GEODE

The Hague Centre for Strategic Studies

CyberPeace Institute

Paris Call for Trust and Security in Cyberspace

Working Group 5: Building a Cyberstability Index

Executive Summary and Final Report

EXECUTIVE SUMMARY

Overview

Multistakeholder initiatives, such as the Paris Call for Trust and Security in Cyberspace, aim to bring together different actors such as states, local governments, private-sector entities and civil society organizations. Paris Call Working Group 5: Building a Cyberstability Index (Working Group) brought together the CyberPeace Institute, a civil society organization; GEODE, a research and training center; and The Hague Centre for Strategic Studies, a think tank. Together, the Working Group worked on a methodology to evaluate the evolution of cyberstability.

Assessing the state of global cyberstability is important to understand which existing practices are successful, such as international fora and agreements, as well as to evaluate technical requirements and their contribution to cyberstability. The concept of cyberstability can also raise the understanding of the consequences of cyberattacks and support advocacy work aimed at lowering the level of conflict in cyberspace. As such, cyberstability is envisaged both as a precondition for trust and security in cyberspace and as an objective of the Paris Call.

This work was conducted on the basis of the Global Commission on the Stability of Cyberspace's definition of cyberstability, and the Working Group focused on building a solid theoretical framework around it. The framework is based on the following categories: confidence in using cyberspace safely; general availability and integrity of products and services; general availability and integrity of information; management of change in relative peace; and resolving tensions in a non-escalatory manner.

Based on the definition of cyberstability and these categories, the Working Group conducted a review of existing indices to identify ad hoc indicators as well as specific indicators that could be useful for a methodology to measure cyberstability. These indicators include, for example, looking at the operational risks of an entity that could affect a user's confidence when interacting in digital spaces, or analyzing how business disruptions affect the availability of services that a user can and should be able to access. Although these indicators are based on technical traits, they provide insight into the question of impact, which is linked to cyberstability as a precondition for trust and security in cyberspace.

Throughout the review and analysis process, it became clear that no existing index focuses solely on cyberstability, and the need for such an index became apparent. At the same time, the Working Group faced challenges related to data collection and limitations, as it was agreed from the start that they did not want to create another "black-box" index that depends on hidden or solely subjective criteria.

Data accessibility and overall methodological usability has been a core concern of the Working Group, and this approach guided the creation

of the methodology. With this in mind, the methodology was developed in consultation with experts from the field in order to understand what is feasible, especially from a data perspective, and what is not.

Way forward

The Working Group focused its mandate on building a methodology to evaluate cyberstability over time, and identified several key findings and challenges. Overall, the Working Group found that accessible, publicly available data is a key limitation to measuring cyberstability. Without this data, the multistakeholder community will never have a complete picture of the current state of cyberstability.

The Working Group therefore calls on the wider multistakeholder community to work together to bridge the information gap between entities. It is the Working Group's hope that following the Paris Peace Forum 2021, researchers and practitioners will use this methodology for their own work and refine it as they see fit. The goal is to create something practical that furthers our collective understanding of cyberspace. It is now up to others to see what makes the most sense in this regard.

The members of the Working Group hope that this methodology provides a solid theoretical foundation for others to continue on this path. Should you be interested in carrying on this work and would like to discuss the methodology in more detail, please contact any of the members of the Working Group.

INTRODUCTION

The Paris Call for Trust and Security in Cyberspace, launched by French President Emmanuel Macron in November 2018, is a multistakeholder initiative to improve trust, security and stability in cyberspace. It brings together states, local governments, private sector entities and civil society organizations through its 9 Principles that promote and ensure international cyberspace security and the safer use of information and communications technology (ICTs).

To grow and strengthen the Paris Call community, as well as to create practical outputs based on the Paris Call Principles, the French Minister for Europe and Foreign Affairs Jean-Yves Le Drian announced the launch of six working groups at the third gathering of the Paris Peace Forum in November 2020.

Working Group 5: Building a Cyberstability Index worked on a methodology to evaluate the evolution of cyberstability. This methodology serves as a resource to others in the community, for example, to assess global cyberstability. This assessment of global cyberstability is an important step to understand which existing practices are successful, such as international fora and agreements, as well as to evaluate technical requirements and their contribution to cyberstability.

As such, cyberstability is envisaged both as a precondition for trust and security in cyberspace and as an objective of the Paris Call. Based on the Working Group's analysis, no existing index captures cyberstability in this way, and so this methodology can contribute to advancing stability in cyberspace. The Working Group is co-chaired by the CyberPeace Institute, GEODE and The Hague Centre for Strategic Studies.

What is cyberstability?

Several definitions of cyberstability can be found in official state documents and academic papers.[1] They all tend to contain two dimensions: preserving the benefits of cyberspace and avoiding harm and suffering.

