other needs. The kinds of interventions that are viable also depend on the capabilities and resources available in the country. Likewise, a country's ability to take effective action against perpetrators will depend on contextual factors, such as the technical maturity of its law enforcement agencies, and the availability of resources and specialist support in the wider economy.

The transnational nature of cybercrime means that some countries suffer disproportionately from being targeted by cybercriminals from outside their jurisdictions, while others might be home to criminals whose victims are located elsewhere.

Understanding a country's context and risk landscape is therefore crucial when it comes to identifying its cybercrime priorities. These priorities will in turn determine the capabilities and resources that the country needs. Context and risk will define the extent of the authorities' engagement with external stakeholders, including foreign partners and private sector entities. Those two factors will also define what is realistic in terms of public engagement, and the extent to which individuals and small businesses can be expected to protect themselves.

However, while acknowledging the differences between countries, several common enablers can be identified that are necessary to tackle cybercrime. These enablers include the right substantive and procedural legislation; agencies that are empowered and equipped to act; and mechanisms to facilitate collaboration with both domestic and international partners. There are also specific technical capabilities that most, if not all, countries need to investigate and prosecute cybercrimes, or other crimes with a digital component – such as an ability to preserve, collect and share digital evidence nationally and across borders.

---

12 See, for example, Cross, S. and Lim, M-A. (2021), *National Cybercrime Strategy Guidebook*, Lyon: INTERPOL, https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf; World Bank and United Nations (2017), *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies (English)*, Washington, DC: World Bank Group, http://documents.worldbank.org/curated/en/355401535144740611/Combatting-Cybercrime-Tools-and-Capacity-Building-for-Emerging-Economies.

Methodology

The project team adopted a comprehensive approach in developing the SACC framework, starting with a review of existing guidance on formulating cybercrime policies to identify areas where additional guidance could be beneficial.[13] Following this review, the project team brought together a group of cybercrime experts to advise on methodology, and organized a workshop to gather perspectives on the strategic approaches to combating cybercrime. This workshop served as an interactive platform for cybercrime practitioners operating at both the national and international levels to share insights, and to help inform and validate the framework's methodology.

(It is important to note that the framework also served as the basis for Chatham House's 2023 toolkit on integrating gender in cybercrime capacity-building.[14] This toolkit provides actionable strategies for integrating gender considerations into cybercrime capacity-building efforts.)

To test the SACC framework in a regional context and refine its approach, the project team conducted a series of interviews with ASEAN cybercrime practitioners, and organized a simulation exercise in Singapore in collaboration with INTERPOL. The latter used a real-life scenario and crisis timeline unfolding at both national and regional levels, placing emphasis on the different stages of the framework. The objective of this exercise was to initiate a structured discussion with ASEAN stakeholders about their cybercrime planning, and to collectively identify ways in which the framework could help strengthen national planning and regional collaboration.

The Strategic Approach to Countering Cybercrime (SACC) framework

The SACC framework is based on a cybercrime-response life cycle developed by the team and has five sequential stages. This life cycle shows the multifaceted nature of addressing cybercrime, and the complex interplay between policy, technology and the evolving landscape of online criminal activity.

The five stages of the framework are:

- **Stage 1: Strategy development.** At the outset of developing a strategy to tackle cybercrime, it is critical to understand the context and risk, establish how tackling cybercrime supports the country's broader political, economic and social objectives, and translate this insight into a set of strategic interventions that suit the country's specific circumstances and needs.
- **Stage 2: Establishing the enablers.** Subsequently, government bodies must put in place the legislation, operational mandates and collaborative frameworks needed to counter cybercrime.

13 Ibid., p. 11.
14 Emerson-Keeler, R., Swali, A. and Naylor, E. (2023), *Integrating gender in cybercrime capacity-building*, Toolkit, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784135515.

— **Stage 3: Establishing operational capability.** Capacity-building is critical through the development of technical capabilities and the provision of operational resources for criminal justice authorities, law enforcement and other entities mandated to counter cybercrime. These efforts need to achieve the right balance between disruptive measures to pursue and deter cybercriminals and preventative measures to reduce the susceptibility of potential victims.

— **Stage 4: Tasking and prioritization.** Governments must establish processes to apply resources in a way that ensures optimal impact, and which retains and develops public confidence and trust in the country's ability to respond effectively.

