Global Overview of existing national cyber capacity Assessment Tools (GOAT)

GLOBAL
FORUM ON
CYBER
EXPERTISE

Authors

This document has been developed by the Global Forum on Cyber Expertise (GFCE), Working Group A - Task Force Strategy and Assessments, as a project under its Work Plan 2020. The project team members are:

- Carolin Weisser Harris, Global Cyber Security Capacity Centre (GCSCC)
- Ian Wallace, Chair of GFCE Working Group A on Strategy and Policy
- James Boorman, Oceania Cyber Security Centre (OCSC)
- Orhan Osmani and Marwan Ben Rached, International Telecommunication Union (ITU)
- Melissa Hathaway and Francesca Spidalieri, Potomac Institute for Policy Studies (PIPS)
- Radu Serrano, e-Governance Academy (eGA)
- Kerry-Ann Barrett, Organization of American States (OAS).

The project team would like to extend its appreciation to the Australian Strategic Policy Institute (ASPI), the European Union Agency for Cybersecurity (ENISA), the MITRE Corporation and the World Bank for their comments and contributions; as well as to Kathleen Bei, GFCE Secretariat, for her design, logistical and organizational support. Thanks are also due to ITU for reviewing and editing this document and for translating it into the French and Spanish languages.

The information and views set out in this paper are those of the authors and do not necessarily reflect the official opinion or position of GFCE, its Secretariat or its members and partners. Neither GFCE nor its members may be held responsible for the use which may be made of the information contained therein.

Table of contents

Introduction

The global community has been deploying increasing efforts to understand nations' cybersecurity postures in order to diagnose gaps and make better-informed decisions on interventions and investments to enhance cyber capacity. Research institutions, regional organizations and companies have developed frameworks, models and indices and applied them across the globe, building the knowledge base on where countries stand in terms of cybermaturity and their preparedness in the face of increasing cyberthreats to governments, industry, businesses and citizens.

The positive feedback received from the session on Cyber Capacity Assessments organized at the GFCE V-Meeting in April 2020 highlighted the need to create awareness of the cyber capacity assessment tools that exist and to provide details on their methodologies, outputs and impact, in order to help the GFCE community (beneficiaries, funders and implementers) identify suitable tools and approaches geared to the prevailing needs and knowledge gaps.

Accordingly, this document aims to assist in the decision-making process by providing a comprehensive overview of the different tools, their approaches, benefits and outputs, and what to do and whom to contact if a country wishes to be assessed.

The GFCE Strategy and Assessments Task Force specifically selected tools that serve to assess a country's cyber capacity. On that basis, the following tools have been included:

- Combating Cybercrime: Capacity-Building Tool, The World Bank
- Cyber Maturity in the Asia-Pacific Region, Australian Strategic Policy Institute (ASPI)
- Cyber Readiness Index 2.0 (CRI), Potomac Institute for Policy Studies (PIPS)
- Cybersecurity Capacity Maturity Model for Nations (CMM), Global Cyber Security Capacity Centre (GCSCC)
- Cyber Strategy Development and Implementation Framework (CSDI), MITRE Corporation
- Global Cybersecurity Index (GCI), International Telecommunication Union (ITU)
- National Capabilities Assessment Framework (NCAF), European Union Agency for Cybersecurity (ENISA)
- National Cyber Security Index (NCSI), e-Governance Academy (eGA).

Other tools that meet the above criterion will be added to the document as they are identified.

For the purpose of this document, a questionnaire was sent to the organizations responsible for each tool, seeking information on the following:

- Implementer(s) and contact information
- Themes and topics
- Indicators
- Methodology, data collection and quality control
- Outputs and presentation
- Impact and benefits
- Role in the coordination of cyber capacity-building activity and the GFCE matchmaking process.

Combating Cybercrime: Capacity-Building Assessment Tool

The World Bank

The World Bank's *Combating Cybercrime: Capacity-Building Assessment Tool* ("Assessment Tool") was created under the auspices of the Combating Cybercrime project to support developing countries in identifying priority areas so as to facilitate allocation of their scarce capacity-building resources.

The Assessment Tool is unlike other assessment frameworks in that it is a self-diagnosis tool encompassing nine dimensions, namely: (1) Non-legal framework; (2) Legal framework; (3) Substantive law; (4) Procedural law; (5) E-evidence; (6) Jurisdiction; (7) Safeguards; (8) International cooperation; and (9) Capacity building.

The Assessment Tool can be used both for a standalone activity conducted by a country for its own purposes and also as an essential due-diligence tool to enable operational task teams to appraise a country's readiness to combat cybercrime.

Overview

Date tool was last updated	The last update of the publication was completed in 2017. We are in the process of updating the current assessment tool, which is scheduled to be completed by July 2020.
What is the name of the assessment tool?	Combating Cybercrime: Capacity-Building Assessment Tool
What is the name of the organization maintaining the tool?	The World Bank
Who are the implementers of assessments?	The tool is available as a global public good. Anyone can go to the site (see below) and download and use the tool. It is designed to be a self-assessment.
Please provide links to the tool and any additional information	https://www.combattingcybercrime.org/
Whom should I contact to discuss arranging an assessment?	Mr David Satola, Lead Counsel, Legal Vice Presidency, The World Bank
Geographical coverage	Global
Who can use the tool?	• Policy-makers • Legislators • Law-enforcement authorities • Civil society in developing countries • Any interested individuals
What are the themes or topics covered?	Conceptually, the assessment is organized around the following nine dimensions: • **Non-legal framework**, covering national strategies and policies and other matters of a non-legal nature such as cooperation with the private sector; • **Legal framework**, covering national law and whether a country has joined a treaty; • **Substantive law**, addressing activities that have been criminalized; • **Procedural law**, mainly addressing investigatory matters; • **e-Evidence,** focusing on admissibility and treatment of digital evidence in the cybercrime context; • **Jurisdiction**, focusing on how the jurisdiction of the crime is determined;

	• **Safeguards**, focusing on three elements: “due process”, data protection and freedom of expression; • **International cooperation**, focusing on, first, extradition, and, second, both formal and informal levels of mutual legal assistance (MLA); and • **Capacity building**, looking at both institutional (e.g. law-enforcement training academies) and human capacity building focusing on training needs for law enforcement, prosecution and the judiciary.
What are the GFCE themes or topics covered?	Policy and strategy ☒ Strategies ☒ Assessments ☐ CBMs and norms ☐ Cyber diplomacy ☒ International law in cyberspace Incident management and CIIP ☒ National computer security incident response ☐ Incident capture and analytics ☐ Cyber security exercises ☒ Critical information infrastructure protection Cybercrime ☒ Legal frameworks / Cybercrime law ☒ Law enforcement in cyberspace ☒ Cybercrime training ☒ Cybercrime prevention Culture and skills ☒ Cyber security awareness ☒ Education and training ☒ Workforce development Standards ☐ Open Internet standards ☐ Internet of Things
Type of indicators	Both quantitative and qualitative indicators
How many indicators are used and how are they applied?	The Assessment Tool consists of **115** indicators, which are grouped in nine dimensions: Non-legal framework, Legal framework, Substantive law, Procedural law, e-Evidence, Jurisdiction, Safeguards, International cooperation and Capacity building. In the Assessment Table, the nine dimensions are divided into four levels. **Level 1** designates each subject matter area (the dimension). **Level 2** sets a general frame for each question, which is asked in **Level 3** and may be further refined in **Level 4.** The last column (indicator) provides for a "yes/no" answer or a single choice from among a range of answers.
Methodology – what type of assessment is used?	**Case-specific:** The Combating Cybercrime team conducts an initial assessment of a client country based on desk research and then shares findings and verifies and validates assessments with responsible government authorities of the client country.
Primary data-collection method	• Publicly available information • Unpublished documents • Questionnaires and surveys • Observations • Documents and records

	• In person Interviews
Do you have a secondary data collection?	Yes. After initial desk research, the team makes a visit to the client country and consults with responsible government authorities to verify and validate the initial assessment. • Observations • Documents and records
What mechanisms do you adopt to ensure the accuracy of the data collected?	Combating Cybercrime team members, led by the ICT Lead Counsel at the World Bank, usually have cybercrime background/expertise and handle diverse ICT matters at the World Bank. Furthermore, the initial assessment conducted by the team members is verified and validated by responsible government authorities in client countries to ensure the accuracy of the data collected.
What are the main outputs of the assessment?	A "Cybercrime Capacity-Building Assessment Report" for each client country is created in each iteration.
Presentation format of the assessment outputs	• Cybercrime Capacity-Building Assessment Report (PDF) • Visualization tool (Excel graphic charts)
Can the assessment outputs be published?	Yes. However, it is at the discretion of the client country to publish the results of the assessment.
How can previous reports be accessed?	Access to previous reports is at the discretion of the client country.
What evidence is there of impact?	The team has conducted Cybercrime Capacity-Building Assessments for client countries in the Africa and Asia-Pacific regions, including Namibia, Ethiopia, Kenya, Micronesia and Myanmar. In addition, the team has received new requests for assessment from 22 countries (Benin, Burundi, Democratic Republic of the Congo, Gambia, Liberia, Mali, Niger, Nigeria, Republic of the Congo, Sierra Leone, Tanzania, Uganda, Zambia, Burkina Faso, Cabo Verde, Comoros, Morocco, Cameroon, Mauritania, Rwanda and Senegal). Furthermore, one of our partner organizations, the United Nations Office on Drugs and Crime (UNODC), has adopted the Assessment Tool as its exclusive assessment methodology for assessing cybercrime preparedness. Lastly, the team has presented the Assessment Tool at the following events: GFCE Annual Meeting in Singapore (2018) and Working Group meetings in The Hague (2018 and 2019); Council of Europe (CoE) annual meeting in Strasbourg (2019); International Association of Prosecutors (IAP) annual conferences in South Africa (2018) and Argentina (2019); joint meeting of CoE and the African Union (AU) on building capacity to combat cybercrime in Africa (2018); and Colloquium on International Law in Hong Kong, China (2019).
What are the benefits of conducting an assessment?	The Assessment Tool enables effective and universally applicable assessment of a nation's cybercrime preparedness by ensuring objectivity, richness and accessibility. The combination of these three features of the Assessment Tool places policy-, law- and decision-makers in a position to best decide how resources should be allocated. • **Objectivity** is achieved by making the response to each question in the Assessment Tool a binary "yes/no" answer to the greatest extent possible or a clear choice along a small scale of options. • **Richness** is achieved by "weighting" each criterion. The Assessment Tool uses some 115 indicators grouped into nine themes (or dimensions). • **Ease of comprehension** is achieved through graphic representations of assessment in a single "spider" chart. The chart helps the client country to identify whether its current practice is in line with international good practices. Each dimension on the general spider chart can also be drilled down to a more granular level showing performance on each of the different sub-criteria.
Do you have a weightage calculation process?	Yes. However, the specific weightage calculation process is not disclosed to users to prevent manipulation of the Assessment Tool.

Do you adopt a scoring and/or ranking mechanism in your assessment?	No. There is no scoring or ranking of results.