Working Group 5 based its work and methodology on the definition of cyberstability provided by the Global Commission on the Stability of Cyberspace (GCSC):

"Stability of cyberspace means everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner."[2]

1 For example, see UNIDIR's report Towards Cyber Stability: A User-Centred Tool for Policymakers and the International Security Advisory Board's Report on A Framework for International Cyber Stability.

2 GCSC, Final Report, p. 13.

The Working Group selected this definition based on its comprehensive nature and its general acceptance within the cyber community. The GCSC definition was crafted by a group of 29 prominent Commissioners representing a broad range of geographic regions, as well as government, industry, technical and civil society stakeholders with legitimacy on various aspects of cyberspace. The GCSC also solicited feedback on its definition from the wider community through a public consultation process. After three years of work, the GCSC published a report with key recommendations to advance cyberstability.

Why a cyberstability index?

Many indices have tried to evaluate different dimensions of cyberspace to "measure the commitment of countries to cybersecurity in order to raise cybersecurity awareness"[3], examine cyber maturity in a given region of the world[4], develop a comprehensive knowledge of states' cyber power[5] or "measure[s] countries' preparedness to prevent cyber threats and manage cyber incidents"[6].

These indices have been developed by international organizations, think tanks and academia. They have helped to develop a better understanding of the facets of peace and security in cyberspace, such as states' level of cybersecurity and implementation of good practices and policies to ensure cybersecurity, states' engagement in cyber diplomacy, or their military capabilities. Yet, these indices do not provide a broad picture of the state of (in)stability of cyberspace as they tend to focus only on the actions of individual states. To fill this gap, the Working Group started to build a methodology for a global, multistakeholder index that would provide a more comprehensive picture of the evolution of cyberstability.

Ultimately, measuring cyberstability can help to:

- Gain a better understanding of the consequences of cyberattacks;
- Evaluate whether state and non-state actors' efforts are producing results that help to ensure that everyone can enjoy the benefits of ICTs; and
- Support advocacy work to identify fields in which particular efforts are needed.

How this supports the wider work of the Working Group

Each of the entities that comprise the Working Group have an interest in working on a cyberstability index, though from different perspectives. The CyberPeace Institute, GEODE and The Hague Centre for Strategic Studies

3 See 'Acknowledgements' of the International Telecommunication Union (ITU) Global Cybersecurity Index 2018.
4 See the Australian Strategic Policy Institute's (ASPI) report Cyber Maturity in the Asia-Pacific Region 2017.
5 See the Belfer Center's report National Cyber Power Index 2020.
6 See the e-Governance Academy's National Cyber Security Index methodology for more.

believe that each of their unique perspectives and work streams have helped to build a more comprehensive index methodology.

The CyberPeace Institute's mission is to ensure people's rights to security, dignity and equity in cyberspace. The team works with partners to reduce the harm from cyberattacks on people's lives worldwide and to provide assistance. By analyzing cyberattacks through an evidence-led approach, the Institute exposes their societal impact and how international laws and norms are being violated, and advances responsible behavior to enforce cyberpeace. Cyberpeace cannot exist without accountability, and the Institute believes that accountability needs to be evidence-led and based on accessible data. The proposed cyberstability index methodology reinforces this belief as it works to create a tool that is based on verifiable, accessible data.

GEODE's mission is to conduct research and train students to better understand the strategic challenges of the digital revolution. The multidisciplinary team comprises more than 40 researchers, including 12 PhD students, and develops new methodologies and tools to measure and represent cyberspace and better understand actions, operations and confrontations between a multiplicity of actors in this new environment and their consequences. GEODE raises awareness of the systemic risk linked to the proliferation of offensive tools and behavior for the stability of cyberspace and of societies, which are increasingly dependent on cyberspace. This index will allow the team at GEODE to track evolutions and the impact of multistakeholder efforts to advance cyberstability.

The Hague Centre for Strategic Studies (HCSS) has been at the forefront of cyberstability since it initiated the Global Commission on the Stability of Cyberspace (GCSC) in 2017 with the support of partners from government, industry and civil society. It led the Secretariat of the GCSC and contributed directly to its output. Beyond its commitment to advancing norms of behavior that enhance cyberstability, HCSS seeks to further the work of this index through its research and data-visualization tools. The forthcoming "Cyber Arms Watch" will provide much-needed transparency on the offensive cyber capabilities of more than 70 states. The "Cyber Transparency Index" will be based on accessible data and aims to reduce the scope for misunderstanding among states, provide clarity of intent and predictability in cyberspace, and advance norms of restraint, confidence building measures, and other stability measures that collectively contribute to international cybersecurity.

METHODOLOGY

Overview

Establishing a solid theoretical framework is the first step to building an index. The Working Group focused on this theoretical framework and identified the subgroups as well as the type of indicators that could be used to measure cyberstability. In doing so, it hopes that it will create incentives to take the project a step further, including through data and information sharing. Moreover, as the Paris Call is a multistakeholder initiative, the aim of this methodology is to include all types of actors, rather than just governments.

