



UNIDIR

Towards Cyber Stability

A User-Centred Tool for Policymakers

**Lisa Rudnick and Derek B. Miller
with Leeor Levy**

UNIDIR RESOURCES

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR)—an autonomous institute within the United Nations—conducts research on disarmament and security. UNIDIR is based in Geneva, Switzerland, the centre for bilateral and multilateral disarmament and non-proliferation negotiations, and home of the Conference on Disarmament. The Institute explores current issues pertaining to the variety of existing and future armaments, as well as global diplomacy and local tensions and conflicts. Working with researchers, diplomats, government officials, NGOs and other institutions since 1980, UNIDIR acts as a bridge between the research community and governments. UNIDIR's activities are funded by contributions from governments and donor foundations.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The views expressed in this publication are the sole responsibility of UNIDIR. They do not necessarily reflect the views or opinions of the United Nations or UNIDIR's sponsors.

www.unidir.org

© UNIDIR 2015

Table of Contents

| | |
|--|-----|
| Acknowledgements | ii |
| About the Authors and Project Team | iii |
| Foreword | iv |
| 1. Introduction: From Study to Tool | 1 |
| 2. Goals and Methods | 6 |
| 3. Findings from the Design Research | 12 |
| 4. Needs and Functions of a Tool | 18 |
| 5. Proposed Models | 25 |
| 6. Next Steps | 39 |
| 7. Conclusions | 41 |

Acknowledgements

UNIDIR would like to thank the Government of the Federal Republic of Germany for its financial support to the Cyber Index, in its written form, and to this initial phase of transition towards a strategic tool.

We would also like to thank all subject experts, diplomats, and other policymakers who contributed their time to the project through participation in interviews and consultations.

The project was conducted within UNIDIR's Emerging Security Threats Programme, which is led by Ben Baseley-Walker. The authors express their appreciation to Daniel Golston at UNIDIR who provided research support to the project team.

About the Authors and Project Team

Lisa Rudnick is a Senior Researcher and Project Manager at UNIDIR, where she directs the Institute's work on Evidence-Based Design (EBD), which she co-developed in partnership with Derek B. Miller. Since joining UNIDIR in 2006, the work of Ms. Rudnick and her team has focused on improving programming effectiveness from the local point of view. Prior to joining UNIDIR in 2006, Ms. Rudnick taught courses in ethnography, culture, and communication at the University of Massachusetts at Amherst, and worked as a consultant on matters of small arms and community security. Ms. Rudnick was educated at Sarah Lawrence College and the University of Massachusetts at Amherst, where she holds an MA and is a PhD candidate.

Derek B. Miller, PhD, is Director of The Policy Lab (est. 2011, Boston), a policy design institute dedicated to improving the impact and adoptability of policy initiatives. Dr. Miller has been working as a scholar and practitioner in international affairs and public policy for 20 years. From 2003–2010 he was a UNIDIR staff member. He is the co-developer of UNIDIR's Evidence-Based Design (EBD) approach in partnership with Ms. Rudnick. Dr. Miller was educated at Sarah Lawrence College, Georgetown, the University of Oxford, and the University of Geneva.

Leor Levy is a senior design and innovation consultant whose process combines ethnographic research with strategic and design processes. She regularly consults on service design, product development and strategic direction for the private, public, and healthcare sectors. In 2013, Ms. Levy assisted in the development of UNIDIR's evidence-based design tool prototype. She holds a Bachelor of Science degree in Physiology and Psychology, a Design and Communication degree, a Master's degree in Sociology, and is a Senior Associate of The Policy Lab.

Ben Baseley-Walker is Programme Lead of the Emerging Security Threats Programme at UNIDIR. Mr. Baseley-Walker has led the programme since 2011, with particular expertise in the topics of outer space and cyberspace, and developing key conceptual frameworks on emerging issues. He studied at the University of Edinburgh, the Universiteit van Amsterdam, and the International Space University.

Foreword

The Internet and other cyber resources are now the backbone of the lives of many global citizens. Yet cyber attacks are becoming more frequent, and are now also being perceived by some as offensive capabilities to be used by states against other states. Given this burgeoning reality, the importance of achieving a stable, predictable cyber environment in which cyber activities can be carried out, unimpeded by conflict or potential conflict, cannot be underestimated.

Since 2012, UNIDIR has chosen to focus on conflict prevention in cyberspace and the concept of cyber stability. The prototype proposed in this paper is a contribution to the international security community that aims to address these key areas of concern.

I am delighted that UNIDIR is publishing *Towards Cyber Stability: A User-Centred Tool for Policymakers*. This prototype of a practical tool is aimed at helping governments and other relevant actors to prepare and structure their thinking and decision-making.

This project builds on the work of a previous UNIDIR project, *The Cyber Index: International Security Trends and Realities*, published in 2013. That study, which presented a compendium of snapshots of states' cyber capabilities and key issues related to confidence-building, was UNIDIR's first contribution to supporting diplomats and policymakers as they tackle international security aspects of the cyber policymaking. This new phase of work lays out a coordinated strategy and develops a prototype for transitioning from providing a cyber information resource, to a practical tool for developing cyber stability policy.

This project also builds upon UNIDIR's ground-breaking work in Evidence-Based Design (EBD), which focuses on how to enable better use of information in the development of policies towards the end of achieving more effective outcomes.

This tool fits into a wider agenda at UNIDIR to develop innovative means to practically address international security challenges. Over the last few years, UNIDIR has increasingly seen the need for developing relevant tools that are tailored to the specific needs of the diplomatic and policymaking community.

In applying the Evidence-Based Design approach to this new area of thematic concern, UNIDIR now lays the foundations for a new approach to policymaking in the highly complex, globalized cyber domain.

Jarmo Sareva
Director
UNIDIR

1. Introduction: From Study to Tool

1.1. The Starting Point

Cyber policy development is becoming increasingly high-profile in nearly all Member States of the United Nations. Over the last decade the United Nations Institute for Disarmament Research (UNIDIR) has been focused on cyber policy in the international security domain, and since 2012 has been developing projects designed to work towards a more stable international security environment in the cyber arena. To this end in 2013 UNIDIR published *The Cyber Index: International Security Trends and Realities*. The purpose of that study was to “serve as a snapshot of [then] current cybersecurity activities at the national, regional, and international levels” in order to “help policymakers and diplomats understand the complexity of the arena”.¹

At the time of publication, the Index was one of very few texts available that provided state-level overviews of cybersecurity efforts in the military and civilian domains, in addition to overviews of activities by international organizations and regional forums. The feedback on this project from key stakeholders working in ministries, international organizations, and NGOs was that the study was a useful and foundational contribution in an area where little work had yet been done. On the basis of this feedback, and with a desire to make the Index more useful to policymakers working in this fast-paced thematic area, a decision was taken to transform it into an online resource, so that it could be updated more frequently than a print publication, and could reach a wider audience to provide a greater range of policymakers with needed information on cyber issues.