Details

What key questions can the tool help to answer?	• Are there existing national cybersecurity strategies and policies in place? **(Non-legal framework)** • Has there been any domestic legislation on cybercrime? Has a country joined any treaties on cybercrime? **(Legal framework)** • Does a country criminalize traditional crime committed by/through computer-related activities or newly emerged cybercrime? **(Substantive law)** • Are there procedural laws governing investigation and prosecution of cybercrimes? (**Procedural law)** • Has a country implemented rules specific to admissibility and treatment of e-Evidence? • How does a country determine the jurisdiction of cybercrime? (**Jurisdiction)** • Does a country ensure “due process” (data protection and freedom of expression) for its citizens? **(Safeguards)** • Has a country implemented extradition procedures or formal/informal MLA principles at an international level? **(International cooperation)** • Are there cybercrime capacity-building institutions or programs for law-enforcement officials, prosecutors and judges?
At what point in the strategy lifecycle should the assessment occur?	• Initiation • Stocktaking and analysis • Production of the strategy • Implementation • Monitoring and evaluation The first use of the Assessment Tool will provide a baseline, while periodic updating of the results using the tool will facilitate monitoring of progress.
How does the assessment help to align other activities?	The Assessment Tool serves to identify a country’s priority areas within the nine dimensions, which in turn facilitates focused and targeted allocation of scarce capacity-building resources for establishing a national strategy to build a country’s capacity to combat cybercrime. Hence, the Assessment Tool can be used both for a standalone activity conducted by a country and as an essential due-diligence tool to enable operational task teams to assess and appraise a country’s cybercrime preparedness.
What role does the assessment play in the GFCE matchmaking process?	The Assessment Tool would contribute to the GFCE’s matchmaking process by providing a solid and objective baseline from which to plan and implement its cyber capacity-building activities.
What case studies or testimonials are available regarding the benefits of the tool?	As stated above, the benefits of the Assessment Tool have been demonstrated through the successful performance of Cybercrime Capacity-Building Assessments in a number of client countries, and recognition by our partner organization UNODC, which now uses the Assessment Tool as its exclusive assessment methodology for assessing cybercrime preparedness.
What are the mechanisms to ensure the independence, impartiality and neutrality of your results?	• The Assessment Tool has been evaluated and validated by our partner organizations, including CoE, ITU, UNODC, the United Nations Conference on Trade and Development (UNCTAD), the Supreme Prosecutors Office of the Republic of Korea (KSPO) and GCSCC (University of Oxford). • An independent group of experts contributed to determining the weightages of each indicator in the Assessment Tool.

Cyber Maturity in the Asia-Pacific Region

Australian Strategic Policy Institute (ASPI)

Cyber Maturity in the Asia-Pacific Region is an annual report issued by the Australian Strategic Policy Institute (ASPI) that examines cybermaturity trends across Asia and the Pacific. It surveys a wide geographical and economic cross-section of the region, encompassing 25 countries from South, North and Southeast Asia, the South Pacific and North America.

The 'cyber maturity metric' methodology assesses the various facets of States' cybercapabilities. The model has been refined through engagement with Asia-Pacific experts and stakeholders so that it effectively assesses changes in State approaches and technological developments. 'Maturity' in this context is demonstrated by the presence, effective implementation and operation of cyber-related structures, policies, legislation and organizations. These indicators of cyber maturity cover whole-of-government policy and legislative structures, responses to financial cybercrime, military organization, business and digital economic strength, and levels of social cyberawareness.

The research base underpinning each of these indicator groups has been collated exclusively from information in the public domain; in other words, the report's conclusions are based solely on open-source material.

Overview

Date tool was last updated	2017
What is the name of the assessment tool?	Cyber Maturity in the Asia-Pacific Region
What is the name of the organization maintaining the tool?	Australian Strategic Policy Institute (ASPI)
Who are the implementers of assessments?	Australian Strategic Policy Institute (ASPI)
Please provide links to the tool and any additional information	https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017
Whom should I contact to discuss arranging an assessment?	Ms Danielle Cave, Deputy Director, International Cyber Policy Centre, ASPI Mr Tom Uren, Senior Analyst, International Cyber Policy Centre, ASPI Mr Bart Hogeveen, Head of Cyber Capacity Building, ASPI
Geographical coverage	Regional
Who can use the tool?	Anyone. The report is publicly available.
What are the themes or topics covered?	**1. Governance** The governance topic addresses the State's organizational approach to cyber issues, including the composition of government agencies engaged on those issues; the State's legislative intent and ability; and the State's engagement on international cyberpolicy issues such as Internet governance, the application of international law and the development of norms or principles. These indicators provide guidance for

	diplomatic, government, development, law-enforcement and private-sector engagement in Asia–Pacific States. **2. Financial cybercrime enforcement** Financial cybercrime is a critical issue for all States in Asia and the Pacific. The effect of cybercrime on ordinary people in the region is considerable and includes significant financial losses. Understanding the State’s capacity to address financial cybercrime can guide engagement on enforcement, including through information sharing and capability-development assistance from the public and private sectors. **3. Military application** This topic addresses the State’s military organizational structure (if any) relating to cyberspace and the State’s known views on the use of cyberspace by its armed forces. This can guide military-to-military engagement between States as well as diplomatic and political–military engagement. Military uses of cyberspace, particularly national capabilities, are a sensitive topic for all Asia–Pacific countries, so this area requires careful consideration before States seek or agree to engage with one another. **4. Digital economy and business** Whether the State understands the importance of cyberspace and the digital economy, and how it understands them to be economically important, is an indicator of cybermaturity. This can guide engagement on capacity building, regional business links and engagement between government and business on cybersecurity. **5. Social engagement** Public awareness of and engagement on cyber issues, such as Internet governance, Internet censorship and cybercrime, indicate the maturity of public discourse between the government and its citizens. Educational programmes on ICT and cyber issues could also indicate a high level of technical and issue-based understanding. The proportion of a State’s population with Internet connectivity indicates the type of business and personal engagement in cyberspace, the quality of ICT infrastructure and the level of citizens’ trust in digital commerce. This can guide development agencies seeking to build regional economies and businesses wanting to develop trade in the region.
What are the GFCE themes or topics covered?	Policy and strategy ☒ Strategies ☒ Assessments ☒ CBMs and norms ☒ Cyber diplomacy ☒ International law in cyberspace Incident management and CIIP ☒ National computer security incident response ☐ Incident capture and analytics ☐ Cyber security exercises ☒ Critical information infrastructure protection

	Cybercrime ☒ Legal frameworks / cybercrime law ☒ Law enforcement in cyberspace ☐ Cybercrime training ☐ Cybercrime prevention Culture and skills ☒ Cyber security awareness ☒ Education and training ☒ Workforce development Standards ☐ Open Internet standards ☐ Internet of Things
Type of indicators	Quantitative indicators and qualitative indicators
How many indicators are used and how are they applied?	The ‘cyber maturity metric’ contains 10 indicators. The indicators were weighted according to their importance to a State’s cybermaturity. A group of cyberexperts and stakeholders from government agencies and the private sector weighted them on a scale of 1 to 10, where 1 is ‘not important at all’ and 10 ‘extremely important’. These expert weightings for each category were then averaged to produce a weighting factor that could be used in the calculation of an overall score. In the final step, each country was then rated against the 10 factors, on a scale of 0 to 10 (10 being the highest level of maturity). The assessments were based on extensive qualitative and quantitative open-source research and, where possible, a comparison with the research and results from 2014, 2015 and 2016. The overall score for each country was the sum of the scores against each factor weighted by the average calculated importance. To aid interpretation, the overall scores were converted to a percentage of the highest possible score, given the assigned weights: $$\overline{S} = 10 \times \frac{\sum_i S_i w_i}{\sum_i w_i}$$ where $\overline{S}$ = weighted score, *S* = score and *w* = weight.
Methodology – what type of assessment is used?	Comparative, with rank
Primary data-collection method	Open-source information
Do you have a secondary data collection?	• Interviews • Questionnaires and surveys • Observations • Focus groups

What mechanisms do you adopt to ensure the accuracy of the data collected?	Embassies and high commissions of countries that are covered by the report are invited to fact-check their country profile.
What are the main outputs of the assessment?	- Individual country profiles - Regional comparative ranking - Overview of regional trends - Assessment of international engagement opportunities.
Presentation format of the assessment outputs	Report
Can the assessment outputs be published?	Yes. Results are published with a report.
How can previous reports be accessed?	https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2016 https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2015 https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2014
What evidence is there of impact?	See the answer on ‘testimonials’ below
What are the benefits of conducting an assessment?	See the answer on ‘point in strategy lifecycle’ below
Do you have a weightage calculation process?	Yes. See the answer on ‘indicators and how they are applied’ above
Do you adopt a scoring and/or ranking mechanism in your assessment?	Yes. See the answer on ‘indicators and how they are applied’ above

Details

What key questions can the tool help to answer?	What are regional trends in cybermaturity across the Asia-Pacific region? How do countries in Asia and the Pacific compare across five policy topics that make up cybermaturity? What opportunities for international engagement exist with Asia-Pacific countries?
At what point in the strategy lifecycle should the assessment occur?	The metric looks at the Asia-Pacific region from a comparative perspective. For developing a national cyberstrategy, the reports are best suited in the phases of initiation, stocktaking, and monitoring and evaluation (M&E). When developing a regional approach, or developing a regional ‘picture’, the tool is suitable for agenda-setting, strategic-level analyses and comparisons of national practices. The annual cycle of the report makes it valuable for M&E and trend analyses.
How does the assessment help to align other activities?	The report provides an authoritative source of fact- and evidence-based analysis for the benefit of national, regional, public- and private-sector policy-makers.

What role does the assessment play in the GFCE matchmaking process?	The report provides potential entry points for conversations between recipients and providers of cyber capacity building.
What case studies or testimonials are available regarding the benefits of the tool?	The report tends to be picked up by media: • https://www.zdnet.com/article/only-us-tops-australia-in-asia-pacific-cyber-maturity-aspi/ • https://www.theaustralian.com.au/commentary/opinion/threat-posed-by-evil-nations-and-criminals-in-cyberland-is-rising/news-story/fdebd93f3dc0206afe0705e6f6ec045c • https://vovworld.vn/en-US/spotlight/vietnam-ranks-9th-in-cyber-maturity-in-asiapacific-region-379580.vov • https://theaseanpost.com/article/cyberattack-malaysia-imminent-or-imagined The report is referenced in speeches, including by leading (Australian) politicians: • https://www.rusi.org.au/resources/Documents/2015_10_05%20Brodtman.pdf The report is used as a source in other policy and academic publications, such as: • https://www.austcyber.com/resources/sector-competitiveness-plan/executive-summary • https://www.swp-berlin.org/fileadmin/contents/projects/BCAS2015_Maurer_Tim_Web.pdf • https://www.standards.org.au/getmedia/952ea009-ffc2-490a-905f-8f731fa84a52/Pacific-Islands-Cyber-Security-Standards-Cooperation-Agenda.pdf.aspx
What are the mechanisms to ensure the independence, impartiality and neutrality of your results?	As implementer, ASPI is governed by its charter, in which independence and non-partisanship are enshrined. Furthermore, the report is written on the basis of open and verifiable sources. Observations or conclusions are not subject to approval by any government or funding provider.
Please add any further information	The report was last published in December 2017 in anticipation of new funding and a reassessment of potential research outputs.