As the Working Group focused on the index methodology and began to identify the indicators that could be used to measure cyberstability and the potential challenges, it became evident that more work is needed to create and operationalize the index itself. This would include working on data availability, collection and analysis, as well as the combination and validation method of the index.

Data sources and data collection

The Working Group defined criteria for selecting indicators inclusive of the Paris Call's multistakeholder approach:

- *Transparency*: The choice was made to avoid "black-box" indicators as much as possible. These include indicators that are not transparent in terms of how the data is collected, aggregated and transformed. Close attention was paid to the methodology of existing indices, bearing in mind that transparency might be included in the calculation if the index methodology is adopted further.
- *As few policy indicators as possible*: This type of indicator is more prone to subjectivity than those based on objective and established numbers. Yet, the Working Group agreed that including policy indicators might be inevitable as they provide a wider context for cyberstability.
- *Causation*: The Working Group selected indicators based on their potential ability to measure each subgroup, although this came with challenges that will be discussed in the "Assumptions" section.

The methodology was created in consultation with experts from the field in order to understand what is feasible, especially from a data perspective, and what is not.

As mentioned earlier, one of the goals of the Working Group was to create a methodology for an index with as much open-source information as possible, so as to avoid creating another "black-box" index. Based on this, potential data sources were identified that could support the selected indicators. These sources range from IT professionals, to information and reports from industry actors, to official state documents. A more detailed overview of the data sources for each indicator category is included later in this report.

Data limitations

Data accessibility was a key and consistent challenge in building the methodology for a cyberstability index. More often than not, the data used for existing indices is not publicly available, and so the raw data cannot be verified or used by others in the community.

Alternatively, in some cases where the data is publicly available, it cannot be verified whether it is the same data used by another existing index. The Working Group devoted time in this area, to understand what data is available and what is not. However, more research needs to be done to be clear on these questions. Data availability is a key point of action for the wider community if it is interested in moving forward with the application and use of this methodology.

Assumptions

Throughout this process, several assumptions had to be made in order to build a relevant and employable methodology:

1. Parts of the methodology are based on the responses of individuals. The Working Group assumes that these individuals are the right people to be responding to the questions. This means that:
   a. The level of cybersecurity knowledge is assumed; and
   b. This assumption can be mitigated by asking some qualifying questions.
2. The causation between each indicator and its relevance to cyberstability is assumed. This means that indicators that could be useful depending on their interpretation of cyberstability have been identified separately.
3. The data is available for all of these indicators, either because it is publicly available or there is potential for partnerships with entities who have the data. An internal overview has been created to track the data that is available and where we would need to call on others for further support and collaboration.

Building the index

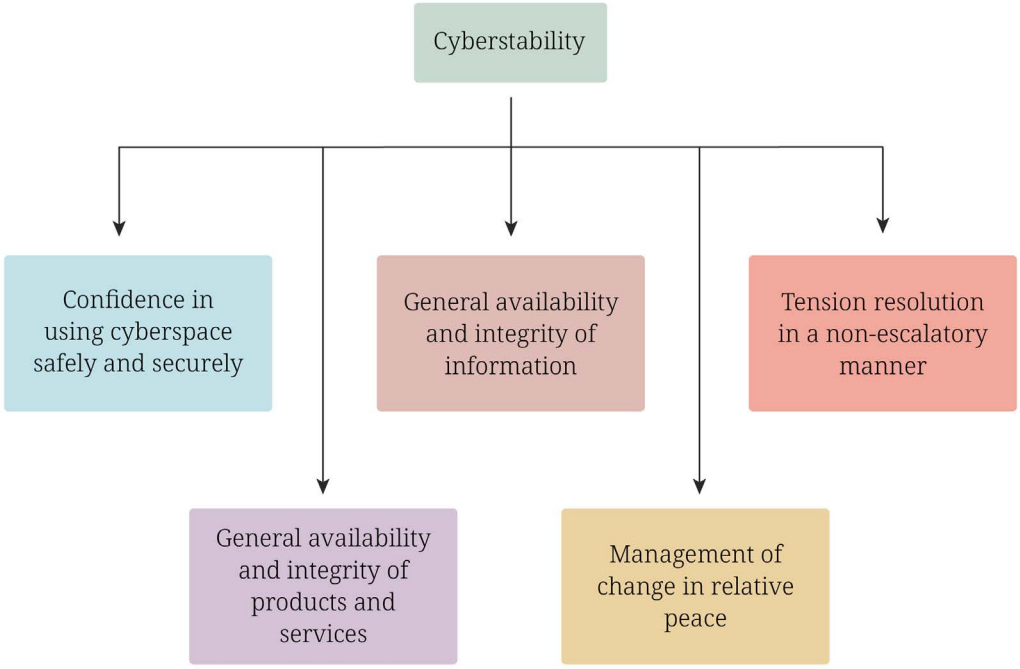
Five cumulative categories were identified by the Working Group to measure the evolution of cyberstability. As previously mentioned, these categories are based on the GCSC's definition of cyberstability:

"Stability of cyberspace means everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner."[7]

The Working Group divided this definition of cyberstability into five categories, each with its own set of ad hoc indicators as well as specific indicators

7 GCSC, Final Report, p. 13.

from existing indices that could be useful for a methodology to measure cyberstability.