— **Stage 5: Evaluation.** Finally, authorities must develop mechanisms and procedures to evaluate the outcome of individual actions to counter cybercrime, alongside the overall effectiveness of their approach.

The consequences of cybercrime can vary significantly based on who the victims are. For instance, online harassment and stalking, unauthorized sharing of intimate content and identity theft are all examples of online crimes that disproportionately affect women and marginalized groups. Recognizing such differentiated impacts is crucial for the development of effective cybercrime policies that address the unique vulnerabilities of diverse groups and ensure comprehensive protection for all victims.

The consequences of cybercrime can vary significantly based on who the victims are. Recognizing such differentiated impacts is crucial for the development of effective cybercrime policies.

Each stage of the framework includes questions relating to equality, diversity and inclusion (EDI) aimed at assisting policymakers in embedding EDI practices into their strategic processes. The questions in the framework have been devised with groups in mind, and can be amended as appropriate to focus on groups specific to a country's context. For example, if a country requires a gender-based analysis of the impact of cybercrime, the framework's questions can be amended to refer more specifically to gender (rather than race, religion or other protected characteristics).

The following section elaborates on the relevance to practitioners of each of the five stages, followed by the questions to be asked during each stage.

Stage 1: Strategy development

Stage 1 enables practitioners to explore how cybercrime risks and priorities are perceived, identified and assessed at the national level – particularly with regard to their impact. In addition, this stage can be used to examine whether strategic assessment is reflected in an existing formal or informal cybercrime strategy (or other documents), and, if so, how this strategy was developed, how it is implemented, and the extent to which it has political support and commitment from national leaders.

The questions included in this stage explore how cybercrime is defined, how different stakeholders are engaged in the development and implementation process, what authority they have over other stakeholders responsible for delivering aspects of the strategy, and what the existing mechanisms are for accountability. Stakeholder engagement is an ongoing process. This stage therefore also includes questions on how the strategy and progress is communicated. In addition, it covers the existing budgetary models and how they are applied. Finally, Stage 1 includes questions on EDI, to ensure interventions do not reinforce traditional or outdated perceptions of crime and crime prevention measures.

Stage 2: Establishing the enablers

While measures aimed at countering cybercrime can fall within existing statutes, most countries have found that new substantive and procedural legislation is required to effectively investigate cybercrimes, particularly those taking place across jurisdictions, and to protect victims. Stage 2 explores the enablers – such as legislation and funding – needed to support the delivery of effective cybercrime interventions. This stage also examines the agencies involved in tackling cybercrime, their mandates, and the existing checks, balances and safeguards in place.

Furthermore, Stage 2 includes questions regarding the budgetary arrangements necessary to align resource allocation with the actual demands on both policymaking and operational agencies. The establishment of processes is crucial for resolving trade-offs in the realm of cybercrime, and those between cybercrime and other urgent public safety concerns.

The set of questions at Stage 2 also interrogates how legislation, operational mandates and collaborative frameworks acknowledge the EDI implications of justice processes. This involves assessing legislative frameworks for any aspects that may reinforce marginalization; improving access to justice for marginalized individuals; and ensuring that legislative drafting is inclusive and representative.

Stage 3: Establishing operational capability

Combating cybercrime is intensive in terms of technology and resources. Each country must identify its own capability, priorities and gaps, and allocate adequate resources. The questions at Stage 3 seek to examine the basis on which budgeting decisions are made. The rolling or incremental budgeting practices that are common in the public sector across the world tend not to be suited to dealing with the dynamic nature of the cybercrime threat. It may therefore be necessary to conduct regular reviews of the overall level of priority accorded to cybercrime relative to other types of crime, rather than simply assuming that historic priorities reflect the current level of harm. The set of questions also seeks to explore the balance between disruptive measures to pursue and deter cybercriminals, and preventative measures to reduce potential victims' exposure to risk. Scalable cybercrime prevention measures can provide a much greater return on investment than reactive investigation, although both are important deterrents.

These efforts should also consider mechanisms, means and opportunities to enable individuals, institutions, groups and organizations to foster advocates, perform functions, solve problems, and set and achieve EDI objectives, in ways that are both sustainable and transformative.