Cyber Readiness Index 2.0 (CRI)

Potomac Institute for Policy Studies (PIPS)

The *Cyber Readiness Index 2.0* (CRI) provides a comprehensive, comparative, experience-based methodology to assess countries' commitment and maturity in regard to securing their national digital infrastructure and services upon which their economic growth and national resilience depend. CRI 2.0 built on the 2013 Cyber Readiness Index 1.0, which was the first available methodological framework for assessing cyber readiness. The CRI assessment tool can help countries identify existing gaps, strengthen their current cybersecurity posture, and better manage national-level cyber risk.

Since 2013, CRI has been applied to over 100 countries and 14 in-depth reports have been completed.

Overview

Date tool was last updated	We are regularly adding new questions and indicators to each of the seven essential elements in the tool.
What is the name of the assessment tool?	Cyber Readiness Index 2.0
What is the name of the organization maintaining the tool?	Potomac Institute for Policy Studies (PIPS)
Who are the implementers of assessments?	Members of the Cyber Readiness team (Ms Melissa Hathaway and Ms Francesca Spidalieri)
Please provide links to the tool and any additional information	• PIPS website: https://www.potomacinstitute.org/academic-centers/cyber-readiness-index • Cybil portal: https://cybilportal.org/tools/cyber-readiness-index-2-0/
Whom should I contact to discuss arranging an assessment?	• Melissa Hathaway, PIPS Senior Fellow and CRI Principal Investigator: hathawayglobal@icloud.com • Francesca Spidalieri, CRI Co-Principal Investigator: francescaspidalieri@gmail.com
Geographical coverage	Global
Who can use the tool?	• Global leaders • National/regional governments • Ministries/government agencies • Cybersecurity agencies/policy-makers • Academia • Cybersecurity experts • Individual researchers

What are the themes or topics covered?	CRI 2.0 uses over 70 unique indicators across seven essential elements to discern operationally ready activities and identify areas for improvement in the following categories: 1. **National strategy**: Publication of a national strategy; designation of a competent authority; identification of key government entities and key commercial entities responsible for implementation; mechanisms to secure critical infrastructure; identification of critical services; identification of national standards for continuity of service. 2. **Incident response**: Publication of an incident response plan; identification of cross-sector dependencies; evidence that the plan is exercised and updated; publication of a cyberthreat assessment; establishment of a computer security incident response team (CSIRT); financial and human resources. 3. **E-crime and law enforcement**: Ratification of international cybercrime treaty; efforts to reduce e-crime; institutional ability to fight cybercrime; commitment to review existing laws and mechanisms; efforts to clean up infected infrastructure; law-enforcement training and capability development. 4. **Information sharing**: Policy on information sharing; institutional structure to share information with government agencies and/or industry; evidence of cross-sector and cross-stakeholder coordination mechanisms; ability and processes for the government to declassify intelligence information. 5. **Investment in R&D, education and capacity**: Government incentive mechanisms to encourage cybersecurity innovation and investments; financial and human resources for R&D and technology transfer; degree programmes in cybersecurity; sponsorship of cybersecurity awareness campaigns and educational programmes. 6. **Diplomacy and trade**: Identification of cybersecurity as an essential element of foreign policy and international economic negotiations; establishment of dedicated personnel for cyber diplomacy in a country's foreign office; participation in and enforcement of international, multinational and regional cybersecurity agreements. 7. **Defence and crisis response**: Establishment of national-level military and/or non-military organization for cyber defence; evidence of national-level cyberexercises with commercial partners and/or international partners; establishment of standards for responsible State behaviour in cyberspace; establishment of rapid assistance mechanisms. For a complete description of each essential element, refer to the full methodology: https://www.potomacinstitute.org/images/CRIndex2.0.pdf

What are the GFCE themes or topics covered?	Policy and strategy ☒ Strategies ☒ Assessments ☒ CBMs and norms ☒ Cyber diplomacy ☒ International law in cyberspace Incident management and CIIP ☒ National computer security incident response ☒ Incident capture and analytics ☒ Cyber security exercises ☒ Critical information infrastructure protection Cybercrime ☒ Legal frameworks/cybercrime law ☒ Law enforcement in cyberspace ☒ Cybercrime training ☒ Cybercrime prevention Culture and skills ☒ Cyber security awareness ☒ Education and training ☒ Workforce development Standards ☒ International and/or national standards
Type of indicators	The data collection under CRI 2.0 is qualitative and each indicator is assessed across four key categories: (1) Statements/strategies/policies; (2) Organization/competent authority; (3) Resources; and (4) Implementation.
How many indicators are used and how are they applied?	CRI 2.0 users over 70 indicators across seven essential elements to evaluate a country's cybersecurity maturity and discern areas that are fully operational, partially operational, or where insufficient evidence is available. All CRI 2.0 indicators share a common structure, and questions asked in one version of the methodology are comparable to similar questions in previous or future versions. Every indicator is given the same weight and then described in the country report as part of a broader context based on the country's needs, capabilities, priorities and objectives.
Methodology – what type of assessment is used?	CRI 2.0 uses primary sources, including national strategies, policies, legislation, leaders' official statements, national assessments and reports, etc., to assess countries' cybermaturity and develop in-depth country profiles. ⇒ Countries are not ranked against each other.

Primary data-collection method	• Open-source information • Unpublished or official confidential documents • Interviews/observations • Documents and records
Do you have a secondary data collection?	Yes. Secondary data collection is conducted to corroborate, correct or broaden information collected during our analysis of primary sources and interviews with country officials and experts.
What mechanisms do you adopt to ensure the accuracy of the data collected?	All our research is based on primary sources and official documentation, and then corroborated by in-country officials and/or subject-matter experts.
What are the main outputs of the assessment?	In-depth country reports are published on the PIPS website and publicly available in all six UN languages. These reports can help governments still developing their cybersecurity practices and policies and provide an actionable blueprint of priorities required to strengthen their cybersecurity posture, enabling governments to recognize actions to be taken to reduce risks irrespective of their existing in-house expertise.
Presentation format of the assessment outputs	• In-depth country reports • Visualization tool (radar graph and "Harvey Balls" chart) • PowerPoint presentation, if requested by the country
Can the assessment outputs be published?	Yes. All CRI country reports are publicly available on the PIPS' CRI webpage: https://www.potomacinstitute.org/academic-centers/cyber-readiness-index
How can previous reports be accessed?	See above.
What evidence is there of impact?	The CRI has directly influenced cyberreadiness policies and leadership thinking in the following countries and organizations: Australia, Azerbaijan, Bangladesh, Bosnia and Herzegovina, Bulgaria, Canada, China, Czech Republic, Egypt, Estonia, France, Georgia, Germany, Iceland, India, Indonesia, Israel, Italy, Japan, Jordan, Kyrgyzstan, Lithuania, Mexico, the Netherlands, New Zealand, Oman, Philippines, Poland, Romania, Saudi Arabia, Serbia, Slovakia, South Africa, Sweden, Switzerland, Ukraine, the United Kingdom; African Forum of computer incident response teams (Africa CERT), Asia-Pacific Computer Emergency Response Team (APCERT), ITU, Inter-American Development Bank (IDB), North Atlantic Treaty Organization (NATO), Nordic Council, Organization of American States (OAS) and the World Bank. The CRI continues to have a global impact, and its principal investigator, Melissa Hathaway, has reinforced the education of leaders around the world on these matters. She is routinely invited to senior-level international engagements and discussions, is featured in multiple international publications and continues to inform national leaders on the practicality of using CRI 2.0 as a tool for planning/benchmarking and ensuring the participation of various stakeholders in national cybersecurity efforts and processes and increasing funding for cybersecurity capacity building.

What are the benefits of conducting an assessment?	The CRI 2.0 assessment can help countries identify gaps between their current cybersecurity posture and the national cybercapabilities needed to support their digital future. The tool can also be used to assess where a country is on a maturity curve from whole-of-government and whole-of-nation perspectives. When taken together, the indicators can help governments assess and align their digital and national security initiatives. Through the data collected, the CRI can also highlight best practices that countries can implement to facilitate and help drive cyberpreparedness efforts across industries and sectors as well. CRI 2.0 emphasizes the tools that national leaders can leverage, including policy, legislation, regulations, standards, market incentives and other initiatives, to protect the value of their digital investments and address ongoing economic erosion from cyberinsecurity. Such an assessment can help national leaders recognize that realizing the full potential of the digital economy in terms of economic growth, increased productivity and efficiency, enhanced workforce skills and improved access to business and information requires aligning economic development strategies with national security priorities. It exemplifies how ICTs can deliver economic growth, but only if the right policies, processes and technologies are put in place to protect and secure the cyberinfrastructure and cyber services upon which a country's digital future and growth depend.
Do you have a weightage calculation process?	Yes. In our internal database we assign a score of 5.0 to indicators that are fully operational, 3.0 to partially operational ones, and 1.0 when specific elements are classified or there is insufficient evidence of their existence or implementation. The weighting calculation is only used to create radar graphs and other visuals, but not to rank countries.
Do you adopt a scoring and/or ranking mechanism in your assessment?	CRI 2.0 provides a maturity score for each essential element but does not rank countries.

Details

What key questions can the tool help to answer?	• Are the country's short- and long-term goals, including digital agenda, industrial policies, economic objectives and national security priorities, aligned with its national cybersecurity strategy? • What kind of cyberthreats could put these objectives at risk or disrupt the achievement of these objectives? • What are the country's most critical digital dependencies (e.g. companies, services, infrastructure and assets) that, if harmed, would have grave economic and national security consequences? • Are there clear lines of accountability and responsibility to ensure that the country's objectives are achieved and that risk-reduction measures are implemented? • Have cybersecurity and resilience considerations been a core part of the planning process? • What steps can the country take to become more digitally resilient? CRI 2.0 can also be referenced as a benchmark for countries to identify gaps between their current cybersecurity posture and the national cybercapabilities needed to correct deficiencies and support the country's future economic and security priorities. Government leaders may use CRI 2.0 to facilitate and help drive cyberpreparedness efforts across industries and sectors as well, thus constantly keeping focus on the linkage between their digital and industrial strategy and their national security priorities.
At what point in the strategy lifecycle should the assessment occur?	The CRI methodology should be part of the entire strategy lifecycle and its assessment tool can be used before and/or after the development of a national cybersecurity strategy, including during: Initiation / Stocktaking and analysis / Production of the strategy / Implementation / Monitoring and evaluation / Updating the strategy.
How does the assessment help to align other activities?	CRI 2.0 links economic growth and development to national security policies, and thus can help countries better align their national cybersecurity strategy with their digital and growth strategies.
What role does the assessment play in the GFCE matchmaking process?	CRI 2.0 can corroborate or complement other assessment tools endorsed by GFCE, including the Oxford CMM and ITU's GCI.

What case studies or testimonials are available regarding the benefits of the tool?	In addition to all the countries and international organizations listed above that have used the CRI to inform their policies and strategies, the CRI methodology has been cited or utilized in multiple articles, speeches, briefings, reports and derivative publications. For example, OAS and IDB employed the CRI 2.0 methodology and database to corroborate and validate their international report on member countries' level of cyber capacity and readiness (Cybersecurity: Are We Ready in Latin America and the Caribbean?). The CRI team has actively worked with ITU to exchange data, align efforts, amplify impacts and contribute to two of the latter's seminal projects on cybersecurity – development of the second iteration of the ITU's Global Cybersecurity Index (GCI), and creation of the ITU-led multipartner Guide to Developing a National Cybersecurity Strategy. Additional CRI 2.0 media coverage can be found under "Cyber Readiness in the News": https://www.potomacinstitute.org/academic-centers/cyber-readiness-index
What are the mechanisms to ensure the independence, impartiality and neutrality of your results?	Country reports are based on primary source data and independently validated by our team of experts.