UNIDIR’s assumption, shared by many other research centres and think tanks, was that by improving the utility of the Index and providing that information online we would be contributing to the improvement of policy dialogue and decision-making pertaining to cyber issues.

1.2. Challenging Assumptions

In conducting a preliminary analysis of potential approaches for providing the index online, we quickly noted parallels with another area of work at UNIDIR that had captured key insights on how to most effectively contribute to improved dialogue and decision-making. Between 2011 and 2014, UNIDIR conducted a three-phased project to develop an approach to Evidence-Based Design (EBD)² for programming on the reintegration of ex-combatants. While the topic is unrelated to the cyber sphere, that project, like this one, was also principally concerned with improving the use of information in dialogue and decision-making.

1 UNIDIR, *The Cyber Index: International Security Trends and Realities*, 2013, p. xii. See page xii for a description of the purpose of the original study.

2 See, for example, Derek B. Miller and Lisa Rudnick, *A Framework Document for Evidence-Based Programme Design on Reintegration*, UNIDIR, 2012; and Derek B. Miller and Lisa Rudnick, *A Prototype for Evidence-Based Programme Design for Reintegration*, UNIDIR, 2014.

Hence, that project focused on precisely the same practical challenge that UNIDIR's work on the *Cyber Index* sought to address, which was how to enable better use of information in the development of policies towards the end of achieving more effective outcomes. The research findings from the EBD project demonstrated that the mere provision of more readable, searchable, and timely information could not alone ensure that it would be used in dialogue and decision-making, nor could it necessarily improve it. In fact, the research revealed a number of barriers to the use of information in these practices that had direct bearing on our project team's objectives for an online Index.

We believe findings about three key barriers from the EBD project are relevant in the context of the present project as well:

1. Provision of Irrelevant Information

When complex and consequential decisions are at hand, there is the tendency to believe that the more information that is made available for use, the better the decision-making process will be. Thus, there is a tendency to try to provide more and more data and information to policy actors and to create new (and more) ways of providing it to policy actors.

Experience has shown that this is rarely useful.

In this age of "information proliferation", a central challenge for policymakers (and their support teams) is sorting out what is "nice to know" given the discussion or decision at hand, from what is immediately and strategically relevant and applicable and therefore "need to know" for getting a job done.

For information to be a real resource, it needs to be aligned with and targeted to a task. But frequently, policy discussions and decisions are hampered due to a proliferation of information that is ultimately irrelevant to the discussions or decisions at hand, in part because it is not oriented to the tasks policymakers must perform, or the specific strategic goals they must address.

A key barrier, therefore, to the use of information is the difficulty for policy actors in determining what information is relevant to which discussions or decisions. This is especially challenging when the problems being addressed are unfamiliar (as with new kinds of actors, threats, contexts, technologies, or applications), and where guidance (in the form of norms and policies) is either no longer adequate in its present form or non-existent.

2. Lack of Knowledge about Users

Policymakers are users of information. But their ways and means of doing so in their day-to-day jobs are often unknown or otherwise invisible to the people who provide the information (for example, at research centres, think tanks, and universities).

Providers can therefore end up pushing information at users that may not be fit for purpose, or creating resources that may be difficult to use. This creates a gap between the provision of information, and its application by people whose practical needs are not really understood by information providers.

Resources developed without the target users and their needs clearly in view face fundamental challenges in serving the very purposes they are conceived to address. The result is a proliferation of tools, platforms, and databases that, while varied in terms of the quality and kind of information provided, resemble each other in both form and function, and therefore face similar challenges to uptake and use.

3. Information Biases

A great deal of policy dialogue and decision-making is ideologically driven, or otherwise centrally concerned with advancing positions for unilateral political gain; it is often challenging to find a non-biased view or else (as we came to observe with cyber issues) a sufficiently broad range of views. The substantive information that may be crucial for arriving at well-informed decisions from the point of view of practical consequences (for example, viable implementation), can sometimes be nearly impossible to identify when it is arguably needed most. Increasing the readability, searchability, and timeliness of information cannot address the problem of political positioning often taking precedence over the provision of balanced information in many dialogue and decision-making contexts. This is a widely known, yet persistent barrier to the use of information across a range of policy and policy-related processes.

These findings suggest that new attention needs to be directed to the conditions of information use, and the barriers that might get in the way if our goal is to do more than simply provide information, and instead actually improve policy dialogue.

1.3. Implications for UNIDIR's Cyber Resources

In-house expertise and other expert consultations on cyber issues suggested that these findings from UNIDIR's EBD projects might be of direct relevance to UNIDIR's strategic goals for the *Cyber Index*. Therefore, UNIDIR decided to reconsider the otherwise expected and familiar move of putting the Index online as a sufficient approach for improving policy dialogue in the cyber domain.

Instead, we took the decision to embrace the EBD findings about information use, and utilize the evidence-based design methods that were developed to address such barriers, for the purpose of contributing to cyber stability.³ Our collective goal was to create a new kind of solution that not only provides information but also—uniquely—facilitates its use in the policymaking process.

In this way, we have turned our attention away from solutions for *accessibility* of information, and towards practices of use, focusing instead on how to make information visible, and usable, to policymakers and diplomats, and relevant for their actual uses. While unconventional in policy circles (at least when applied to policy design itself), this move enables us, as an Institute, to innovate new ways for improving policymaking

³ For the purpose of this document, “cyber stability” is defined as a geostrategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels. This is further explained in Section 2.

in an area where many actors are struggling to effectively digest, manage, and use information to achieve effective policy results and outcomes.

1.4. Revised Parameters: Studies, Compendiums, and Tools

Shifting our attention to the *use* of information as a potentially powerful way of improving policy dialogue directs our attention to the creation of a tool to enable people to do so.

A study (as with the original Index) provides information and analysis to inform the reader. An online resource makes such information and analysis accessible. By contrast, a tool assists the tool user in accomplishing a task.

To design a tool for policymakers working on cyber stability, we needed to understand the users for the proposed tool and the uses to which users actually put information. Only then could we understand the specifications needed for the tool, much as an engineering team needs to understand the specifications of a project in order to design an approach to solve it.

1.5. Aims of a Tool

Advancing towards a tool presented a new set of investigative and design requirements. Specifically, it required an understanding of the uses to which information would be put, and then building a conceptual framework to guide the generation and organization of that information for those uses. This approach is entirely different from that used to create a study, because it first identifies the practices to which information will be put, and then the means of application specific to the user group. Unlike the creation of a generic “cyber profile” for a state, the components of which are determined a priori by researchers, this approach makes the eventual cyber profile a response to users practical needs, and their uses for information. This is not a subtle intellectual modification of emphasis: it is a paradigm shift in the application of information to affect outcomes in policymaking.