Stage 4: Tasking and prioritization

To meaningfully reduce the harm caused by cybercrime, high-level objectives need to be translated into operational actions. Given the range of potential interventions available, decision-makers – in consultation with other stakeholders – need to decide which combination will be most effective.

Stage 4 can be used to assess how operational decisions on resource allocation are made, and how the balance between pursuing strategic outcomes and responding to more immediate threats is struck. The questions focus on which cybercrimes are prioritized in terms of response, investigation and prevention. They also cover the sources, use and application of intelligence to inform priorities, and the operating procedures in place to support anti-cybercrime activities like crime reporting and victim support.

Those responsible for making and delivering operational decisions and processes should understand the causes of vulnerability. Teams that are equipped to understand how EDI interacts with their area of work, and which include diverse voices in their governance, will be able to develop processes that better reflect the needs of victims and reduce the targeting of specific vulnerable groups.

Stage 5: Evaluation

The ultimate measure of a strategy's success is the extent to which the damage caused by cybercrime is reduced and the country's overall economic and social goals remain unaffected. As the cybercrime landscape is constantly evolving, it is important to have mechanisms in place to measure the effectiveness of an approach in order to readjust it as necessary.

Stage 5 of the framework can be used to examine how a country evaluates its activities at the operational, tactical and strategic levels, and how this information is used to improve that country's strategic response to cybercrime risks. This includes (but is not limited to): evaluating the efficacy of operations, investigations and the overall strategy; monitoring; and addressing budgetary considerations. This stage also looks at the exercises already in place to prepare key stakeholders for major cybercrime incidents, and how lessons are learned for future activities to improve the country's resilience.

From an EDI perspective, Stage 5 also involves ensuring and actively seeking meaningful multi-stakeholder interventions, reassessing EDI considerations, and committing to evaluate anti-cybercrime actions through an EDI lens.

Questions

Stage 1: Strategy development	
Strategic risk assessment	• What are the strategic risks for the country from cybercrime? How are these risks affecting the country's broader national, social, political and economic development objectives? • What is considered a cybercrime in the country? • What are the country's specific national priorities when it comes to cybercrime? • What mechanisms are in place to ensure that the needs of the most vulnerable groups are being addressed? • How have risks been identified and have the relevant stakeholders been involved in this process? • What are the social, political and cultural barriers to realizing equality, diversity and inclusion (EDI) commitments and considerations?
Formal documents and strategies	• What documents reflect the country's strategic approach to dealing with cybercrime? • Is cybercrime addressed in the cybersecurity strategy (if one exists)? How is cybercrime addressed in other national-level strategies (e.g. crime, national security, digital development)? How does the country's strategic approach to cybercrime address the needs of these other strategies? • What are the principal lines of activity in existing cybercrime or cybersecurity strategy documents? How do they collectively address the risks? • How have these principal lines of activity been identified? • Have the relevant stakeholders been involved in this process? • Has a human rights impact assessment been applied to the country's cybercrime strategy? • How are existing obligations to EDI-related international commitments – such as the UN Sustainable Development Goals – accounted for in the cybercrime strategy?
Strategy governance	• Who is accountable for delivering the cybercrime strategy? • Is the strategy accompanied by an action plan? • How are actions to be funded? • How is progress monitored and how is success defined?
Communication plan	• Have the cybercrime strategy and action plan been documented? • How are they communicated to relevant stakeholders and the public? • How is the effectiveness of the communication plan evaluated? • Does the communication plan take EDI considerations into account? For example, have efforts been made to ensure effective communication to people who are less digitally literate or who have access to fewer information sources?
Stage 2: Establishing the enablers	
Substantive legislation	• How is cybercrime currently defined or scoped in substantive legislation? • What laws have been placed on the statute book to cover cybercrime in the past 20 years? • Are these laws based on any specific international or regional conventions or standards? • What are the gaps in substantive legislation? How are they being addressed? • To what extent does the development of laws, regulations and policies consider the gendered impacts of cybercrime on victims?
Procedural legislation	• How is procedural law used to investigate and prosecute cybercrime? • What measures are in place to ensure that criminal investigations account for the particular needs and concerns of women and other marginalized groups? • Which procedural powers have proved most useful in cybercrime investigations? • What are the major gaps in procedural processes (e.g. obtaining data/evidence from overseas)? • What other powers do the government and criminal justice authorities have to prevent and/or investigate cybercrime (e.g. regulatory requirements for businesses)? • What safeguarding and due diligence measures are in place? • How has the country's legal infrastructure historically handled cases of cybercrime targeting people from marginalized groups?