Cybersecurity Capacity Maturity Model for Nations (CMM)

Global Cyber Security Capacity Centre (GCSCC), University of Oxford, and partners

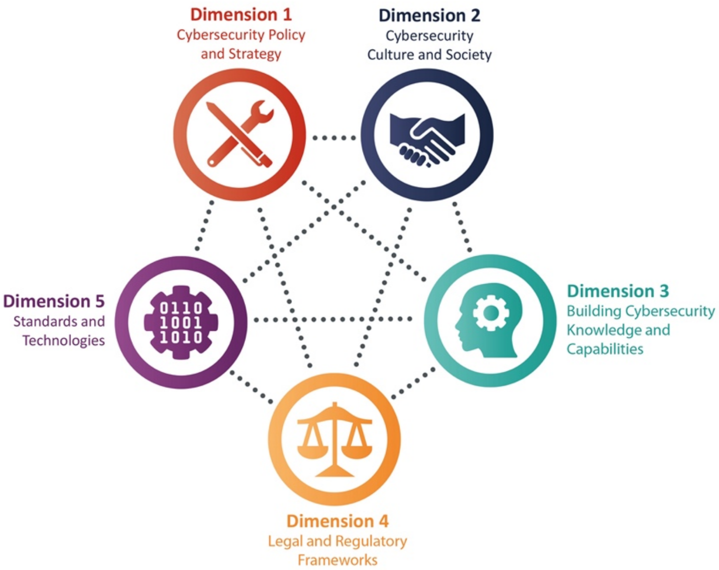
The *Cybersecurity Capacity Maturity Model for Nations* (CMM), developed by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, serves to benchmark a country's cybersecurity capacity across five dimensions, thereby enabling nations to self-assess, better plan investments and national cybersecurity strategies and set priorities for capacity development. Since 2015, more than 110 CMM reviews in over 80 countries have been completed across the world.

GCSCC and its partners define cybersecurity capacity broadly to span policy, strategy, social and cultural factors, education and training, law and regulation, and cybertechnologies and standards. In line with this definition, its research approach is multidisciplinary, tackling cybersecurity capacity across all of its dimensions from multiple academic perspectives.

The CMM was developed with the intention to research the nuances of capacity building across and within these multiple dimensions; the types of activities which can deliver and increase capacity; where best practice exists; the conditions under which increases in capacity should be sought; and the ways in which the dimensions relate to and depend upon each other for success. With this aim, the CMM also provides a framework that supports comparison of cybersecurity capacity across different nations in the world and over time. Its methodology serves to collect insights from different actors and stakeholder groups in order to reflect a broad view of cybersecurity capacity in each nation.

Overview

Date tool was last updated	March 2021
What is the name of the assessment tool?	Cybersecurity Capacity Maturity Model for Nations (CMM), 2021 edition
What is the name of the organization maintaining the tool?	Global Cyber Security Capacity Centre (GCSCC) Oceania Cyber Security Centre (OCSC) Cybersecurity Capacity Centre for Southern Africa (C3SA)
Who are the implementers of assessments?	Global Cyber Security Capacity Centre (GCSCC), Oceania Cyber Security Centre (OCSC), Cybersecurity Capacity Centre for Southern Africa (C3SA), Organization of American States (OAS), the World Bank, NRD Cyber Security Implementation partners: International Telecommunication Union (ITU); Global Forum on Cyber Expertise (GFCE); Commonwealth Telecommunications Organization (CTO); Asia Pacific Network Information Centre (APNIC); Asia-Pacific Telecommunity (APT); Norwegian Institute of International Affairs (NUPI); German Corporation for International Cooperation GmbH (GIZ), Germany
Please provide links to the tool and any additional information	https://gcscc.ox.ac.uk/the-cmm
Whom should I contact to discuss arranging an assessment?	Global Cyber Security Capacity Centre (GCSCC), global, Ms Carolin Weisser Harris: carolin.weisser@cs.ox.ac.uk Oceania Cyber Security Centre (OCSC), Oceania region, Mr James Boorman: james.boorman@ocsc.com.au

	Cybersecurity Capacity Centre for Southern Africa (C3SA), Africa region, Ms Nthabiseng Pule: npule@researchictafrica.net
Geographical coverage	Global
Who can use the tool?	Anyone. The CMM is a publicly available document. To conduct a CMM review it is recommended to work with one of the implementers who are familiar with the CMM methodology
What are the themes or topics covered?	The CMM looks at cybersecurity capacity through the five dimensions crucial to building a country's cybersecurity capacity:  Dimension 1 Cybersecurity Policy and Strategy Dimension 2 Cybersecurity Culture and Society Dimension 3 Building Cybersecurity Knowledge and Capabilities Dimension 4 Legal and Regulatory Frameworks Dimension 5 Standards and Technologies 0110 1001 1010 **Dimension 1 (*Cybersecurity policy and strategy*)** explores the country's capacity to develop and deliver cybersecurity strategy and enhance its cybersecurity resilience through improving its incident response, cyberdefence and critical infrastructure protection capacities. This dimension considers effective strategy and policy in delivering national cybersecurity capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general. **Dimension 2 (*Cybersecurity culture and society*)** reviews important elements of a responsible cybersecurity culture, such as the understanding of cyber-related risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online. Moreover, this dimension explores the existence of reporting mechanisms functioning as channels for users to report cybercrime. In addition, it reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour. **Dimension 3 (*Building cybersecurity knowledge and capabilities*)** reviews the availability, quality and uptake of programmes for various groups of stakeholders, including the government, the private sector and the population as a whole, and relates to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes and professional training programmes. **Dimension 4 (*Legal and regulatory frameworks*)** examines the government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation and related legislation. The capacity to

	enforce such laws is examined through law enforcement, prosecution, regulatory bodies and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime. **Dimension 5 (*Standards and technologies*)** addresses effective and widespread use of cybersecurity technology to protect individuals, organizations and national infrastructure. This dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls and the development of technologies and products in order to reduce cybersecurity risks.
What are the GFCE themes or topics covered?	Policy and strategy ☒ Strategies ☒ Assessments ☒ CBMs and norms ☒ Cyber diplomacy ☐ International law in cyberspace Incident management and CIIP ☒ National computer security incident response ☒ Incident capture and analytics ☒ Cyber security exercises ☒ Critical information infrastructure protection Cybercrime ☒ Legal frameworks/cybercrime law ☒ Law enforcement in cyberspace ☒ Cybercrime training ☒ Cybercrime prevention Culture and skills ☒ Cyber security awareness ☒ Education and training ☒ Workforce development Standards ☒ International and/or national standards

Type of indicators	Qualitative indicators
How many indicators are used and how are they applied?	The CMM covers about 600 indicators to rate maturity on five dimensions crucial to building a country's cybersecurity capacity: *Cybersecurity policy and strategy*; *Cybersecurity culture and society*; *Building cybersecurity knowledge and capabilities*; *Legal and regulatory frameworks*; and *Standards and technologies*. Each CMM ***Dimension*** comprises a set of ***Factors***, which describe and define what it means to possess cybersecurity capacity. Most of the factors are broken down into several ***Aspects***. Each factor/aspect has a series of ***Indicators*** within five ***Stages*** of maturity: *Start-up*, *Formative*, *Established*, *Strategic* and *Dynamic*. These indicators describe the steps and actions that must be taken to achieve or maintain a given stage of maturity in the aspect/factor/dimension hierarchy. In order for a country to demonstrate its assessed maturity within a given aspect/factor, every indicator needs to be evidenced; otherwise, the country cannot be seen to have progressed to consideration of the following stage.
Methodology – what type of assessment is used?	Deployment of the CMM is a multistep and multistakeholder process, and consists of three main stages: 1) Contextualizing desktop research conducted by the implementation team. 2) In-country modified focus group discussions over three to four days with key stakeholders, such as academia, criminal justice, law enforcement, information technology officers and representatives from public-sector entities, critical infrastructure owners, policy-makers, information technology officers from the government and the private sector (including financial institutions), telecommunication companies, the banking sector, as well as civil society and international partners. 3) A detailed CMM report which describes the in-country cybersecurity context, summarizes the findings for each factor and aspect of the CMM, outlines the stages of cybersecurity capacity maturity and provides recommendations that enable the country to enhance its cybersecurity capacity. The report is peer-reviewed by the GCSCC Technical Board and submitted to the government for comment. For more details, visit: https://gcscc.ox.ac.uk/cmm-review-process
Primary data-collection method	• Modified focus groups (main primary data collection) • Questionnaires and surveys (OAS regional studies) • Interviews (optional to obtain additional evidence)

Do you have a secondary data collection?	Yes (as part of desktop research before/after the CMM focus groups) • Open-source information • Unpublished documents • Documents and records • Questionnaires and surveys
What mechanisms do you adopt to ensure the accuracy of the data collected?	• Each of the CMM modified focus group discussions relates to one or more dimensions, which allows evidence to be gathered against each dimension at least twice. This also enables the triangulation and collection of different answers to the same question from different stakeholders. • With prior consent, CMM modified focus group sessions are recorded and some implementers use anonymized transcripts of the sessions to analyse responses to questions across the review dataset. • The desktop research confirms evidence from the CMM modified focus groups. • The CMM report is peer-reviewed by the GCSCC Technical Board and submitted to the government for comment. • Some implementers use the structured field coding (SFC) tool, which allows them to enter and code the answers from desktop research and CMM focus groups, enabling them to validate indicators at each stage of the review process. The methods are evolving with the introduction of the SFC tool, which testifies to the constant drive to improve on the CMM review methodologies.
What are the main outputs of the assessment?	An evidence-based report that is submitted to the government
Presentation format of the assessment outputs	• Written report including recommendations (PDF) • Executive summary presentation to the host (optional) • Validation workshop with the host and key stakeholders (optional) • Visualization tool (OAS: https://www.cybersecurityobservatory.org)
Can the assessment outputs be published?	Yes. It is at the discretion of the government to share and/or publish the report or any parts of it.
If yes, how can previous reports be accessed?	All CMM reviews, including links to published reports, can be found on the following websites: • https://gcscc.ox.ac.uk/cmm-reviews • https://cybilportal.org/tools/portal-of-cybersecurity-capacity-maturity-model-cmm- review-reports/ (For details on the status of the report, check on CYBIL Portal by searching "CMM+country name")
What evidence is there of impact?	An independent evaluation of a sample of CMM deployments in February 2020 found that: • The CMM review increased cybersecurity awareness and capacity building. • The CMM review contributed to greater collaboration within government. • Countries cited the CMM as foundational to their strategy and policy development (e.g. North Macedonia, Lithuania, and Georgia). • The CMM review enhanced internal credibility of the cybersecurity agenda within governments. • The CMM review helped define roles and responsibilities within governments.