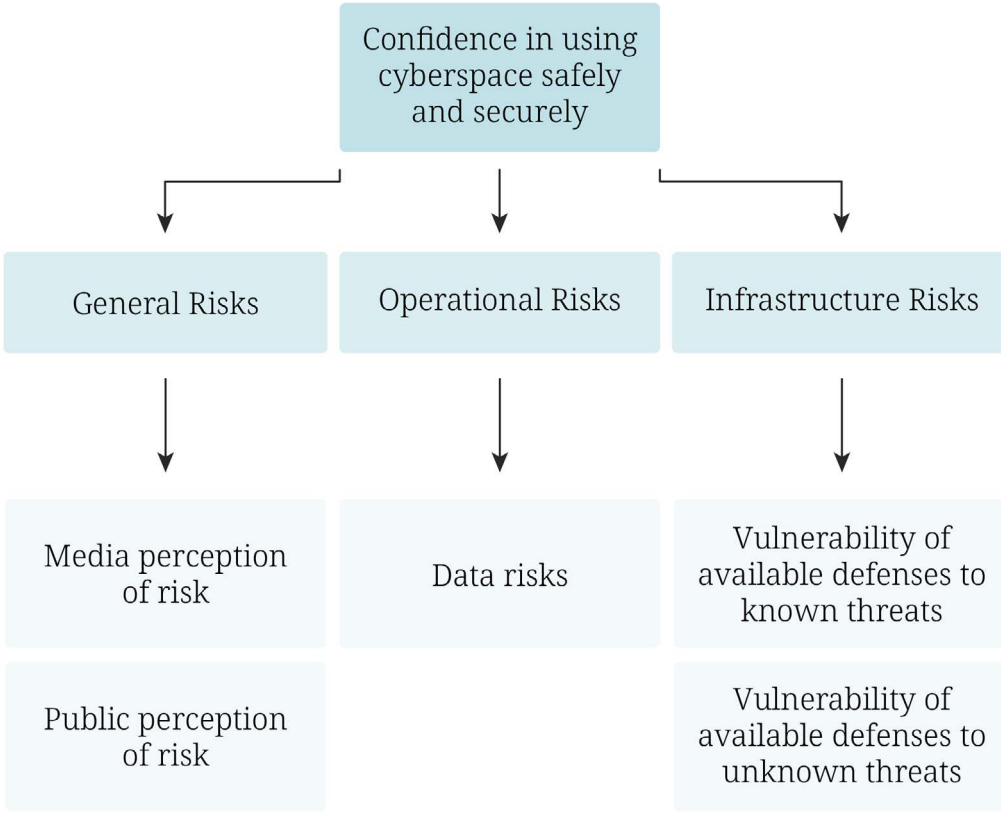


1. Confidence in using cyberspace safely and securely

Confidence in using cyberspace safely and securely refers to the ability of anyone to interact in digital spaces without fear that their rights and security will be threatened (i.e. not having data stolen, not being subject to unlawful surveillance, etc.). Confidence in the user's ability to operate in cyberspace safely and securely requires secure hardware, software and protocols. This is not just based on facts but also on the perception of threats and reliability of the technological environment that comprises cyberspace. As soon as a system is unreliable – or there is a perception that such a system is unreliable – its use will be limited.

Potential data sources for this category include assessments and direct reports from Chief Risk Officers and Chief Information Security Officers. Academics conducting field work in this area could also provide context and information that would support the category's evaluation. Additionally, annual cybersecurity threat reports by both public and private organizations, surveys of public trust in digital technologies, as well as reports from Government Accountability Offices are potential data sources to measure the confidence of a user's ability to interact in cyberspace.

The analysis revealed that very few existing indices contain indicators relevant to measuring confidence, and data is rarely provided. Indices containing indicators that measure different types of risk appeared to be the most useful for measuring confidence. The conclusion is that measuring confidence will require collecting data from scratch or getting the data from existing indices with a substantial risk that data verification will not be possible.