Operational mandates	• Which are the main agencies involved in the prevention, detection, investigation and disruption of cybercrime? • What mandates or remits do those agencies have to conduct this work? • How is the work of operational agencies overseen? (e.g. to monitor performance; to avoid overreach or inappropriate application of powers) • What mechanisms for remedial actions are necessary and available for victims of cybercrime? • Which stakeholders should be included in consultations to determine whether updates to the legislative framework (e.g. a new law, or amendments to an existing law) are needed, and to ensure the reporting burden is not placed wholly on the individual?
Stage 3: Establishing operational capability	
People and skills	• What human resources are currently deployed against cybercrime? • How are skills requirements determined, and what training do practitioners receive? • How is the required level of resourcing determined, and how is this paid for? • What standard operating procedures have been developed to guide cybercrime investigations, and how are these put into practice? • How does training focus specifically on the needs and characteristics of the most vulnerable victims? • How are EDI considerations integrated into hiring and training practices?
Technical capabilities	• What are the key technical capabilities required (e.g. digital forensics, data analysis, malware analysis, open-source, financial investigation)? Which agencies, entities or organizations (in both public and private sectors) are responsible for providing these? • What are the most significant gaps in technical capability and how are they being addressed? • What other capabilities (technical and non-technical) are being applied to cybercrime investigations? • What kind of planning and programmes are in place to prepare key stakeholders for major cybercrime incidents?
Crime prevention measures	• What are the key cybercrime prevention measures and who is responsible for implementing these? • What public awareness activities are in place and how are they delivered? • What is done to protect potential victims? • Which stakeholders are involved (e.g. technology firms, the retail and financial sectors)? • How has EDI been considered in crime prevention measures?
Intra-governmental collaboration, public–private partnerships and international collaboration mechanisms	• What role do governmental agencies other than law enforcement agencies (e.g. computer emergency response teams – CERTs, financial intelligence units, security agencies) play in combating cybercrime and how is their involvement coordinated? • What role does the private sector play in preventing and/or investigating cybercrime? • How are operational activities coordinated with various stakeholders? • What role, if any, is played by communities, schools and small businesses? • To what extent are joint operations with foreign partners, and/or regional or international organizations undertaken? • How is such collaboration enabled? • How is participation in international networks (e.g. INTERPOL I-24/7) facilitated? • To what extent is the country engaged in international discussions on cybercrime policy and strategy? • How does the country ensure that its needs are being acknowledged and addressed? • In addition to outreach to relevant industries, how can longer-term and structural barriers to realizing EDI be addressed?

Stage 4: Tasking and prioritization	
Setting top-level operational priorities	• How are the strategic objectives of the country's national cybercrime strategy translated into tactical objectives for operational agencies? • Who decides the balance between proactive and reactive interventions? • How does the country balance the requirements of local crime reporting, national organizations (e.g. ministries, security agencies, regulators) with those of international partners?
Intelligence and threat assessment	• How is intelligence used to drive tactical priorities? • How is intelligence used to assess the overall social and economic impact of cybercrime on the country? • How is intelligence from regional and international partners used? • What data and independent evidence on cybercrime need to be monitored and collected to meet EDI commitments?
Crime reporting and victim support	• How do victims of cybercrime report incidents? • What happens to these crime reports? • What support is available for cybercrime victims? • What kinds of crime statistics are generated by these processes? How are those statistics used? • Are crime statistics disaggregated by intersecting characteristics and identities? • What measures are in place to ensure that data are treated in a confidential and sensitive manner?
Tasking processes	• On what basis is an operation or investigation initiated? • How are individual operations/investigations prioritized and tasked? Who decides? • What standard operating procedures are in place to support anti-cybercrime activities?
Stage 5: Evaluation	
Operational	• How is the effectiveness of individual operations and investigations measured? • Do monitoring and evaluating processes involve multi-stakeholders, including those working with/supporting victims and those advocating for women and other marginalized groups? • Are monitoring and evaluation processes accessible and subject to EDI commitments?
Tactical	• How is the success of individual actions in the cybersecurity/crime strategy (and any associated action plans) measured?
Strategic	• How is the impact of cybercrime on the country measured or understood? • How would a country determine if that impact has been reduced? • How is the overall effectiveness of the cybercrime strategy in the country measured? • Is the specific impact on reducing harm on vulnerable groups measured?
Strategic review	• How are the outputs of the evaluations used to improve the response to strategic cybercrime risks? • Is evaluation carried out with a view to assessing protection of, and the delivery of justice for, the most vulnerable?
Exercising	• Is there a formal programme for conducting exercises to test strategic and operational response? • If so, what are the key priorities and objectives of this programme?