	• The CMM review increased funding for cybersecurity capacity building. • The CMM review helped enable networking and collaboration with business and wider society. The CMM has been completed more than 120 times, with CMM deployments in over 85 countries, working with national governments in all regions of the world. This includes: • Two regional studies (2016 and 2020) by the Organization of American States (OAS) • Over 25 reviews in collaboration with the World Bank and the Korea Internet and Security Agency (KISA) on their Global Cybersecurity Capacity Programmes phase I and phase II and as part of the National Cybersecurity Capacity (CMM) Reviews for the Commonwealth and the ECOWAS programme portfolio • Computer Emergency Response Team (CERT) and Capacity Assessments in the Pacific with ITU, APT, APNIC and other partners • Cybersecurity Capacity Building in the Commonwealth with the CTO. The data from the CMM reviews were used for the following academic papers: • Creese, S., Shillair, R., Bada, M., Reisdorf, B. C., Roberts, T. and Dutton, W. H. (2019). 'The Cybersecurity Capacity of Nations', pp. 165-179 in Graham, M. and Dutton, W. H. (eds), *Society and the Internet: How Networks of Information and Communication are Changing our Lives*, 2nd edition. Oxford: Oxford University Press. • Dutton, W. H., Creese, S., Shillair, R. and Bada, M. (2019). 'Cyber Security Capacity: Does It Matter?'. *Journal of Information Policy*, 9: 280-306. doi:10.5325/jinfopoli.9.2019.0280 • Creese, S., Dutton, W. H., Esteve-González, P. and Shillair, R. (2021). 'Cybersecurity Capacity Building: Cross-National Benefits and International Divides'. Paper to be presented at the TPRC Conference, Washington D.C., February 2021. Available on SSRN at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3658350
What are the benefits of conducting an assessment?	The goal of a CMM review is to gather data about a country's cybersecurity capacity landscape, and to determine which of the five stages of cybersecurity maturity the country has reached across the CMM dimensions. The data is used to produce an evidence-based report that is submitted to the government with recommendations to: • benchmark the maturity of a country's cybersecurity capacity; • detail a pragmatic set of actions towards reducing and eliminating cybersecurity capacity maturity gaps; • identify priorities for investment and future capacity building; and • build business cases for investment and corresponding expected national cybersecurity performance enhancements.
Do you have a weightage calculation process?	No
Do you adopt a scoring and/or ranking mechanism in your assessment?	Yes – scoring of maturity, but not a ranking. The CMM consists of five stages of maturity ranging from *start-up* to *dynamic*. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt to changing

	environmental considerations. Being in a particular stage means that a country is in a specific position in terms of maturity in cybersecurity capacity. The CMM proposes the evidence that would be required to determine a certain stage of maturity has been reached for a factor/aspect. To reach a level of maturity in any CMM dimension, all indicators for a factor/aspect of that dimension must have been met. The CMM, therefore, directly indicates what areas require further development in order to reach the next stage of maturity and the data required to evidence such a level of capacity maturity.

Details

What key questions can the tool help to answer?	• What are the existing cybersecurity capacities in a country? • What are the existing cybersecurity gaps in a country? • What is the status of strategy and policy implementation? • Which actors are involved and what are the roles and responsibilities? • What steps can a country take to become more cybersecure?
At what point in the strategy lifecycle should the assessment occur?	Initiation / Stocktaking and analysis / Monitoring and evaluation
How does the assessment help to align other activities?	As the CMM modified focus groups bring together in one place a large set of stakeholders at the national level as well as international partners (where possible), the CMM reviews are ideally positioned to be coordinated with other activities before, after and in parallel. The CMM modified focus group format also allows input to be gathered during the session for other assessments, where appropriate.
What role does the assessment play in the GFCE matchmaking process?	Together with national incident response capacity reviews and national risk assessments, cyber capacity reviews are the first activity in the GFCE menu for the national strategy process and part of its initiation phase. Thanks to its multistakeholder approach, its comprehensiveness and its transparent approach, a CMM review is ideal for bringing together the various stakeholders in a country, as well as funders and implementers, and to provide a common basis on which to plan and implement cyber capacity-building activity.
Are case studies or testimonials publicly available regarding the benefits of the tool?	CMM case studies: North Macedonia, Ghana, Samoa, Georgia and OAS regional reports: https://gcscc.ox.ac.uk/case-studies Senegal case study: GFCE Annual Meeting Singapore, *"National Strategies. Interviews Behind the Cover"*: https://thegfce.org/national-strategies-interviews-behind-the-cover World Bank: Global Cybersecurity Capacity Programme. Lessons Learned and Recommendations Towards Strengthening the Programme: https://cybilportal.org/publications/global-cybersecurity-capacity-program-lessons-learned-and-recommendations-towards-strengthening-the-program/ Cybersecurity in Pacific island nations: https://t.co/smxYhtrqBz?amp=1
What are the mechanisms to ensure the independence, impartiality and neutrality of your results?	Most implementers are research institutions and have received ethical approval from their respective research boards to collect the data for this assessment. Each CMM report is peer-reviewed by the GCSCC Technical Board, consisting of senior academics and cybersecurity experts.

Please add any further information	How CMM reviews inform research on cyber capacity building: https://gcscc.ox.ac.uk/our-approach OAS/IDB 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean: https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean OAS/IDB 2016 Cybersecurity: Are We Ready in Latin America and the Caribbean?: https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean GFCE – Assess national cybersecurity capacity using a maturity model: https://thegfce.org/wp-content/uploads/2020/04/Assessnationalcybersecuritycapacityusingamaturitymodel.pdf GFCE Initiative: Progressing Cybersecurity in Senegal and West Africa: https://cybilportal.org/projects/progressing-cybersecurity-in-senegal-and-west-africa-gfce-initiative/ GFCE Initiative: Assessing and Developing Cybersecurity Capability: https://cybilportal.org/projects/assessing-and-developing-cybersecurity-capability-gfce-initiative/

Cyber Strategy Development and Implementation Framework (CSDI)

MITRE Corporation

MITRE's *Cyber Strategy Development and Implementation Framework* (CSDI) comprises a four-phase model for (1) understanding national cyber risk/opportunity context; (2) assessing current capacity across eight key capability areas as well as strategic foundations ("capacity to build capacity"); (3) developing and prioritizing strategic goals and investments based on assessed capacity gaps; and (4) developing implementation roadmaps for long-term sustainability.

Overview

Date tool was last updated	September 2020
What is the name of the assessment tool?	Cyber Strategy Development and Implementation Framework (CSDI)
What is the name of the organization maintaining the tool?	MITRE Corporation
Who are the implementers of assessments?	MITRE Corporation
Please provide links to the tool and any additional information	https://cybilportal.org/tools/national-cyber-strategy-development-implementation-framework/
Whom should I contact to discuss arranging an assessment?	Gary Bundy: gbundy@mitre.org Cynthia Wright: cawright@mitre.org Johanna Vazzana: jvazzana@mitre.org
Geographical coverage	Regional, national or organizational
Who can use the tool?	Anyone
What are the themes or topics covered?	The eight areas assessed are: 1) Civil law, regulation and accountability 2) Policy and standards 3) Risk-informed resourcing 4) Resilient operations 5) Incident response 6) Cybercrime prevention and prosecution 7) Cyber workforce development 8) Public awareness/culture of cybersecurity. In each of these areas, multistakeholder involvement and partnerships are regarded as key enablers, and implementation approaches for workforce development in particular are focused on establishing effective public-private partnerships. Strategic foundations are also included in assessments, the most important of these factors being leadership commitment and stakeholder involvement.

What are the GFCE themes or topics covered?	Policy and strategy ☒ Strategies ☒ Assessments ☐ CBMs and norms ☐ Cyber diplomacy International law in cyberspace Incident management and CIIP ☒ National computer security incident response ☐ Incident capture and analytics ☐ Cyber security exercises ☒ Critical information infrastructure protection Cybercrime ☒ Legal frameworks / cybercrime law ☒ Law enforcement in cyberspace ☒ Cybercrime training ☒ Cybercrime prevention Culture and skills ☒ Cyber security awareness ☒ Education and training ☒ Workforce development Standards ☒ International and/or national standards
Type of indicators	Indicators are primarily qualitative, focusing on governance mechanisms, policies, processes and resourcing. They are generally not specifically technical in nature (i.e. not focused on particular network architectures or hands-on system testing).
How many indicators are used and how are they applied?	More than 100 indicators are used, grouped within the appropriate capacity areas.
Methodology – what type of assessment is used?	Research-driven analysis and stakeholder survey/interviews
Primary data-collection method	• Open-source information • Interviews • Questionnaires and surveys • Documents and records
Do you have a secondary data collection?	Stakeholder workshops
What mechanisms do you adopt to ensure the accuracy of the data collected?	• Internal quality review • Questionnaires are administered across as broad a stakeholder group as feasible to broaden/validate insights • Machine-scored survey
What are the main outputs of the assessment?	The results of a combination of open-source research, threat/opportunity analysis, an administered assessment and follow-on interviews are combined to produce an intuitive “radar chart” output designed to facilitate risk-informed goal and investment prioritization across the eight capacity areas, along with a detailed report containing prioritized recommendations.

Presentation format of the assessment outputs	• Report • Visualization tool
Can the assessment outputs be published?	Yes, with approval of the requesting entity
How can previous reports be accessed?	On request to the assessed government/organization
What evidence is there of impact?	In every country with which MITRE has a sustained relationship, the assessed government and/or organizations have made changes to strategic goals, governance structures/mechanisms, operational coordination processes, incident response communications and processes, workforce development approaches and/or public awareness programme themes that reflect the priorities identified through this engagement.
What are the benefits of conducting an assessment?	Assessed countries, organizations and/or assistance entities gain deep insights into their strategic risk/opportunity context and their capacity drivers, needs and gaps in a form that facilitates a key aspect of capacity investment: prioritization. Through follow-on strategy development and implementation workshops, they identify key stakeholders' roles and responsibilities; governance best practices; partnership opportunities; resourcing approaches; legislative and policy gaps and ambiguities; and foundational (pre-requisite) requirements, all framed within the context of their unique threat landscape and capacity-development needs. In addition, because the assessment is focused on a whole-of-government or whole-of-organization approach, and workshops are conducted using proven design-thinking participative tools, it fosters stakeholder participation and buy-in that is essential to effective implementation.
Do you have a weightage calculation process?	Capacity areas are of equal "weight" in the assessment. However, different capacity areas will be more important than others to particular assessed countries/organizations, based on their strategic context, current capacity and human/financial resources. This approach is specifically intended to identify which areas should be more heavily "weighted" for each assessed entity based on their unique risk/opportunity needs.
Do you adopt a scoring and/or ranking mechanism in your assessment?	The radar chart (one output tool, in addition to a detailed analysis and recommendations report) produced is on a four-point scale. However, it is not a maturity model: capacity gaps are assessed in the context of the country's/organization's desired end states rather than an objective set of benchmarks. This approach helps ensure that countries/organizations are not "chasing" metrics that are less important to their strategic threat context, and allows implementers to help tailor investment strategies to the needs that are most relevant to economic and security goals.