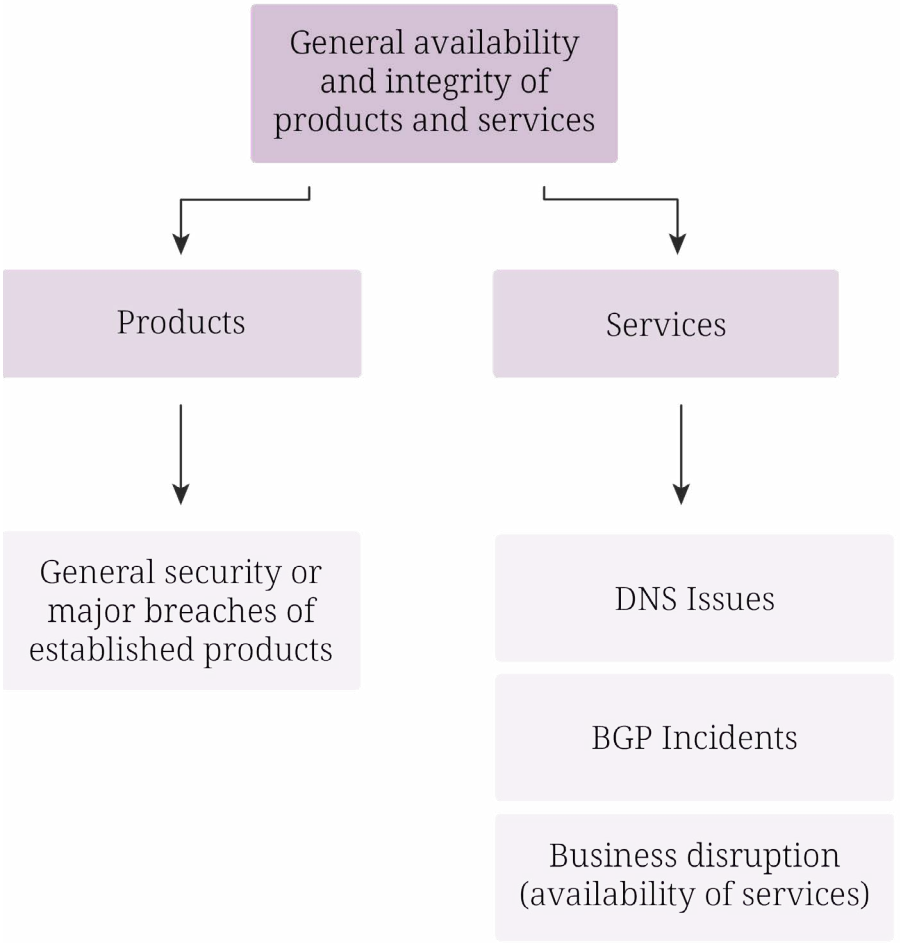
2. General availability and integrity of products and services

The criteria of availability and integrity of products and services help to define the security of networks and information systems based on the idea that the assurance of these services comes from providers of the service and product. Products and services are understood in a broad sense and cover both the technologies made available to users and the activities to which users can gain access (i.e. online banking, social media, etc.).

The user should be assured that these products and services are doing what they are stated to do by the providers. It should be noted that the GCSC definition uses a standard, “generally”, meaning that it does not exclude that in some cases the availability and integrity of services cannot be assured, without this leading to a presumption of instability. Some potential data sources that are relevant to this category include reports from Chief Risk Officers and Chief Information Security Officers, the work of academics in the field, reports and analysis from global and regional initiatives, as well as Internet governance initiatives, such as the IGF (Internet Governance Forum), ISOC (Internet Society) and ICANN (The Internet Corporation for Assigned Names and Numbers).

The Working Group has identified very few relevant indicators in existing indices for this category; however, indicators on Border Gateway Protocol (BGP) incidents, Domain Name System (DNS) issues and other areas of concern would need to be created. Yet, many indicators in existing indices measure infection rates and provide data to measure stability. Such data is usually provided by non-state actors.
The issue here lies within the precision of the data versus the category of the

definition. Indeed, most of the time, this data does not distinguish between the type of impact (integrity, availability, confidentiality) whereas the GCSC definition excludes confidentiality from its scope for several reasons, including that information communicated over cyberspace is not, by default, confidential.