Without question there is widespread need for producing information relevant to concerns of cyber stability, and UNIDIR continues to make contributions in this area, as do other international organizations, private sector actors, universities, think tanks, and NGOs. However, we believe that impact from a tool is about more than “uptake” of information by policymakers in their deliberations and decisions. Rather, we see the purpose of a tool as facilitating or improving practice in some domain. This means that, on the one hand, the goals that policymakers set for themselves can be better achieved through use of the tool, and on the other hand, that strides are made towards the preferred conditions we wish to create—in this case, conditions of international cyber stability.

If this fundamental reorientation is not undertaken, we realized, then the new tool runs the risk—as with a multitude of other studies, surveys, and research products created at think tanks across the world, and at great effort and expense—that the valuable

information generated and presented will become part of the ever-growing pile of ignored, misused, or unapplied information that policymakers contend with daily.

Past experience affords us limited precedent in the face of present and emerging cyber realities. In the face of changing contexts, technologies, actors, and problems, there is no map of this new and uncharted territory. What is needed in such situations is **not a map but a compass**—a tool that can help people navigate a rapidly shifting terrain in order to head in desired directions. We believe that providing such a tool is a practical and targeted way of building policymakers' capacity to engage more effectively in cyber stability policy discussions.

Therefore, in this document we present a model for a Cyber Stability Policy Tool that can assist users in the selection and use of valuable and appropriate information to their specific tasks across a range of circumstances and needs. We believe that this approach is best suited to supporting informed, considered, pragmatic policymaking in the cyber stability field.

2. Goals and Methods

2.1. Impact Goal

The shift in orientation discussed above, from providing information to also facilitating the effective use of that information, requires an articulation of a new goal for the tool—one that specifies the kind of impact the tool should be designed to contribute to. As such we have developed the following overall impact goal:

To contribute towards the achievement of international cyber stability by improving the capacity of diplomats and policymakers to participate in a more informed and effective manner in dialogue and decision-making processes pertaining to stability in the cyber sphere.

Note that the impact goal specifies practices to improve (dialogue and decision-making), users to address (diplomats and policymakers), events or situations where the use of information can improve participation, and thematic issues of concern (those pertaining to stability in the cyber sphere).

2.2. Parameters for Tool Development

The impact goal thus provides a clear target of what to address and to achieve, and creates certain parameters and criteria to guide the process of tool development.

The following are of particular relevance:

- *An orientation to improved conditions:*
The impact goal is oriented towards the conditions in the world that we aspire to achieve—in this case improved “cyber stability”.
- *A focus on dialogue and decision-making practices:*
The impact goal focuses on the particular domain of “informed and effective” dialogue and decision-making because this is where information is most directly applied to consequential activity in administrative activity, in the political sphere, and in multilateral processes.⁴
- *An emphasis on building capacity of individual users:*
The impact goal targets the need for improving the capacity of diplomats and policymakers as individuals, in part because we came to learn through the research process that a significant lack of personal knowledge and expertise in navigating cyber policy topics was perceived by many to be one of the greatest hurdles to effective participation in policy development. This was especially emphasized at the multilateral level.

⁴ These findings further support, and are informed by, an established base of knowledge on decision-making; see, for instance, Herbert A. Simon, *Administrative Behavior: A Study of Decision-making Processes in Administrative Organizations*, 4th ed., 1997.

- *A requirement of adoptability:*
No tool is developed or sustained in a political or financial vacuum. It is our judgment that a tool focused on improving individual performance is a realistic and attainable impact objective for a UNIDIR-based tool with its attendant resource profile, and in the context of other tools now available or in development by other actors.

2.3. Key Concepts

2.3.1. A Working Definition of Cyber Stability

In addition to these parameters, the development of the tool is also guided by a definition of cyber stability. Since this concept represents the set of conditions the tool is meant to contribute to, we must specify what those conditions are. After all, to know whether progress is being made in a journey, one needs to know the final destination.

Cyber stability is an emerging concept. The term is enjoying growing uptake in general use, owing to its utility in helping us focus some cyber policy discussions on concerns of international peace and security. Because it is an emerging concept, the primary purpose of which thus far has been to frame issues and discussions, “cyber stability” has not yet been developed as an analytic category. A key aspect of UNIDIR’s ongoing cyber work is to continue to refine this working definition and demarcate the boundaries of the concept. Such a category sufficient for guiding information-gathering and decision-making processes is needed in order for policymakers to work productively towards cyber stability as a shared goal. It is also foundational for orienting the development of a tool that can support policymakers in such efforts.

For the purpose of this document, therefore, we define cyber stability as:

A geostrategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels.

This definition creates a basis from which to discern—when stability is the goal—what is potentially relevant, useful, and strategic information about activity in the cyber domain from what is not. It can also serve as a basis for determining what resources and activities can be directed purposefully towards that end.

2.3.2. The Target User-Group: Supporting the Individual

The nature of the cyber sphere presents many challenges to stakeholders endeavouring to be more effective in their roles as diplomats and policymakers. Among other matters, the technology itself is pervasive, touching every aspect of modern life—whether directly or indirectly—in much of the world today. Unlike some other thematic concerns of international peace and security, such as anti-personnel landmines for example, the parameters of the problem are not easily defined: in fact they are extremely nebulous and opaque. Likewise, technological developments and applications advance rapidly, therefore so do the concomitant benefits and risks and hence topics to address and consequences to be understood.

This is exacerbated by the extreme interconnectivity produced by, and in, the cyber sphere, which makes security at the national and international levels inherently inter-related and difficult to parse in a way that may be different than other thematic concerns.

In terms of interstate cooperation, there is also the challenge that the level of capacity and awareness across national actors (and staff within national governments) is highly varied, as is the approach taken within different governments to address and manage cyber issues as a matter of security and stability.

Given these conditions, and from our position as a United Nations institute focused on international peace and security, we believe that one way to contribute to the achievement of global cyber stability is to support capacity-building at the individual level.

Therefore, our target user group consists of policymakers and diplomats,⁵ working at a variety of levels, who are involved in practices and activities pertaining to the development and negotiation of policy relevant to the conditions of cyber stability at the regional and international levels.

The impact goal's focus on improving the capacity of diplomats and policymakers at the individual level is a practical approach that could bring added value to the community, and that has the potential to create more long-term benefits than we know is possible with the provision of information alone. Indeed, as cyber stability is both emergent and rapidly evolving (both as a concept and a set of conditions), capacity-building for diplomacy and policymaking in this sector is in strong demand and vitally needed as one (of many) means to contribute towards the achievement of cyber stability.