Deploying the SACC framework

The SACC framework aims to help countries to achieve three aims: first, to develop interventions that address their specific needs and priorities; second, to identify gaps in any current or existing plans; and finally, to benefit from the established good practice and practical support available from the international community. The framework is designed to facilitate a structured conversation among policymakers from relevant ministries and agencies – such as ICT, interior and security ministries, and police and security agencies – on how to tackle cybercrime comprehensively and strategically.

There are no 'right' answers to the questions set out in the framework. Instead, the questions are designed to prompt discussion among decision-makers, practitioners and other stakeholders. Such discussions will facilitate choices that best suit a country's circumstances.

The absence of *any* answer to a question will usually indicate that there is a gap in that country's overall approach to tackling cybercrime and therefore in its strategic thinking around the issue. For example, if there is no clear answer to the question 'What are the country's specific national priorities when it comes to cybercrime?', that could suggest a lack of proper analysis on the actual impact of cybercrime on the country, or perhaps that there is a lack of consensus on which crimes need to be tackled with the greatest urgency. Likewise, if there is no answer to the question 'What role does the private sector play in preventing and/or investigating cybercrime?', that could suggest that the private sector has not been engaged with effectively.

It follows that there is little point in giving cursory answers to the questions in the framework. Instead, they should be seen as an opportunity to explore the options that might exist, and to engage relevant stakeholders in a meaningful debate about which of those options are best for the country concerned.

To be effective, such debates need to be:

- **Inclusive.** All relevant stakeholders need to be involved (or at least represented) in the process. For example, the framework includes a focus on EDI because the needs of otherwise marginalized groups risk being under-represented.
- **Informed.** It is difficult to make judgements on priorities if there is little data available. For example, on the actual harm being experienced by the victims of cybercrime, or on the impact of interventions made. Intelligence and evaluation are therefore both important features of the framework.
- **Realistic.** Policy options are viable only when policymakers have assurance regarding the availability of requisite resources, specialized capabilities and political commitment to support them. The framework therefore consistently emphasizes accountability, resource allocation and prioritization.
- **Connected.** Effective cybercrime interventions require collaboration both inside a country's borders and with international partners. It is important to think through the kinds of partnerships needed and how they can be enabled both in practical terms and by law. Including partners in the SACC process is one way to draw out these issues.

Deployment options

Deployment of the SACC framework can take various forms, offering flexibility to accommodate different needs and preferences. This section elaborates on three distinct options for consideration. However, the decision regarding which deployment method to adopt ultimately depends on the specific circumstances, resources and objectives of the context in which the assessment if being conducted.

Option 1: Focus group methodology

The first option is to use independent experts to facilitate focus group interviews, supporting participants in answering the SACC framework questions. By involving different groups of stakeholders at the same time, multiple perspectives can be obtained.

This methodology has been used extensively for conducting maturity assessments, such as in the Cybersecurity Maturity Model for Nations (CMM). The benefit is that the independent experts can 'facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives… making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained'.[15] The SACC framework is not a maturity model but it does lend itself to the focus group approach. In this approach, facilitators with experience and expertise in the various elements of the framework convene mixed groups of stakeholders over the period of one or two days in-country to examine the questions and identify where there are gaps or decisions to be made. Such a process would normally culminate in a final report, setting out the outstanding issues that the country can then take forward as part of their internal policy and capacity-building processes.