Details

What key questions can the tool help to answer?	• What is our cyberthreat/opportunity landscape? • In the light of that landscape, what are our goals with regard to building and securing ICT/cyber/digital capabilities and services? • Who are our stakeholders in this space, and what are their roles? • What are our capacity gaps in relation to our strategic goals? • Among those gaps, where should we prioritize our efforts? • What objectives could help achieve our prioritized goals? • 'How Might We' design initiatives to achieve them? • Of the various initiatives we could pursue, which have the greatest return on investment in terms of impact and feasibility? • What resources can be brought to bear? • Who are our potential partners in pursuing selected initiatives? • How do we develop and execute an implementation roadmap? • How can we increase stakeholder buy-in and public support?
At what point in the strategy lifecycle should the assessment occur?	Initiation / Stocktaking and analysis / Production of the strategy / Implementation
How does the assessment help to align other activities?	By providing a whole-of-government/organization perspective anchored in a defined threat/opportunity landscape, this approach provides a common framework for stakeholders to identify, prioritize, resource and pursue common goals. By differentiating capability gaps by key capacity area, it helps entities maintain focus on those areas most relevant to them, while still providing visibility into other areas in which capacity-building opportunities may arise, such as assistance programresources that can grow capacity without diverting scarce internal resources. Finally, because it is set in a multistakeholder framework, it facilitates a focus on communications, information sharing and transparent processes that ensure stakeholders and partners are aware of (and buy into) top priorities and ongoing activities.
What role does the assessment play in the GFCE matchmaking process?	It clarifies prioritized areas of need, appropriate stakeholder contacts, other ongoing/available programs and available human/financial resources.
What case studies or testimonials are available regarding the benefits of the tool?	All assessments to date have been carried out for countries/organizations at their request or that of the US State Department. None have been published, although the governments of Botswana, Ghana, Ukraine and Ecuador have publicly expressed appreciation in public speeches, social media releases and/or government-to-government summits. The greatest testimonial may be that US federal agencies and partner countries continue to request, trust and act on our assistance recommendations, and that the number of countries with which we are directly engaged has grown from three to more than two dozen in the four years we have been employing this framework; and each country actively solicits our continued advice and assistance. At the regional level, the number of countries we engage with is over 90 and continues to grow, with new requests for specific assistance arising from each engagement.

What are the mechanisms to ensure the independence, impartiality and neutrality of your results?	MITRE is a federally funded R&D organization with rigorous internal quality-control requirements and a public charter that expressly commits to impartial service, free of conflict of interest, in support of the public interest.
Please add any further information	This framework was developed under the sponsorship of the US Department of State Office of the Coordinator for Cyber Issues, and its refinement has come about through State Department-directed bilateral and regional engagements. Use of this assessment outside of US State Department-directed engagements does not necessarily imply the support of the US Government or alignment with its policies; however, United States values, including freedom of information, commitment to a free and open Internet, the rule of law and human rights, are implicit in our model and our recommendations.

Global Cybersecurity Index (GCI)

International Telecommunication Union (ITU)

The *Global Cybersecurity Index* (GCI) supports countries in identifying areas for improvement in the field of cybersecurity, as well as motivating them to take action to improve their ranking, in turn raising the overall level of cybersecurity worldwide. The GCI's scope and framework is set out in Resolution 130 (Rev. Dubai, 2018) of the ITU Plenipotentiary Conference, on strengthening the role of ITU in building confidence and security in the use of ICTs. The GCI Questionnaire, from which indicators, sub-indicators and micro-indicators are derived, is created and approved by a consultation under Question 3/2 ("Securing information and communication networks: Best practices for developing a culture of cybersecurity") entrusted to Study Group 2 of the ITU Telecommunication Development Sector (ITU-D). The survey is administered by means of an online platform through which supporting evidence is collected.

The fourth iteration of the GCI questionnaire (2019-2020) measures 20 general indicators by means of 82 questions. The 20 indicators reflect the five pillars of ITU's Global Cybersecurity Agenda (GCA): *Legal*, *Technical*, *Organizational*, *Capacity development* and *Cooperation*. The GCIv4 questionnaire and relevant GCI-related documentation were submitted by the ITU Telecommunication Development Bureau (BDT) to ITU-D Study Group 2 in October 2019, ahead of the launch of the survey. In March 2020, BDT reported to Study Group 2 on the status of responses to the questionnaire; informed members of the next steps in the process of data analysis; and signalled that weightage development would be completed by engaging a group of experts formed through an open consultation process with the ITU Member States, Sector Members and BDT partners. In October 2020, the Weightage Expert Group put forward weightage recommendations for the GCIv4 indicators, sub-indicators and micro-indicators, and proposed changes to the GCI questionnaire for future iterations. Verification of questionnaire responses is ongoing, for ultimate validation by submitting countries. The final report is expected to be published in early 2021.

Overview

Date tool was last updated	The last update of the publication was carried out in March 2019. We are in the process of collecting data and completing verification of submitted data for the GCIv4 report.
What is the name of the assessment tool?	Global Cybersecurity Index (GCI)
What is the name of the organization maintaining the tool?	International Telecommunication Union (ITU)
Who are the implementers of assessments?	International Telecommunication Union (ITU)
Please provide links to the tool and any additional information	• ITU website: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global- cybersecurity-index.aspx • Cybil portal: https://cybilportal.org/projects/itu-global-cybersecurity-index-gci-programme/
Whom should I contact to discuss arranging an assessment?	• GCI Team: gci@itu.int
Geographical coverage	Global

Who can use the tool?	• Member States: ministries/agencies • Cybersecurity agencies/policy-makers • Academia • Cybersecurity experts • Any interested individuals ITU membership might be required for Academia and organizations that would like to partner in collaboration on the GCI.

What are the themes or topics covered?	The GCI themes include: **Legal measures**: • Cybercrime substantive law • Cybersecurity regulation **Technical measures**: • National/government incidence response teams (CERT/CIRT/CSRIT) • Sectoral CERT/CIRT/CSRIT • National framework for the implementation of cybersecurity standards • Child online protection (COP) **Organizational measures:** • National cybersecurity strategies (NCS) • Responsible/national agencies • Cybersecurity metrics **Capacity-building measures**: • Public awareness campaigns • Cybersecurity training for professionals • National education programmes and academic curricula • Cybersecurity research and development programmes • National cybersecurity industry • Government incentive mechanisms to support cybersecurity development **Cooperation measures:** • Bilateral agreements • Participation in international mechanisms (forums) • Multilateral agreements • Public-private partnerships • Inter-agency partnerships. For a complete description of each measure, refer to the published reports at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
What are the GFCE themes or topics covered?	Policy and strategy ☒ Strategies ☒ Assessments ☒ CBMs and norms ☒ Cyber diplomacy ☒ International law in cyberspace Incident management and CIIP ☒ National computer security incident response ☒ Incident capture and analytics ☒ Cyber security exercises ☒ Critical information infrastructure protection Cybercrime ☒ Legal frameworks / cybercrime law ☒ Law enforcement in cyberspace ☒ Cybercrime training ☒ Cybercrime prevention

<table>
<tr><td></td><td>Culture and skills
☒ Cyber security awareness
☒ Education and training
☒ Workforce development

Standards
☒ International and/or national standards</td></tr>
<tr><td>Type of indicators</td><td>GCI data collection is qualitative, with the use of a binary system to evaluate the existence or absence of a specific activity, department or measure.</td></tr>
<tr><td>How many indicators are used and how are they applied?</td><td>The GCI does not follow a pre-arranged set of indicators. In each iteration, the questionnaire is modified and revised taking into consideration feedback received from the countries’ focal points and the membership. The number of indicators may therefore decrease or increase, and there is not a fixed number of indicators for each theme. For instance, see the table below with details of numbers of indicators in each iteration to date.

<table><tr><th>GCIv1</th><th>GCIv2</th><th>GCIv3</th><th>GCIv4</th></tr><tr><td>17 indicators with 17 main questions</td><td>25 indicators with 157 questions</td><td>25 indicators with 50 main questions</td><td>20 indicators with 82 main questions</td></tr></table></td></tr>
<tr><td>Methodology – what type of assessment is used?</td><td>The GCI uses both primary and secondary methods of assessment. The GCI team collects data for countries that do not participate and shares findings with them for approval, as well as verifying and validating responses submitted by ITU Member States’ focal points.</td></tr>
<tr><td>Primary data-collection method</td><td>• Open-source information
• Unpublished documents
• Questionnaires and surveys
• Documents and records</td></tr>
<tr><td>Do you have a secondary data collection?</td><td>Yes. Secondary data collection is conducted for countries that respond to the GCI questionnaire through the following steps:
• ITU carries out verification, identifying missing responses, supporting documents and links, using open-source information, unpublished documents, questionnaires and surveys and documents and records publicly available.
• The verified responses are sent back to the country focal point, who improves the accuracy of the responses where necessary.
• ITU validates the final amendments from the country focal point and returns the document again to each focal point for final approval.
• The validated questionnaire responses are subsequently used for analysis, scoring and ranking.</td></tr>
<tr><td>What mechanisms do you adopt to ensure the accuracy of the data collected?</td><td>GCI focal points appointed by ministries usually have cybersecurity background/expertise and work in cyber-related positions within the different ministries. Moreover, the relevant links and documents requested and validated are from the official public websites of the governments, and sometimes confidential official documents are provided. We have recourse to experienced validators from cyber-related fields who are required to carry out the verification process more than once for each country and share back with countries until final confirmation is obtained to ensure accuracy.</td></tr>
<tr><td>What are the main outputs of the assessment?</td><td>In each iteration, the final report and findings are published.</td></tr>
<tr><td>Presentation format of the assessment outputs</td><td>Report</td></tr>
<tr><td>Can the assessment outputs be published?</td><td>Yes. The output can be published. The GCI is open material to raise awareness globally. All the previous reports can be found at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx</td></tr>
</table>

<table>
<tr><td>How can previous reports be accessed?</td><td>Previous reports can be accessed and downloaded from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx</td></tr>
<tr><td>What evidence is there of impact?</td><td>The growing participation of Member States in the GCI demonstrates the continually growing interest in the index:
<table>
<tr><th>GCIv1 (2015)</th><th>GCIv2 (2017)</th><th>GCIv3 (2018)</th><th>GCIv4 (2019-2020)</th></tr>
<tr><td>105 countries</td><td>134 countries</td><td>155 countries</td><td>Currently 163 countries</td></tr>
</table>
Many countries request ITU to support them in the development of their cybersecurity posture, such as, <i>inter alia</i>, in developing and improving national strategies, in establishing CERTs and in capacity-building activities. Low- and medium-scoring countries (based on score ranges, held constant over time) have been able to receive targeted interventions, leading to a steady decline in the number of such countries.
<table>
<tr><th>Year</th><th>High</th><th>Medium</th><th>Low</th></tr>
<tr><td>2018-2019</td><td>54</td><td>53</td><td>87</td></tr>
<tr><td>2016-2017</td><td>30</td><td>60</td><td>104</td></tr>
<tr><td>2014-2015</td><td>19</td><td>52</td><td>122</td></tr>
</table>
</td></tr>
<tr><td>What are the benefits of conducting an assessment?</td><td>The assessments help to identify gaps in cybersecurity development within nations and regions, as well as raising awareness regarding cybersecurity worldwide. The assessment also helps to identify countries that most need support in improving their cybersecurity posture.