2.3.3. Defining Capacity in Cyber Policymaking

The capacity for informed and effective participation can be defined in many ways. We learned that, for many policymakers, this involves competence in three key areas:

- a. Knowledge**, which concerns whether an actor has sufficient content or thematic knowledge about the problem, technology, challenge, risk, etc. to be discussed;
- b. Practice**, which concerns whether there is sufficient experience or expertise for performing the role and task assigned;

and linking the two together in:

- c. Strategic application**, which concerns the ability to mobilize content knowledge effectively and appropriately in the performance of an assigned task or role.

As we will develop in greater detail below, strategic application is a rich point for moving towards our impact goal.

Therefore, for the tool to satisfy the impact goal, we will need to determine what kind of functions could support capacity in these three areas and how.

⁵ From this point on in the document (for sake of simplicity), we use the term “policymakers” broadly to also include diplomats to refer to this target user group. We also use the term “users” when discussing policymakers and diplomats in reference to their engagement with the proposed tool.

2.4. Methods

As an approach, EBD is particularly well-suited to the present problematic thanks to three key features:

1. *It is impact driven.* Designing for impact means working explicitly and intentionally towards the achievement of a specified impact goal or set of impact goals. The EBD approach begins with the identification of impact objectives, and develops a research and design agenda specifically in the service of those objectives. Placing the impact goal at the centre is a radical and innovative departure from other administration-driven approaches that are directed towards output goals. The EBD approach better ensures transparent and strategic progression towards the changes we want to see in the world.

2. *It is user oriented.* In a mandate-driven system, we become accustomed to top-down approaches to creating change. But, a key tenet in the design of products and services is “know your customer”, and for good reason. There is demonstrated value and wisdom in having knowledge of the day-to-day experiences, preferences, and practical requirements of the target user groups for any tool, as these matters are crucial for designing effective solutions. A key element of the EBD approach is therefore user research, which focuses on understanding the real and practical user needs relevant to the achievement of the impact goal.

3. *It is practice based.* An inherent driver in any impact-driven endeavour is practice—that is, the things people do that have beginnings, middles, endings, and consequences. In order to work towards impact, we have to know what kinds of tasks and activities can help to bring it about, or might stand in the way. The practice-based approach—both analytically and for the benefit of design—steps away from received or presumed categories about action and takes a fresh, methodologically sophisticated, and applied approach to understanding the real-world practices that users are actually engaged in, so that these practices can be supported or modified directly through innovative design solutions.

EBD provides a framework organizing a range of approaches to both research and design, selected on the basis of relevance for the particular research needs and design tasks at hand. However, the three features listed above mean that approaches sufficient to the discovery and description of practices and needs are typically involved. Methods and techniques for data generation and analysis are drawn from various approaches to ethnography, organizational analysis, user research, and design research. These are combined with relevant thematic expertise, which in this instance includes international relations, security studies, and diplomacy.

2.4.1. Project Structure

Using UNIDIR’s EBD process, the project was designed around five phases of research, analysis, and design (with iterative practices occurring in each).

Phase I: Developing the impact goal and research design

The first phase of analysis consisted of the identification of an impact goal for the tool, and the design of a research phase. Following an orientation to the content area, the team used EBD techniques for goal identification, stakeholder mapping, and developing success criteria to serve as guiding parameters for the research and design process to follow. Information for this phase was generated through a literature review, and through consulting a range of political documents, conference proceedings, and briefings, the review of project documents, conducting observations at a conference on cyber stability, and a usability analysis of the 2013 *Cyber Index*. This information was then used to develop the research agenda and interview guides, and to set preliminary parameters for the design of the tool.

Phase II: Establishing user information needs

The second phase of analysis was dedicated to learning about the information needs of policymakers engaged in cyber policy discussions. For this phase, a series of open-ended interviews was conducted with cyber policy experts, many of whom advise governments and participate in international forums, from both the public (universities, think tanks, and NGOs) and private sector. Interviews were also conducted with a range of members of the diplomatic corps (both acting and retired) from different global regions. Findings from the two groups about the information needs of policymakers, pertaining to cyber stability, were subjected to comparative analysis.

Phase III: Understanding user practice

The third phase of analysis consisted of discerning key needs and challenges in the practices of the target user group relevant to dialogue and decision-making in the cyber sphere. Preliminary interviews were conducted with members of the diplomatic corps in order to understand better the nature of a policymaker's or diplomat's day-to-day experiences. A sequence of activities was developed for how policymakers prepare for performing their tasks and roles in dialogue and decision-making events or activities. Analysis was conducted to understand the relationship between these findings and the parameters set by the impact goal.

Phase IV: Aligning needs and functions

In the fourth phase the team initiated the first cycle of the iterative design process, in which needs and challenges were refined and prioritized, and functions for the tool were developed. A user journey was mapped, and an initial design direction was proposed, with various design solutions being proposed for performing tool functions. Revisions to the initial designs were completed following an internal feedback session at UNIDIR, and again following a design assessment meeting.

Phase V: Creating the visual design of the prototype

In the fifth and final phase, technical expertise was engaged in order to develop the visual design for the prototype presented in this document.

2.5. Outcomes Included in this Document

With our impact goal in mind, we tasked ourselves with developing the conceptual and practical foundations needed to develop the new resource. Consequently, this document:

1. Produces an initial assessment of the needs of the community and of users to identify both the information-based needs and the practice-based needs of our target user group in relevant situations or events where tasks will need to be performed;
2. Identifies the key functions a tool must provide in order to address these needs; and
3. Proposes an initial model for further development.

In the following sections we share the key findings from our research, and develop a set of needs the tool should address. We then indicate the functions that the tool would have to perform in order to address these needs, to contribute to the impact goal, and to address the preliminary success criteria. Finally, we present the visual design for the tool prototype created from this research, design, and analysis work.

3. Findings from the Design Research

There are many challenges to effective participation in dialogue and decision-making around cyber stability. Learning about these is crucial in order to determine what kinds of functions a tool must serve if it is to create improvements. Having developed the impact goal and overall research design, the project team conducted a series of interviews and consultations with policy experts and policymakers as potential users of the tool in order to learn about some of these difficulties or potential obstacles. Our objective in such inquiry was not to understand the contours of the debate, for example, around internet governance, or the solutions to specific technical cyber challenges being advanced by different actors (though of course it is important to be aware of all this). Rather, as key activities in policy action, we wanted to understand something about the challenges to effective dialogue and decision-making in the case of cyber stability, as seen from the vantage points of different stakeholders to such activities.