The SACC framework has been already deployed using the focus group methodology as part of the CMM for Fiji, delivered by the Oceania Cyber Security Centre (OCSC) in February 2024. As a regular feature of the CMM reviews, the OCSC uses a combination of in-country focus groups and desktop research to collect the necessary data to perform a national assessment. The participants in the focus groups are carefully selected based on their knowledge of the local cyber landscape, and are divided into groups in line with the different dimensions of the CMM. In preparation for the focus groups addressing Dimension 4 of the CMM – 'Legal and Regulatory Frameworks'[16] – the OCSC used the SACC framework to redesign their question sets and develop a more comprehensive research agenda that better interrogated Fiji's cybercrime enablers and barriers. Furthermore, the structure and quality of many of the questions, such as those on EDI, also proved useful in the non-legislative focus groups, contrary to the research team's initial expectations. Overall, the rigorous scope of the framework broadened the team's investigative focus compared to previous reviews, and facilitated a more holistic data-collection process. This data will inform the analysis and recommendations of the final report currently being written and help Fiji to further advance its national cyber strategy.

---

15 University of Oxford Global Cyber Security Capacity Centre (undated), 'CMM Deployment Methodology', https://gcscc.ox.ac.uk/cmm-deployment-methodology.
16 University of Oxford Global Cyber Security Capacity Centre (undated), 'CMM Dimension 4: Legal and Regulatory Frameworks', https://gcscc.ox.ac.uk/dimension-4-legal-and-regulatory-frameworks.

Option 2: Self-assessment

Countries may prefer to conduct their own internal reviews, using the framework as a prompt – for instance, at the very start of a strategy development process or as part of a periodic review. It is important to ensure that, irrespective of the reviewer(s), the process remains 'informed, inclusive, realistic and connected', and that the right stakeholders are involved. It is important to recognize that self-assessment by policymakers or operational practitioners alone may fail to uncover all pertinent issues, or could lead to a misleading assessment, due to issues such as biases, limited perspectives or incomplete information. For that reason, independent scrutiny is an important part of the process. This scrutiny could take the form of incorporating external experts to facilitate discussions and ensure an impartial review and assessment.

Option 3: Simulation exercises

A third way to deploy the framework is to use it as the basis for a simulation exercise. This approach was tested as part of the development process of the SACC project, and proved effective not only in getting the stakeholders to agree on gaps in their current responses, but also in identifying improvements to the framework itself. The test simulation exercise took place alongside the INTERPOL Global Cybercrime conference in Singapore in October 2023, and involved eight countries from the ASEAN region. The scenario featured advanced remote access Trojan (RAT) malware being sold in the region and used to commit financial fraud, blackmail and online sexual offences.

The framework was designed by the project team to draw out potential dilemmas for the participants to address at each of three phases of the storyline, which are:

- Immediate crisis response;
- Ongoing operation; and
- Post-crisis evaluation.

These three phases enabled individual country representatives to consider the various questions set out in the framework, such as:

- How to prioritize interventions to disrupt the buyers and sellers of the RAT vs direct measures to protect victims and potential victims.
- How to coordinate interventions across multiple local and regional law enforcement agencies.
- How to facilitate cross-border cooperation to disrupt the upper echelons of the organized crime group responsible.
- How to tell if the interventions being taken were having an effect.

Although no assessment was included in the exercise, this element could be added to the process through the participation of external assessors. In the event, individual country representatives were encouraged to take away their own learnings from the exercise and use them to inform their internal strategic planning processes.

Conclusion

The dynamic nature of cybercrime and the constantly evolving cyberthreat landscape pose challenges for states to develop effective strategies that are, and remain, fit for purpose. To address these challenges, it is crucial for countries to tailor their responses to their unique contexts and priorities, rather than replicating solutions from other contexts without proper adaptation. Equally important is ensuring that their responses are holistic, which means that they consider all stages of a cybercrime response. It is common for countries – particularly those with limited resources – to focus on certain aspects of the response, such as the provision of capabilities and equipment, while neglecting other critical areas. This approach often leads to a partial impact and falls short of addressing the full scope of cybercrime challenges.

As articulated in this paper, addressing cybercrime effectively requires a comprehensive approach that includes different stages revolving around: 1) strategy development: 2) establishing enablers; 3) establishing operational capability; 4) tasking and prioritization; and 5) evaluation.