3. General availability and integrity of information

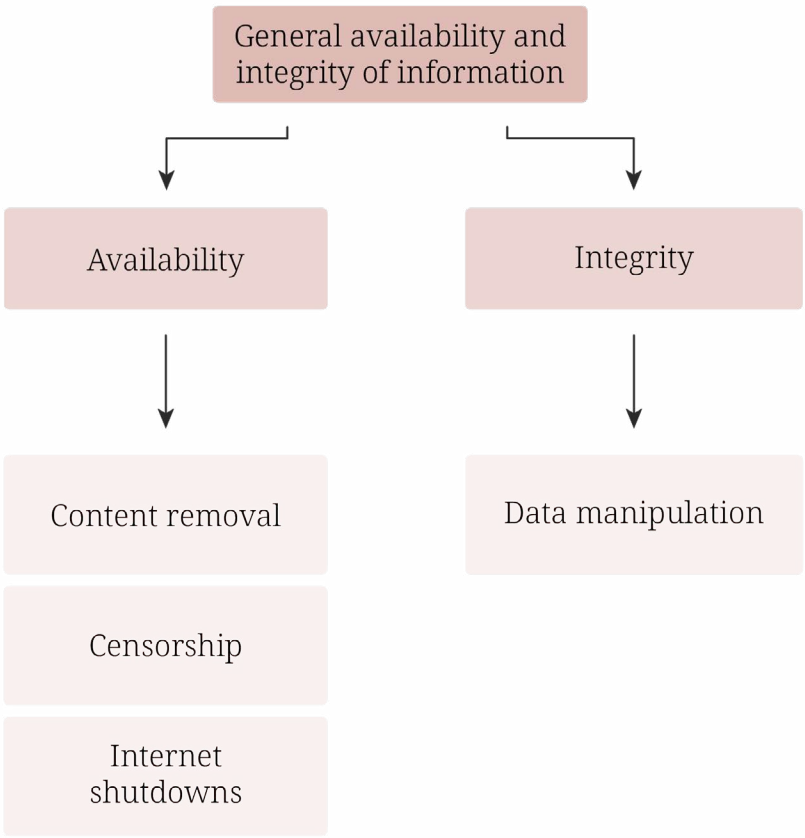
The general availability and integrity of information is closely linked to the previous category on services but focuses on the content of the exchange. Both face similar challenges: when the integrity and availability of a service is threatened, so can the integrity and availability of the information exchanged through such service. One of the most extreme examples is Internet shutdowns that altogether prevent access to online services and to information, thereby impeding freedom of expression, assembly and association.[8]

Again, it should be noted that the definition uses a standard, "generally", meaning that it does not exclude that, in some cases, the availability and integrity of information cannot be assured without this leading to a presumption of instability. For this category, the Working Group identified a number of data sources that could inform the evaluation of the general availability of information. These include public reports on censorship,

8 See Disconnecting from Cyberstability: An Assessment of how Internet Shutdowns in the Democratic Republic of Congo, Tanzania, and Uganda Undermine Cyberstability by Moses Owiny and Sheetal Kumar for more.

internet shutdowns and content removal from industry and civil society actors, such as the Freedom House index and the Freedom of the Press index. The Working Group found that open-source data sources to measure the integrity of information (e.g. through data manipulation) are largely lacking.

The challenges faced by the indicators in the previous category are also relevant to this category.

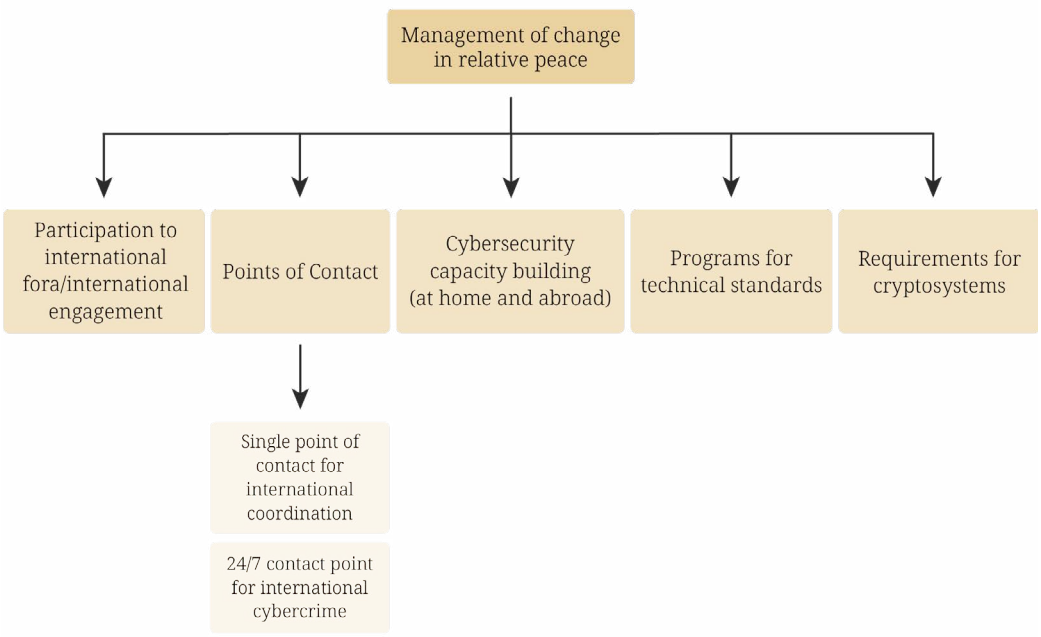


4. Management of change in relative peace

The management of change in relative peace refers to the practices in place that ease changes in cyberspace. This primarily refers to new products, services and especially standards. New products and services constantly change cyberspace, but the open promulgation and widespread use of technical standards – within standard setting organizations such as the Internet Engineering Task Force (IETF) – ensure that such change occurs without open opposition so cyberspace remains resilient and stable. To this end, the technical community, civil society and individuals play a major role. There is also a dependency on capacity-building programs, particularly in the Global South, for all actors to engage in these processes and to develop the appropriate services.