3.1. Substantive Challenges

From these interviews and consultations, a core set of challenges emerged which centred upon issues of information, knowledge, and expertise (or substance):

- When it comes to the cyber sphere, many users do not know where to begin.
- There are multiple definitions of terms and concepts—which makes meaningful discussion challenging among participants in dialogue and decision-making.
- It is difficult to prioritize what is really important for the tasks at hand.
- There is a wide discrepancy among states in terms of their “cyber awareness” (or understanding of and engagement with cyber challenges) and therefore ability to successfully engage the subject matter.
- Political disputes between state parties on matters not related to the cyber sphere tend to “spill over” to cyber sphere discussions, thereby confusing issues and priorities.
- As with other technical areas, the technological information and developments move more rapidly than what individuals can keep up with.
- A characteristic of the cyber domain is “hyper-connectivity” (of people, networks and issues) which makes the security of different actors contingent upon the activities of others in new, pressing, and often continually changing ways.

This first set of observations directs our attention to challenges stemming from a lack of awareness, information, knowledge, and understanding about cyber technology itself on the part of decision-makers, and about the consequences of this across a number of domains relevant to cyber stability. Subject experts told us that many participants in policy conversations on the topic lack a basic understanding of the subject matter, which makes progress difficult or even impossible in some circumstances.

3.2. Practical Challenges

Alongside the observations above, discussions with policymakers highlighted the practical realities they face in performing their roles and carrying out their tasks and responsibilities day to day. Describing and understanding these realities is a crucial aspect of designing for our impact goal, for it helps us understand the “operational context” in which knowledge about cyber stability must be gained and used. Therefore, we gave some attention to learning about those **roles and tasks**, the **typical sequence of activities**, and **key characteristics** of the nature of their work.

3.2.1. Roles and Tasks

Policy work, of course, involves the performance of numerous roles and tasks on the part of any individual, and may depend on the specific position of the policymaker.

When we stepped back to try to discern the most broad yet central roles or responsibilities carried out by policymakers in participating in such practices, and for staff working at a variety levels (in the hierarchy of seniority), we found that these can be described with three general modes: formulating policy, advising on policy matters, and representing policy positions at a range of events and meetings.⁶ These roles and responsibilities shape (and sometimes define) the objectives of a policymaker’s participation in dialogue and decision-making practices and events of various kinds, from informal and internal, to formal, high-level, and external processes. Examples include (but are not limited to) participation in regional conferences and forums, a range of inter-ministerial and intergovernmental meetings, treaty negotiations, drafting sessions, meetings of the General Assembly, the Conference on Disarmament, Groups of Governmental Experts (GGEs), and policy processes (such as the so-called London Process).

3.2.2. Typical Sequence of Activities

Regardless of the role being performed, the task or event being prepared for, and irrespective of the topic at hand, policymakers and diplomats must find a way to move from a set of information, towards the end of achieving some strategic goal. From the descriptions provided by interviewees, we discerned a four-step sequence that seems to represent this general process. The analysis and formulation that takes place throughout this process is highly sophisticated and iterative. Here we describe the basic sequence itself only in terms of the rudimentary steps.

Step 1: Identify relevant information: *What do I need to know?*

Given the task at hand, the role assigned, and the strategic objective in view, policymakers must determine what they need to know. Policymakers and subject experts alike described a wide range of information as being relevant to the policy process, regardless of the topic at hand, including information about the political

⁶ While not intended to be an exhaustive list of roles or tasks performed by policymakers, these three modes of activity seem to sufficiently capture those that are central to dialogue and decision-making, for the benefit of the design objectives at hand. Though aspects of each mode may be involved in the others, the purpose here is, by articulating different responsibilities and practices to identify key aspects of policymaker’s work, to begin to develop the foundations for a tool to be both useful and useable.

positions of key actors, relationships of key actors, historical legal precedent, relevant legal frameworks, relevant technical information, current processes and events, regional positions, and “situational awareness”.

Step 2: Get informed: *How do I learn it?*

Policymakers have a variety of strategies and resources for getting informed. They read briefings prepared by their own ministry; consult with technical experts; consult with a range of actors, including, in some cases, academics, civil society, and private sector actors; and read materials from regional forums and international organizations. They may do some of their own research, consulting conference proceedings, the press and, as more than one interviewee told us, Google, Wikipedia, and through what some call “osmosis”.⁷

Step 3: Make sense: *How can/should I make sense of this information?*

Making sense of information here means interpreting it for relevance to the task and strategic goal at hand. This is both situational (depending on the dialogue or decision-making process to be engaged), and perspectival (depending on the policy objectives of the represented state, region, or international entity). But it is also very individual (depending on the insight, experience, and expertise of the individual policymaker).

Step 4: Apply information to carrying out tasks: *How do I make use of it?*

There are a range of “policy products” or “outputs” that policymakers produce in fulfilling their tasks and roles. Speaking on a conference panel, drafting a policy statement, writing a diplomatic cable, or engaging in negotiations are all instances in which information is being applied to policy processes. The objective of such products and tasks is to advance towards a strategic goal. Both policy discussion itself, as well as these particular work products and others (for example speeches, lectures, position papers, draft legislation, cables, “notes verbales”, agendas for meetings, etc.) are some of the primary means of conducting policy work, and are usefully understood as instances of application, where information and knowledge are substantially used in the shaping of solutions and outputs.

3.2.3. Key Characteristics

When policymakers talked about their day-to-day jobs, they systematically described or cited the following features as characterizing the nature of their work, regardless of the specific tasks or roles discussed:

- *Rapid*: Policymakers are busy people. They often have limited time to prepare for meetings in which they will play a role in either formulating policy, advising on policy matters, or representing the policy position or objectives of their government. They must synthesize many different kinds of information (technical, political, legal) across themes and relationships, and must always do so quickly.

⁷ We understand this usage of the term by the interviewees to refer to the informal process of “absorbing” information by virtue of being in and around a range of discussions, or through experience.

- *Both Analytic and Intuitive*: As one interviewee put it, “Coming up with policy comes down to sophisticated intellectual analysis of the right information”. Doing a good job at this is often described as a function of an individual’s ability to mobilize and combine their education, experiences, situational awareness, and “political intuition” in the service of their job. A good policymaker or diplomat, we were told, is someone who shows exceptional capacity in bringing together many different kinds of information, with such capacity understood as a function of strong powers of analysis, paired with good “political intuition”.
- *Idiosyncratic*: There is no one way to develop or create good policy positions. Indeed, it is precisely an individual’s own way of bringing their expertise together with the many different kinds of information relevant to the topic or decision at hand that makes this a process ill-served by a standard recipe, method, or protocol. Policymakers explained that they have their own processes, individual to them, that they use in coming to their positions, recommendations, etc.
- *Collaborative*: Policy work is by nature collaborative. Policymakers work as part of a team within their ministry or mission, in numerous working groups, task groups, and committees, and with their counterparts in other governments.
- *Emphasizes Communication*: Because of the highly intuitive and collaborative nature of policy work, the ability to communicate ideas, arguments, and positions clearly, and in different contexts, was described as crucial, especially for effective participation in dialogue and decision-making practices.
- *Hierarchical*: The roles and therefore tasks performed by individuals occur within a strict hierarchy or command. These basic activities and key characteristics can be viewed as (at least one version of) the general “terrain” of policy practice, from the point of view of policymaker experience.