Through the data collected, the GCI highlights practices that Member States can implement which are suited to their national environment, promotes good practices and fosters a global culture of cybersecurity.</td></tr>
<tr><td>Do you have a weightage calculation process?</td><td>Yes. Indicator weightage within the GCI is assessed by members of the GCI Expert Group based on indicator importance within the five GCA pillars; relevance to the main GCI objectives and conceptual framework; and data availability and quality. The Expert Group provides unbiased weightage recommendations after the Weightage Expert Group meeting held for each iteration of the GCI.</td></tr>
<tr><td>Do you adopt a scoring and/or ranking mechanism in your assessment?</td><td>Yes. Indicator weights from each expert are averaged for the final weight for each indicator. Through a function applied, a country that has answered YES with documented proof receives a full score for the indicator, while a country without proof or which answers NO receives a zero score for that indicator. The overall scores are normalized and ranked.</td></tr>
</table>

Details

What key questions can the tool help to answer?	• What are the current global trends and patterns in cybersecurity policy? • How can Member States identify their strengths and weaknesses in cybersecurity measures? • What are countries' levels of cybersecurity commitment, and which countries provide best practices in cybersecurity?
At what point in the strategy lifecycle should the assessment occur?	Initiation / Stocktaking and analysis / Production of the strategy / Implementation / Monitoring and evaluation
How does the assessment help to align other activities?	The GCI assessment helps identify areas of relative strength and weakness in Member States' cybersecurity commitments, informing where Member States may need additional support in capacity building, or where they may be able to offer support to others. For example, through the GCI assessment, ITU can identify cybersecurity education needs in members' education systems.

What case studies or testimonials are available regarding the benefits of the tool?	Each year, many countries request assistance in the development of CERTs and national cybersecurity strategies as a result of the GCI assessment, scores and ranking. For example: **Benin** launched a cybersecurity strategy, as a result of awareness raised by the GCI: https://news.itu.int/benin-launches-a-new-national- cybersecurity-strategy/ **Republic of the Congo** adopted the Cybersecurity Act, the law on cybercrime: https://postetelecom.gouv.cg/le-senat-adopte-a-lunanimite-la-creation-de-lagence-nationale-de-securite-des-systemes-dinformation/ In 2018, progress in cybersecurity commitments, as reported to GCI assessments, was seen in: • Benin, Estonia, Poland, Zimbabwe, Zambia, Egypt, South Africa and Eswatini, in establishing laws on cybercrime; • Uganda, in drafting its data/privacy protection legislation; • Australia, Botswana, Canada, Czech Republic, Denmark, Japan, Jordan, the Netherlands, Spain, Samoa, Singapore and Luxembourg, in updating NCSS; and • Cameroon, Malawi, Tanzania and Zimbabwe, in drafting their NCSS. GCI media coverage: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
What are the mechanisms to ensure the independence, impartiality and neutrality of your results?	• Submissions to the GCI are independently validated by our team • An independent group of experts gives input on indicator weightages within the model, with no single expert able to significantly shift weightages alone.

National Capabilities Assessment Framework (NCAF)

European Union Agency for Cybersecurity (ENISA)

The main objective of the *National Capabilities Assessment Framework* (NCAF) was to create a self-assessment tool to support EU Member States in measuring the level of maturity of their cybersecurity capabilities. To achieve this goal, ENISA used the strategic objectives of EU Member States' national cybersecurity strategies (NCSS) as a starting point. As cybersecurity capabilities are the main instruments used by countries to achieve their NCSS objectives, the NCAF encompasses questions on five levels of maturity taking into account 17 strategic objectives included in most European NCSS. The framework provides a simple, representative view of a Member State's cybersecurity maturity at three different levels: objective level, cluster level and global level.

Overview

Date tool was last updated	2 December 2020
What is the name of the assessment tool?	National Capabilities Assessment Framework (NCAF)
What is the name of the organization maintaining the tool?	European Union Agency for Cybersecurity (ENISA)
Who are the implementers of assessments?	EU Member States
Please provide links to the tool and any additional information	https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework The NCAF will be developed into an online tool next year (2021)
Whom should I contact to discuss arranging an assessment?	European Union Agency for Cybersecurity (ENISA)
Geographical coverage	European Union/global
Who can use the tool?	The target audience of the NCAF is policy-makers, experts and government officials responsible for or involved in designing, implementing and evaluating NCSS and, on a broader level, cybersecurity capabilities. Additionally, the findings formalized in the published document can be of value to cybersecurity policy experts and researchers at the national or European level.
What are the themes or topics covered?	The conceptual model of the self-assessment framework covers 17 strategic objectives derived from EU Member States' NCSS and is structured around four main clusters. Each of these clusters covers a key thematic area for building cybersecurity capacity and contains different objectives. Each objective is then assessed by questions on different levels of maturity. The clusters cover the following topics: **(I) Cybersecurity governance and standards** 1. Develop a national cyber contingency plan 2. Establish baseline security measures 3. Secure digital identity and build trust in digital public services This cluster considers aspects of planning to prepare the Member State against cyberattacks as well standards to protect Member States and digital identity.

	(II) Capacity building and awareness 4. Organize cybersecurity exercises 5. Establish an incident response capability 6. Raise user awareness 7. Strengthen training and educational programs 8. Foster R&D 9. Provide incentives for the private sector to invest in security measures 10. Improve the cybersecurity of the supply chain This cluster assesses the capacity of the Member States to raise awareness on cybersecurity risks and threats and on how to tackle them. Additionally, this dimension gauges the country's ability to continuously build cybersecurity capabilities and increase knowledge and skills in the cybersecurity domain. **(III) Legal and regulatory** 11. Protect critical information infrastructure, operators of essential services (OES) and digital service providers (DSP) 12. Address cybercrime 13. Establish incident reporting mechanisms 14. Reinforce privacy and data protection This cluster measures the capacity of the Member States to put in place the necessary legal and regulatory instruments to address cybercrime and also address legal requirements such as incident reporting, privacy matters and protection of critical information infrastructure (CIIP). **(IV) Cooperation** 15. Establish a public-private partnership 16. Institutionalize cooperation between public agencies 17. Engage in international cooperation This cluster evaluates cooperation and information sharing between different stakeholder groups at the national and international level.

What are the GFCE themes or topics covered?	Policy and strategy ☒ Strategies ☒ Assessments ☒ CBMs and norms ☒ Cyber diplomacy ☐ International law in cyberspace Incident management and CIIP ☒ National computer security incident response ☒ Incident capture and analytics ☒ Cyber security exercises ☒ Critical information infrastructure protection Cybercrime ☒ Legal frameworks/cybercrime law ☒ Law enforcement in cyberspace ☒ Cybercrime training ☒ Cybercrime prevention Culture and skills ☒ Cyber security awareness ☒ Education and training ☒ Workforce development Standards ☒ International and/or national standards

Type of indicators	The framework includes qualitative indicators that are built on two levels: Strategic level and Operational level. For each objective included within the self-assessment framework, there are a series of indicators distributed between the five levels of maturity. Every indicator is based on a dichotomous (yes/no) question. The indicator can be a requisite or a non-requisite.
How many indicators are used and how are they applied?	The model provides a score based on the value of two parameters, the ***maturity level*** and the ***coverage ratio***. Each of these parameters can be calculated at different levels: (i) per objective, (ii) per cluster of objectives or (iii) overall. Additionally, to adapt to the specificities of the EU Member States while also permitting a consistent overview, the score is calculated from two different samples at cluster level and overall level: • **General scores**: One complete sample covering all the objectives included within the cluster or within the overall framework (from 1 to 17) • **Specific scores**: One specific sample covering only the objectives selected by the Member State (usually corresponding to the objectives present in the specific country's NCS) within the cluster or within the overall framework. For each cluster, a table presents the comprehensive set of indicators in the form of questions representative of a given maturity level. The questionnaire is the main instrument for the self-assessment. For each objective, there are two sets of indicators to be noted: • A set of strategy maturity questions (9 generic questions), marked from 'a' to 'c' for each maturity level, repeated for each objective; and • A set of cybersecurity capacity questions (319 cybersecurity capacity questions), numbered from '1' to '10' for each maturity level, specific to the area covered by the objective.
Methodology – what type of assessment is used?	**Levels of maturity**: A five-level maturity scale **Attributes**: Based on four dimensions/clusters covering areas to build cybersecurity capacities **Assessment method**: Self-evaluation **Results display**: Presentation of the results at different levels of granularity
Primary data-collection method	• Anticipate coordination activities to gather data and consolidate data. • Identify a central body in charge of completing the self-assessment at national level. • Use the assessment exercise as a way to share and communicate on cybersecurity topics. • Use the NCSS as a scope for selecting the objectives subjected to the assessment. • When the NCSS scope evolves, ensure that the score interpretation remains consistent with the NCSS evolution. The NCSS lifecycle is a multi-year process.
Do you have a secondary data collection?	When filling out the self-assessment questionnaire, keep in mind that the primary goal is to support Member States in cybersecurity capacity building.
What mechanisms do you adopt to ensure the accuracy of the data collected?	The EU Member State/country that undertakes the assessment should ensure accuracy to benefit from the results of framework.

What are the main outputs of the assessment?	The results of the assessment are provided at three different levels: Objective level, Cluster level and Global level. The country is assessed and receives a final generic result that takes into account all the objectives in each cluster, and a final specific result that takes into account only the selected objectives that the country wished to assess. In addition, the NCAF also provides a coverage ratio. The coverage ratio is calculated as the **proportion** between the **total number of questions** within the objective and the **number of questions for which the answer is positive**. The coverage ratio is expressed as a percentage.
Presentation format of the assessment outputs	Report Visualization from online tool (ENISA future work)
Can the assessment outputs be published?	The results of the assessment are published only if the Member State decides to do so on its own initiative.
How can previous reports be accessed?	The Member State is able to track its progress over time based on re-assessments.
What evidence is there of impact?	Overall, some 20 Member States participated in the development of the framework and almost all Member States participated in the validation workshop where the framework was presented and extensively discussed. More specifically, the framework should empower the Member States in: • Conducting an evaluation of their national cybersecurity capabilities; • Enhancing awareness of the country's maturity level; • Identifying areas for improvement; and • Building cybersecurity capabilities.
What are the benefits of conducting an assessment?	The NCAF is a tool that can help countries to: • Provide useful information to develop a long-term strategy (e.g. good practices, guidelines); • Identify missing elements within the NCSS; • Further build cybersecurity capabilities; • Support the accountability of political actions; • Gain credibility vis-à-vis the general public and international partners; • Support outreach and enhance public image as a transparent organization; • Anticipate the issues lying ahead; • Identify lessons learnt and best practices; • Provide a baseline on cybersecurity capacity across the EU to facilitate discussions; and • Evaluate the national capabilities regarding cybersecurity.
Do you have a weightage calculation process?	The EU Member State can display the assessment results by presenting the maturity level of the country's cybersecurity capabilities, of a cluster of objectives or even of a single objective. All assessed objectives are equally relevant within the assessment framework; therefore, they have the same importance. The same applies to the indicators deployed within the framework.
Do you adopt a scoring and/or ranking mechanism in your assessment?	The NCAF aims at measuring Member States' cybersecurity capabilities with regard to the 17 objectives. However, the Member State can choose the objectives it wants to assess against and only assess a subset of the 17 objectives.

National Cyber Security Index (NCSI)

e-Governance Academy (eGA)

The *National Cyber Security Index* (NCSI) is a global index which measures the preparedness of countries to prevent cyberthreats and manage cyberincidents. The NCSI is also a database with publicly available evidence materials and a tool for national cybersecurity capacity building.