To conduct an analysis for this category, the Working Group identified data sources such as statements within international standard setting bodies, as well as statements within the Internet Governance Forum (IGF) and the work of the IGF Dynamic Coalition on Internet Standards, Security and Safety. Other initiatives such as the GFCE's Cybil Platform and the OECD ODA could also provide helpful data on capacity-building.

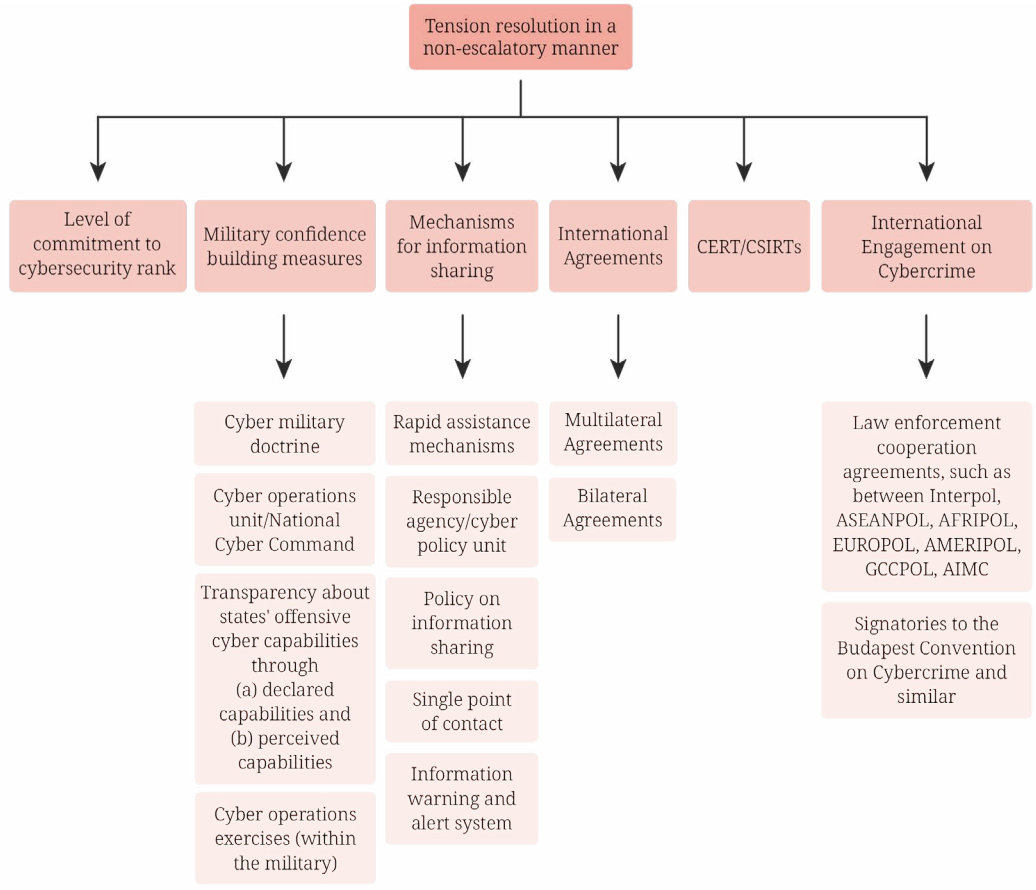
Different potential indicators have been identified. Yet, one of the main challenges is tied to identifying non-state actors' participation in this category (e.g. patching of vulnerabilities).



5. Tension resolution in a non-escalatory manner

Tensions in cyberspace can result from interstate relations, state and non-state actors' relations (e.g. tensions surrounding the transfer of personal data) or inter-non-state actors' relations. Resolving tensions in a non-escalatory manner implies favoring multistakeholder practices and the peaceful settlement of disputes to avoid escalation and putting users in a situation where their safety and security in and out of cyberspace could be threatened. This includes international agreements, either bilateral or multilateral, or multistakeholder agreements, such as on norms, international law, confidence-building measures and capacity-building.

For the most part, data is available for the indicators in this category although, much like the fourth category, these indicators may lose some relevance for private-sector, civil society and academic actors as they were originally intended for public-sector actors. With this in mind, potential data for this category includes signatories to the international conventions to counter cybercrime, the number of countries with a CERT or single points of contact and the degree to which states are transparent about their cyber capabilities. Sources can include databases of the Budapest Convention, INTERPOL, organizations such as ENISA and FIRST, states themselves, as well as existing indices and repositories such as the UNIDIR Cyber Policy Portal, CCDCOE Library and the HCSS Cyber Arms Watch (forthcoming).