When the specific challenges and barriers related to dialogue and decision-making around cyber stability are mapped on to these practical concerns of policymakers, a key set of user needs comes into view—needs that a digital tool must serve in order to contribute to improving the capacity of policymakers to participate more effectively in dialogue and decision-making.

These features or characteristics tell us something about what it is like to carry out the sequence of activities above. They help us understand, qualitatively, some of the key features, skills and requirements of this kind of job which one may never read about in a job description, but which nevertheless are recognizable to policymakers and diplomats regardless of government, rank, or role.

By paying attention to both what users do and how they do it, we learn about the key characteristics of activities through which policymakers prepare for and carry out their work, regardless of topic. This gives us an important insight to consider in determining what kind of support the tool should give. We learn that building capacity in this practical context requires paying attention not only to what policymakers need to *know* about in order to perform their tasks, but also to what they *do*, the nature of those tasks themselves, and the contexts, conditions, and ways in which these are performed. As noted earlier, for many policymakers, participation in the key activities

of dialogue and decision-making involves competence in three key areas: knowledge, practice, and strategic application.

Though perhaps an obvious point, to participate well in policy discussions and other activities, a policymaker requires sufficient content or thematic knowledge about the problem, technology, challenge, risk, etc. to be discussed. A policymaker also requires a degree of competency in the practice of the profession. This requires sufficient education, experience, and expertise. One needs to know what the job is and how to do it. This often means the ability to know what kinds of things need to be understood outside of the content area in order to get things done. Understanding the set of political goals and relationships involved, the relevant legal frameworks and policy tools, as well as the historical context relevant to discussion or decision at hand, are all crucial.

The distinctive capabilities and special skill of the policymaker are both displayed and judged when they are linked together in strategic application. This concerns the ability to mobilize content knowledge effectively and appropriately in the performance of an assigned task or role to bring value to their government, partners, and the processes in which they play a role.

To understand this is to be aware of a central and rich point for discovering new ways to improve capacity for effective participation in dialogue and decision-making.

With these insights in hand, we are in a position to begin determining what kind of support would be most useful and what forms it should take.

When we consider the sequence of activities that policymakers tend to follow, and then consider the means by which they tend to work through the steps, a few conclusions emerge about the conditions and manner in which they work:

- While the process is reasonably linear (in moving from not knowing something to knowing something to using it), the way each of these steps is carried out is not. Rather than proceeding logically or systematically, most policymakers are effectively improvising their way through information chaos, and in their own way. This creates an ambivalent relationship between the policymaker and the conditions they face. On the one hand, they do not like the messiness and recognize that it is a problem that leads to suboptimal results. On the other hand, it is through their unique capacities to manage this state of affairs and still create value and exercise judgment that their special, perhaps unique, competency is both shown and judged.
- Policymakers welcome tools that could help them, but are wary of tools that might restrict, limit, or try to control how they work. As the means of working with information are so varied, and as policymakers have (or are continually developing) their strategies of work, they are cautious but curious about tools that might help.
- Lack of information, per se, is not the problem. The issue is making the best use (that which helps them perform their task or role by bringing the greatest value) of the information one has. This insight in particular foregrounds the importance

of looking at the intersection of knowledge and practice in order to determine opportunities where a tool might lend support.

These findings and insights have special bearing for us in determining what kinds of functions a tool must serve if it is to create improvements. They confirm that there are important information needs to attend to where cyber stability is concerned. But more than that, they also tell us that the intersection of knowledge and practice—strategic application—is crucial to attend to, in order to improve capacity in this or any policy sphere. Whatever content information must be gained for a specific policy discussion, it will be used to accomplish certain tasks, perform certain roles, and do so in the context of certain conditions.

Therefore, to focus on one half of the equation in the face of our findings would be to miss an important opportunity. We can no longer only focus on what people need to know. We must also attend to what they need to do.

In the next section we turn these insights about the challenges policymakers face to effective participation in dialogue and decision-making on cyber stability into an explicit set of defined user needs, and then explain the functions of the proposed tool that might meet them.

4. Needs and Functions of a Tool

The next steps in this process are to discern (from the challenges discussed above) a set of key needs that must be addressed by a tool if we are to meet our goals and be of service to the target user group, and then to propose functions for the tool to perform in order to respond effectively.

To do this the team conducted an iterative “diagnostic” process, cycling through the above findings and insights against the backdrop of the impact goal, success criteria, and additionally the concept of cyber stability as defined in the introduction. This analytic process revealed a primary need that can set the core function of the tool (that is, a tool to do what?).

We then mapped the particular challenges of cyber stability as a topic area onto the “terrain” of policymaker experience and practice just described. In doing this, a specific set of needs or challenges are illuminated. These are the needs or challenges that must be addressed by the proposed tool, in order to build capacity in cyber stability policy activities among policymakers.

To determine the specific functions that could address these needs, we focused on the sequence of practice described above, and identified the key challenges encountered at each step when matters of cyber stability are of concern. We then developed a series of propositions for how the need and challenges might be responded to, by asking what function a tool would need to perform in order to do so.

What emerges are initial indications of a user journey⁸ for cyber stability policymaking and proposed functions to support it that can be delivered in the context of a digital tool. The technical capabilities for performing the proposed functions already exist, however we believe that the blueprint represents a novel assembly of functions to address this particular user group and their specific needs in terms of both content and practice.

In looking across a range of policy discussions and debates relevant to matters of cyber stability, a range of political documents, conference proceedings, and findings from interviews and consultations with policymakers and policy experts as discussed above, we note that, to date, there can be significant challenges associated with framing discussions around cyber risks and threats from an *international peace and security perspective*, especially one that can address policy concerns at the regional and international levels.

A number of factors discussed above contribute to this challenge. We note in particular the proliferation of approaches available and used for identifying various risks and threats, and proposing solutions, in the cyber domain. These include (but are

⁸ The term “user journey” refers to the series of steps that represent a scenario through which a user may travel in interacting with a service, software, or other medium.

not limited to) approaches to cyber maturity,⁹ cyber readiness,¹⁰ cyber warfare,¹¹ cyber instability,¹² and wide-ranging discussions on cyber conflict and cyber security. It is of course neither likely, nor proposed, that a single approach be developed or adopted for such a complex issue. However, from the point of view of some policymakers—especially those who may be novices in addressing the cyber dimension of peace and security—this proliferation of options can be difficult to navigate. This is a broadly experienced challenge to effective participation in a range of policy activities.