The Strategic Approach to Countering Cybercrime (SACC) framework adds to existing guidance for countries aimed at helping them tackle cybercrime and enhance their responses to it. The framework facilitates structured dialogues among policymakers and practitioners, enabling comprehensive and strategic approaches to cybercrime that can adapt to their specific contexts and strategic perspectives. By incorporating the importance of context, the framework ensures that strategies are not only robust but also relevant to the challenges faced by individual nations. As such, the SACC framework supports the ongoing refinement of strategies through regular assessments, adjustments to existing plans and the identification of gaps in current strategies.

By incorporating the importance of context, the framework ensures that strategies are not only robust but also relevant to the challenges faced by individual nations.

Because of the unique nature of each context, the SACC framework is designed to help practitioners ask the right questions. It does not seek to give prescriptive answers or assume that solutions will look similar in all countries. What is crucial is that implementation aligns with the approach outlined in the previous chapter – one that is inclusive, informed, realistic and connected. The paper has identified a set of three implementation methods of the SACC framework, while noting that others may exist that can be deployed instead or in combination.

The SACC framework has already been deployed, using the focus group methodology, as part of the Cybersecurity Maturity Model (CMM) for Fiji, delivered by the Oceania Cyber Security Centre (OCSC) in February 2024. The OCSC used the framework to redesign their question sets and develop a more comprehensive research agenda, leading to a holistic data-collection process that will inform Fiji's

national cyber strategy. Furthermore, the framework was used in a simulation exercise in Singapore to explore ASEAN responses to cybercrime, the gaps and successes. Overall, the rigorous scope of the framework enables a more thorough exploration of the context in which it is implemented. This enhanced understanding will serve for a vital role in refining national cybercrime strategies and help foster national resilience against evolving cyber threats.

Importantly, the SACC framework remains open-source, allowing for flexible use by interested parties. The authors are keenly interested in further understanding how the framework is used in practice, and are actively monitoring its implementation for insights into how the framework can be enhanced further.

About the authors

Joyce Hakmeh is the deputy director of the International Security Programme at Chatham House and co-editor of the *Journal of Cyber Policy*. She leads the institute's work on cyber policy, and provides regular analysis on issues that sit at the nexus between technology and geopolitics. She also oversees the research agenda of the international security programme and supervises its researchers.

Her recent research focuses on the geopolitics of cyberspace, international cyber capacity-building, gender-transformative approaches in cyber policy, the role of China in cyberspace, and the impact of emerging technologies on international security.

Joyce chaired the Global Forum on Cyber Expertise working group on cybercrime in 2018–22, and is a frequent panellist and chair at conferences at national and global events. She currently sits on the advisory boards of the Global Cyber Alliance and the DNS Research Federation. Previously, Joyce worked for the UN, the International Federation of Red Cross and Red Crescent Societies and various non-profit organizations. She received her master's degree in international law from SOAS, University of London.

Jamie Saunders is a security consultant, providing strategic advice to a range of governments and critical national infrastructure organizations. He is an Oxford Martin Fellow at the University of Oxford, where he supports the work of the Global Cyber Security Capacity Centre.

Jamie has spent the majority of his career in UK government service. In 2014–16, he was director of the UK National Crime Agency (NCA)'s National Cyber Crime Unit. Prior to working at NCA, he was the director of international cyber policy at the UK Foreign, Commonwealth & Development Office.

Acknowledgments

The authors would like to thank Global Affairs Canada (GAC) for their generous support of the project on 'Building anti-cybercrime capacity in ASEAN', from which this research paper was developed. The authors also extend their gratitude to the project advisory group members, who provided invaluable advice, and to the anonymous peer reviewers, whose feedback helped strengthen this research paper. Special thanks go to Amrit Swali, Robert Collett and Esther Naylor for their contributions throughout the project. Finally, the authors would like to thank Chris Matthews of the Communications and Publishing department at Chatham House for his editorial guidance and support.

Cover image: Amid panic buying and fears of a shut-down prompted by a ransomware attack on Colonial Pipeline, a petrol pump displays an 'out-of-order' notice, Arlington, Virginia, US, 12 May 2021.
Photo credit: Copyright © Andrew Caballero-Reynolds/AFP via Getty Images

ISBN 978 1 78413 547 8
DOI 10.55317/9781784135478

Cite this paper: Hakmeh, J. and Saunders, J. (2024), *The Strategic Approach to Countering Cybercrime (SACC) framework: Helping countries to tackle the growing threat to their economic and national security from cybercrime*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784135478.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223