Tension resolution in a non-escalatory manner
Level of commitment to cybersecurity rank
Military confidence building measures
Mechanisms for information sharing
International Agreements
CERT/CSIRTs
International Engagement on Cybercrime
Cyber military doctrine
Cyber operations unit/National Cyber Command
Transparency about states' offensive cyber capabilities through (a) declared capabilities and (b) perceived capabilities
Cyber operations exercises (within the military)
Rapid assistance mechanisms
Responsible agency/cyber policy unit
Policy on information sharing
Single point of contact
Information warning and alert system
Multilateral Agreements
Bilateral Agreements
Law enforcement cooperation agreements, such as between Interpol, ASEANPOL, AFRIPOL, EUROPOL, AMERIPOL, GCCPOL, AIMC
Signatories to the Budapest Convention on Cybercrime and similar

KEY FINDINGS AND WAY FORWARD

Over the past several months, Paris Call Working Group 5 collaborated to build a methodology for a cyberstability index to achieve a better sense of how cyberstability can be measured and what data is available to fulfill this measurement. After a review of existing indices and indicators, the Working Group narrowed down and identified the key indicators that can help to evaluate the state of cyberstability over time.

Key Finding 1

The need for open-source data

Overall, accessibility of data remains a limitation to measuring cyberstability. Without accessible data that can be independently verified, the community is at an impasse when it comes to understanding, for example, which measures contribute to a user's confidence in using the Internet or which type of treaty or convention has contributed positively to the management and resolution of tensions between countries. The objective of this initial step was to provide a baseline on which the community can build.

Key Finding 2

The need for standardized surveys and reporting

Beyond accessibility of data, it became apparent that indicators that rely on survey data require a standard approach to ensure comparability between the responses of different organizations. This is a wider complexity in having a multistakeholder index methodology, and raises questions about the reliability of voluntary information sharing for this sort of index.

Key Finding 3

The need for collaboration

Collaboration on the part of the multistakeholder community is necessary in order to adopt the index methodology and to operationalize and improve it based on research needs. After the presentation at the Paris Peace Forum in November 2021, the Working Group hopes that researchers and others from the field will use this methodology for their own work and refine it as they see fit. The goal was to create something practical that helps to further our collective understanding of cyberspace. It is now up to others to see what makes the most sense in this regard.

Key Finding 4

The need to clarify the role of confidentiality in the definition of cyberstability

The Working Group discussed the potential consequences for measurement if confidentiality is included in the definition of cyberstability. The Working Group believes that its inclusion would imply that cyber intrusion for espionage is detrimental to cyberstability. These intrusions make up the majority of nation-state cyberattacks, and most datasets on cyberattacks do not distinguish between attacks that harm confidentiality, integrity and availability. As a result, if the Working Group were to include confidentiality in the definition of cyberstability, then it would facilitate the measure of cyberattacks affecting the services and information categories we have outlined. In contrast, if confidentiality is not included in the definition of cyberstability, as is the case with the GCSC definition, then it is much more difficult to isolate data on integrity and availability only, i.e. by excluding confidentiality, it reduces the volume of data that can be processed.

Key Finding 5

The need for dynamic indicators of success

Cyberspace is a domain of constant change, requiring agile mechanisms to ensure the stability of cyberspace as technologies and attacks evolve. This means that indicators to measure success or the state of stability should not be static, in particular when it comes to measuring vulnerabilities and threats. For example, as ICT providers undertake measures to limit vulnerabilities in operating systems, attackers are forced to change their tactics and exploit other vulnerabilities further up or down the technical stack. The metrics of success should therefore be dynamic so they depict the most accurate state of cyberstability.

Key Finding 6

The need for future iterations of this work

As previously mentioned in the report, this work is just the beginning of what can be built upon. There are many other areas and issues to take into consideration when analyzing cyberstability within the five categories discussed, such as standards and protocols. The Working Group recognizes the importance of these points of analysis, but also recognizes the potential difficulty in capturing standards issues in the form of indicators. This is just one area where the work on cyberstability can be continued in future iterations, but has not been included in the Working Group's current methodology.

Contact information

If you would like to learn more about the Working Group's process and methodology, or to contribute data, expertise or knowledge to the project, please contact any of the following Working Group members.

Juliana Crema, RESEARCH ASSOCIATE
Roxana Radu, RESEARCH ASSOCIATE
Klara Jordan, CHIEF PUBLIC POLICY OFFICER

info@cyberpeaceinstitute.org

contact@geode.science

info@hcss.nl

The Paris Call for Trust and Security in Cyberspace is a multi-stakeholder initiative that was launched by the French government at the Paris Peace Forum in November 2018. The initiative sets out 9 Principles promoting and ensuring international cyberspace security and the safer use of information and communications technology (ICTs).

These Principles promote different aspects of multi-stakeholder collaboration and are intended to support norm-building and their operationalization. In order to take direct action to implement these Principles, the French government launched the creation of six working groups in November 2020. Working Group 5 on building a cyberstability index is co-led by the CyberPeace Institute, GEODE (Géopolitique de la Datasphère) and the Hague Centre for Strategic Studies (HCSS).

November 2021