There is a need, then, to help policymakers more clearly frame discussions around cyber risks and threats from an international peace and security perspective, and address relevant policy concerns at the regional and international levels.

Tool Functions Required:

1. Provide an explicit way of applying a cyber stability lens to the activities policymakers engage in preparing to participate in dialogue and decision-making practices.

The Tool Can Achieve This By:

1. Pioneering the use of a definition of cyber stability as an analytic category to help orient analysis, dialogue, and decision-making among international actors.
2. Creating the first Country Profiles organized on that basis, indicating the key categories through which cyber stability is developed and tracked over time.
3. Framing policy discussions by providing policymakers with an impact-driven, strategic basis upon which to ask questions, analyse information, and ultimately contribute more effectively to meaningful dialogue and decision-making around cyber stability as a policy objective.
4. Revolutionizing the role of information technology for policymaking through providing practice-based functions that respond to the actual practices of the user group with a view to creating a “pull” for cyber stability analysis and information.

The tool can achieve all this if it is developed to attend to the particular the needs that policymakers encounter in the specific steps of the activity sequence as outlined above. The following items, organized by sequence step, identify key user needs and the tool functions required to respond to them.

Step 1: Identify relevant information

User Need

Key activities for policymakers can include participation in a wide range of activities and events pertaining to concerns of cyber stability, such as meetings, conferences, negotiations, GGEs, etc. When preparing for participation it can be challenging to figure out what information, and about what aspect of cyber stability, is relevant.

9 T. Feakin, J. Woodall, and K. Aiken, *Cyber Maturity in the Asia-Pacific Region*, Australian Strategic Policy Institute, 2014.

10 Melissa Hathaway, “Cyber Readiness Index 1.0”, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2013.

11 F. Shreier, “On Cyberwarfare”, DCAF Horizon 2015 Working Paper no. 7, Geneva Centre for the Democratic Control of Armed Forces, 2012.

12 J.C. Mulvenon and G.J. Rattray (eds), *Addressing Cyber Instability: Executive Summary*, Cyber Conflict Studies Association, 2012.

Challenges for Cyber Stability Policymaking

Figuring out what is relevant is partially determined by the kind of activity or task to be performed, the kind of event at which it will be performed (conference, meeting, high-level consultation, etc.), as well as the issue to be discussed (for example, cyber “warfare”, the role of national cyber security strategies, terrorism and cyberspace, etc.). Where cyber stability issues are concerned, some policymakers express their difficulty in “even knowing where to begin”.

Tool Functions Required:

1. Identify the pertinent issues policymakers need to know about from a cyber stability perspective, in order to prepare for their actual tasks.
2. Indicate the types of information important for being informed about those issues.

The Tool Can Achieve This By:

1. Taking a user-centred, task-driven approach to help users align information with their practical needs.
2. Guiding users on what to pay attention to when cyber stability is the goal.

Step 2: Get informed

User Need

Having identified *what* they need to know about, policymakers need then to find the right information quickly in order to be informed. “The right information” means not only that it must be on the right topic, or of the right kind, however. It also means that it must be “readily digestible” if it is to be useable.

Challenges for Cyber Stability Policymaking

Many different kinds of information are drawn upon in preparing to participate in dialogue and decision-making practices. This, coupled with the general condition of “information proliferation”, makes locating useful information a time-consuming task (hence one often delegated to more junior staff). Further, when the topic or problem at hand is unfamiliar, or the cyber stability dimension of it is, useful resources may be missed.

Tool Functions Required:

1. Provide the rapid identification and location of relevant and useful resources.

The Tool Can Achieve This By:

1. Operating according to robust and relevant cyber stability categories for organizing information from a cyber stability perspective.
2. Supporting a strategic approach to preparation by maintaining a task-driven approach.
3. Providing curated links to useful and cutting edge resources.
4. Providing or linking users to information about regional organizations and forums.

5. Providing bespoke issues briefs that can be updated according to relevant events and developments.
6. Providing information and analysis at the state, regional, and international levels (for example, country profiles, topic briefs, etc.).

Step 3: Make sense

User Need

Having located the right information, policymakers must of course make sense of it. For policymakers participating in formulating, representing, or advising on policy, this means analysing and interpreting information for relevance to the task and strategic goal at hand.

Challenges for Cyber Stability Policymaking

While the specific and individual strategic goals for which a policymaker may employ the tool will vary widely, subject experts and policymakers alike stressed the need for support in how to make sense of information for the benefit of common practical goals—participating in cyber stability dialogue and decision-making. Significant national variations in terms of “cyber maturity”, awareness, and prioritization means that there is a very wide range of support needed to include the widest range of states possible—from “the basics”, to more specialized guidance in framing emerging issues and discussions.

Tool Functions Required:

1. Facilitate the user’s application of a cyber stability lens to their own analysis and preparation activities.

The Tool Can Achieve This By:

1. Providing specific forms of information central to assessing, evaluating, and building cyber stability (such as country profiles, topic briefs, and trend reports)
2. Presenting data and information according to categories relevant to assessing, evaluating, and building cyber stability.
3. Incorporating innovative data visualization tools.
4. Enabling the comparison of data and information.

Having completed these initial three stages of information identification, compilation, and interpretation, policymakers then need to use it for a specific purpose—that is, turning information, and personal analysis, into task-relevant outputs (like policy briefs, presentations, policy positions, diplomatic cables, etc.)

The needs and challenges that policymakers encounter at this step are not particular to cyber stability as they are a feature of practice, rather than content. It is our assessment that the needs and challenges at this crucial phase are a function of a gap in the process of moving knowledge to action, where individual techniques and talent are employed to bridge the two.

Above, we learned that—in the words of some policymakers we interviewed—there is no one “technique” or “recipe” for turning information into the “products” (or outputs, or artefacts) through which policy is formulated, advanced, and ultimately instantiated. Rather, each individual has their own way of making sense of materials, information, and experience, and bringing these together through the benefit of their own insights (about political palatability, relational tolerance, knowledge of process and contexts, etc.), born from their own experience, expertise, training, and talents.

Perhaps in part because of this aspect of practice we note that there is no formal means for moving from analysis to output. Policymakers are not only free to develop their own techniques and practices (which they described as “personal”, “organic”—that is, informed but individual); indeed, it is the special capacity of policymakers in this area of strategic application that demonstrates their value in their role.

Because this aspect of strategic application is so central to policymaker competence, we believe this highlights an important opportunity to create a tool function that can support policymakers in making the most of their individual processes to strategic ends.