The NCSI focuses on measurable aspects of cybersecurity implemented by the central government:

1. **Legislation in force** – Legal acts, regulations, orders, etc.
2. **Established units** – Existing organizations, departments, etc.
3. **Cooperation formats** – Committees, working groups, etc.
4. **Outcomes** – Policies, exercises, technologies, websites, programmes, etc.

Since 2016, 160 countries have been evaluated using the NCSI. Data collection, review and publication is a continuous process in the NCSI. The NCSI does not publish annual iterations. When new evidence is provided, it is assessed and, if it is grounded, the necessary changes in the ranking list will be made immediately. The NCSI methodology was developed in 2016 and updated in 2018. Currently, the methodology is under review and the new iteration will be published at the latest in 2022.

Overview

Date tool was last updated	The country entries in the NCSI are continuously being updated, meaning that the NCSI itself is constantly updating.
What is the name of the assessment tool?	National Cyber Security Index (NCSI)
What is the name of the organization maintaining the tool?	e-Governance Academy
Who are the implementers of assessments?	• e-Governance Academy • Cybersecurity related entities and institutions of the ranked countries
Please provide links to the tool and any additional information	Cybil portal: https://cybilportal.org/projects/national-cybersecurity-index/
Whom should I contact to discuss arranging an assessment?	Ms Epp Maaten: epp.maaten@ega.ee Mr Radu Serrano: radu.serrano@ega.ee Ms Merle Maigre: merle.maigre@ega.ee NCSI team: ncsi@ega.ee
Geographical coverage	Global
Who can use the tool?	• Country ministries/agencies • Cyber security agencies/policy-makers • Academia • Cyber security experts • Any interested individual To collaborate with the country data collection for the NCSI, you only need to reach out to the NCSI team.

What are the themes or topics covered?	**1. Cyber Security Policy Development:** 1.1. Cyber security policy unit 1.2. Cyber security policy coordination format 1.3. Cyber security strategy 1.4. Cyber security strategy implementation plan **2. Cyber Threat Analysis and Information:**

	2.1. Cyber threats analysis unit 2.2. Public cyber threat reports are published annually 2.3. Cyber safety and security website **3. Education and professional development:** 3.1. Cyber safety competencies in primary or secondary education 3.2. Bachelor's level cyber security programme 3.3. Master's level cyber security programme 3.4. PhD level cyber security programme 3.5. Cyber security professional association **4. Contribution to Global Cyber Security:** 4.1. Convention on Cybercrime 4.2. Representation in international cooperation formats 4.3. International cyber security organization hosted by the country 4.4. Cyber security capacity building for other countries **5. Protection of Digital Services:** 5.1. Cyber security responsibility for digital service providers 5.2. Cyber security standard for the public sector 5.3. Competent supervisory authority **6. Protection of Essential Services:** 6.1. Operators of essential services are identified 6.2. Cyber security requirements for operators of essential services 6.3. Competent supervisory authority 6.4. Regular monitoring of security measures **7. E-Identification and Trust Services:** 7.1. Unique persistent identifier 7.2. Requirements for cryptosystems 7.3. Electronic identification 7.4. Electronic signature 7.5. Timestamping 7.6. Electronic registered delivery service 7.7. Competent supervisory authority **8. Protection of Personal Data:** 8.1. Personal data protection legislation 8.2. Personal data protection authority **9. Cyber Incidents Response:** 9.1. Cyber incidents response unit 9.2. Reporting responsibility 9.3. Single point of contact for international coordination **10. Cyber Crisis Management:** 10.1. Cyber crisis management plan 10.2. National-level cyber crisis management exercise 10.3. Participation in international cyber crisis exercises 10.4. Operational support of volunteers in cyber crises **11. Fight Against Cybercrime:** 11.1. Cybercrimes are criminalized 11.2. Cybercrime unit 11.3. Digital forensics unit 11.4. 24/7 contact point for international cybercrime **12. Military Cyber Operations:** 12.1. Cyber operations unit 12.2. Cyber operations exercise 12.3. Participation in international cyber exercises
What are the GFCE themes or topics covered?	Policy and strategy ☒ Strategies ☒ Assessments

	☐ CBMs and norms ☒ Cyber diplomacy ☐ International law in cyberspace Incident management and CIIP ☒ National computer security incident response ☒ Incident capture and analytics ☒ Cyber security exercises ☒ Critical information infrastructure protection Cybercrime ☒ Legal frameworks / cybercrime law ☒ Law enforcement in cyberspace ☐ Cybercrime training ☒ Cybercrime prevention Culture and skills ☒ Cyber security awareness ☒ Education and training ☒ Workforce development Standards ☒ International and national standards
Type of indicators	The data collection for the NCSI is qualitative, with the use of a value system to evaluate the existence of a specific legal act, specialized unit, official cooperation format and/or outcome.
How many indicators are used and how are they applied?	There are a total of 46 indicators (presented in the form of the aforementioned themes and topics). The indicators themselves are distributed among 12 capacities. Each indicator has a value, which shows the relative importance of the indicator in the index, and a criterion, which explains what kind of data can be submitted as evidence. To receive a positive value for any criterion, evidence material must be provided as data. If the data provided meets all aspects of the criterion, it will be accepted as sufficient evidence material.
Methodology – what type of assessment is used?	Each country is entered and updated in the NCSI on a case-by-case basis. Once a country has been entered/updated, the NCSI will display it in a global comparative ranking.
Primary data-collection method	• Open-source information • Documents and records • Legislation and other official documents • Official websites
Do you have a secondary data collection?	Yes. The NCSI is not a static index, so the data collection is continuous throughout the year. • Open-source information • Documents and records • Legislation and other official documents • Official websites
What mechanisms do you adopt to ensure the accuracy of the data collected?	All evidence materials have to be public information and publicly accessible. Only official data can be considered as evidence material. Accepted evidence/references are: legal acts, official documents and official websites.

	When data collection is complete, the information provided is reviewed by at least two NCSI experts. After inspection, the dataset is published on the NCSI website.
What are the main outputs of the assessment?	• Updated information on the country page (for existing countries in the NCSI) • Country pages (for countries that have not yet been included in the NCSI) • NCSI ranking (which updates every time a country page is updated)
Presentation format of the assessment outputs	• Website • Visualization tool (with the possibility to compare past or present datasets for a single country or between countries) • Possibility to download a country page into PDF format
Can the assessment outputs be published?	Yes, always.
How can previous reports be accessed?	For any given country page, the NCSI shows when the country's information was updated. Normally, the country page presents the latest information available. The visitor is able to view the information of a previous update by selecting a specific update date from a dropdown menu identified as '*Choose a version*'.
What evidence is there of impact?	• Growing country participation in the NCSI demonstrates the continually growing interest in the index. Individual countries have requested separate detailed individual assessments based on the NCSI, to ascertain the current state of their national cybersecurity and improve upon it. • Academic researchers have used the tool to work on single or multiple case studies.
What are the benefits of conducting an assessment?	Countries can identify their level of preparedness in preventing cyberthreats. By allowing comparability between countries and breaking down scores into indicators, the NCSI supports a transnational, cooperative approach to cybersecurity, where best practices are shared among multiple countries.
Do you have a weightage calculation process?	No
Do you adopt a scoring and/or ranking mechanism in your assessment?	Yes - for the indicators, for the NCSI (country) score, for the Digital Development Level (DDL) and for the difference (between the NCSI score and the DDL). • Each indicator has a value, which shows the relative importance of the indicator in the index. The values are given by the expert group according to the following considerations: 1 point – a legal act that regulates a specific area 2-3 points – a specialized unit 2 points – an official cooperation format 1-3 points – an outcome/product. • The NCSI score shows the percentage the country received from the maximum value of the indicators. The maximum NCSI score is always 100 (100 per cent) regardless of whether indicators are added or removed. • In addition to the NCSI score, the index table also shows the Digital Development Level (DDL). The DDL is calculated according to the ICT Development Index (IDI) and Network Readiness Index (NRI). The DDL is the average percentage the country received from the maximum value of both indexes. • The Difference shows the relationship between the NCSI score and DDL. A positive result shows that the country's cybersecurity development is in line with, or ahead of, its digital development. A negative result shows that the country's digital society is more advanced than its national cybersecurity.

Details

What key questions can the tool help to answer?	• How prepared is my country for a cyberattack/threat? • What is my country missing in order to protect against a cyberthreat? • What are the institutions suitable for the task? • How can we further improve our preparedness against changing cyberthreats? • What are some best practices around the world that we can adapt and/or implement?
At what point in the strategy lifecycle should the assessment occur?	The assessment (country analysis) can occur at any point of the strategy lifecycle, in order to maintain the NCSI as up to date as possible. However, for individual countries it is recommended for the ‘Initiation’, ‘Stocktaking and analysis’ or ‘Monitoring and evaluation’ phase(s).
How does the assessment help to align other activities?	The NCSI helps to identify areas of relative strength and weakness in a country’s level of preparedness for preventing cyberthreats, thus indicating where it may need additional support in capacity building, or where it may able to offer support to others. The NCSI country pages also provide national best practices that can be adapted/implemented by other countries with or without the assistance of donors, international organizations, etc.
What role does the assessment play in the GFCE matchmaking process?	Since the NCSI presents publicly available information, funders and implementers are able to see the areas of relative strength and weakness in a country. Consequently, they may reach out to these respective countries to propose cyber capacity building or similar activities and improvements, where they are needed.
What case studies or testimonials are available regarding the benefits of the tool?	Situation Review: Safety and Security of Cyberspace and e-Democracy in the Eastern Partnership Countries (2017) by the e-Governance Academy
What are the mechanisms to ensure the independence, impartiality and neutrality of your results?	Submissions from country contributors to the NCSI are independently validated by our team.
Please add any further information	**Handbook:** • National Cyber Security in Practice (2020) by the e-Governance Academy **Podcast/article:** • What should governments do to secure their national cyberspace? (2020) by the e-Governance Academy • NCSI – How prepared is your country for a cyberattack? (2020) by the e-Governance Academy • What is cyber hygiene? (2020) by the e-Governance Academy **Article:** • 160 Countries in the NCSI: Barriers, Lessons Learnt, and Interesting Facts (2020) by the e-Governance Academy.

Overview of tools

	Combating Cybercrime Capacity-Building Tool	Cyber Maturity in the Asia-Pacific region	CRI	CMM	CSDI	GCI	NCAF	NCSI
Policy and strategy								
Strategies	●	●	●	●	●	●	●	●
Assessments	●	●	●	●	●	●	●	●
CBMs and norms		●	●	●		●	●	
Cyber diplomacy		●	●	●		●	●	●
International law in cyberspace	●	●	●					
Incident management and CIIP								
National computer security incident response	●	●	●	●	●	●	●	●
Incident capture and analytics			●	●		●	●	●
Cyber security exercises			●	●		●	●	●
Critical information infrastructure protection	●	●	●	●	●	●	●	●
Cybercrime								
Legal frameworks / cybercrime law	●	●	●	●	●	●	●	●
Law enforcement in cyberspace	●	●	●	●	●	●	●	●
Cybercrime training	●		●	●	●	●	●	
Cybercrime prevention	●		●	●	●	●	●	●
Culture and skills								
Cyber security awareness	●	●	●	●	●	●	●	●
Education and training	●	●	●	●	●	●	●	●
Workforce development	●	●	●	●	●	●	●	●
Standards								
International or national standards			●	●	●	●	●	●