To do this, we therefore formalize an interim step in the sequence that presently takes place, but “under the radar”, between the “ Making Sense” and “Applying Information to Action” steps of the four practice steps laid out in Section 3 (Findings from the Design Research). This step has been named “Organize for Use”.

Step 4: Organize for Use

User Need

Policymakers consult and make use of many different kinds of information, on many different topics, in conducting their tasks and creating the various outputs through which they perform their roles and responsibilities. Invariably, they collect and organize these materials, which are then put to several different uses in performing the range of tasks and activities for which they are responsible. These include the range of outputs discussed above (such as speeches and presentations, briefings and diplomatic cables, reports and recommendations, etc.). One way or another, individuals must organize and store such materials.

Challenge

One of the key impediments to using information and evidence in the design of policies and programmes is the lack of visibility of information to the user when designs and decisions are being crafted, which is to say, in those moments when individuals sit down to create their outputs. The sheer volume of information that must be assessed, the number of sources to be consulted, the speed at which it arrives and accumulates (and then corrects or negates earlier information) can make it exceedingly difficult to ensure the efficient and effective use of information in crafting well-considered positions, decisions, and contributions to policy processes and outputs. This situation is exacerbated by the typically large number of tasks and topics attended to by individuals, and the speed with which preparation must take place.

Tool Function Required

1. Help users organize and access their materials for the specific uses they must attend to.

The Tool Can Achieve This By:

1. Providing a dedicated digital workspace that helps users to organize information they have identified and gathered through the tool in a way that:
 - Is personally adaptable, responding to the user’s preferred way of organizing their materials.
 - Is responsive to tasks or events (for example, in preparation for a specific meeting, event, or decision-making activity).
 - Facilitates application of the cyber stability framework.
 - Is portable and can be used on a range of devices.

User Needs and Proposed Tool Functions

| Sequence Steps (user needs/practices) | Practical Challenge | Proposed Function |
|---------------------------------------|---|---|
| Step 1: Identify relevant information | Figuring out what is relevant information, given the task at hand. | Identifying the pertinent issues policymakers need to know about from a cyber stability perspective, in order to prepare for their actual tasks. Indicate the types of information important to being informed about those issues. |
| Step 2: Get informed | Finding the right sources and information quickly. Knowing which information to prioritize. Finding easily digestible material. | Operate according to robust and relevant categories for organizing information from a cyber stability perspective. Support a strategic approach to preparation by maintaining a task-driven approach to the identification of information. Provide curated links to useful and cutting edge resources. Provide or link users to information about regional organizations and forums. Provide bespoke issues briefs that can be updated according to relevant events and developments. Providing information and analysis at the state, regional, and international levels. |

| Sequence Steps (user needs/practices) | Practical Challenge | Proposed Function |
|---------------------------------------|---|--|
| Step 3: Make sense | Knowing how to apply the cyber stability lens in the analysis of information. | <p>Provide specific forms of information central to assessing, evaluating, and building cyber stability (such as country profiles, issues briefs, and trend reports).</p> <p>Present data and information according to categories relevant to assessing, evaluating, and building cyber stability.</p> <p>Incorporate innovative data visualization tools.</p> <p>Enable the comparison of data and information.</p> |
| Step 4: Organize for Use | Select and compile task-relevant information resources efficiently; quickly locate and access materials for use in various tasks. | Provide a personal, practically oriented, portable digital workspace, anchored in the cyber stability framework. |

4.1. In Review

In this section we have presented the key sets of challenges and needs that indicate what the core functions of a Cyber Stability Policy Tool should be. The approach taken has enabled us to keep a steady eye on the impact goal, while keeping both feet firmly planted in the practical tasks and realities through which that goal must be achieved.

The resulting blueprint for a user journey has allowed us to envision how policymakers might make use of an online tool in order to address the practical needs and challenges we have identified. Modelled on the sequence of activities that policymakers use in preparing for participation in a wide range of dialogue and decision-making practices, the user journey (the pathway taken through the tool) is animated by functions that are designed to address key information needs at critical points of practice, and to do so in a way that consistently builds on a cyber stability approach.

The next step in this process is to propose and illustrate how this might be realized with a digital tool—how form might be given to function. The next section therefore presents the visual design for how these individually listed functions, when organized together as a tool, can animate a coherent experience for users of the tool that, we believe, can lead to more informed and effective participation in policy activities from a cyber stability point of view.

5. Proposed Models


This section presents a visual design for the tool and the resources offered in it, to give the reader a sense of the look and feel of the user experience as proposed. While one particular journey through the tool is presented in linear fashion, we underscore that, as with many interactive digital tools, a range of possibilities are available, and are a function of the navigation choices made by individual users within the parameters of the tool generally.

The illustrations here should be taken as the platform, or foundations, for the development of the tool, rather than a finished product. They represent the materials that would be used in the next phase of development, prototype testing.

The first set of illustrations shows each sample page in detail, linking it to the needs addressed, the functions performed, and the key features of the page. There is also an example of a fictional user journey, conducted by “Mark”, to help convey the path from one page to another. This helps to highlight how the user journey for the tool mirrors the activities sequence of policymakers presented above.

1. Landing Page

Sign in



Cyber Stability Policy Tool

A tool for policymakers and diplomats to prepare for briefings, meetings and negotiations related to Cyber Stability policy

What is Cyber Stability

Cyber technologies represent social and economic benefit but are also a key component in many military applications and non-civilian activities. Against this backdrop, there is increasing concern about how the cyber domain might be involved and affected during times of conflict. Without proper escalation controls, it is feared that traditional conflict may be spurred or even triggered by activities in the cyber domain.


In the field of international peace and security, there is a clear realization that cyber has the potential to become a geo-politically unstable domain.

Cyber stability is a geostrategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels.

[DOWNLOAD THE CYBER STABILITY FRAMEWORK](#)

Key features of this tool

Expert analysis, key documents and reference materials structured around Cyber Stability. [Enter](#)

-  [Cyber stability topic briefs](#)
-  [Cyber stability conferences](#)
-  [Cyber stability country profiles](#)

Download our Cyber Stability Quick Essentials Guide

[DOWNLOAD NOW](#)

© UNIDIR - 2014 [Contact us](#)

Needs Supported:

"Help me understand Cyber issues from an International Peace and Security perspective."

"Help me understand Cyber Stability as more than a term, but a policy objective, and a set of conditions."

"Help me understand what this tool is for."

"Help me identify relevant knowledge."

Functions Delivered: Orientation

- establishes and defines Cyber Stability as a distinct policy agenda and approach
- guides users on how to apply a Cyber Stability lens to their inquiry and analysis

Page Features:

- introduction to the "Cyber Stability" approach and definition of terms
- link to the Cyber Stability Framework
- orientation to the key features of the site and who it is for
- link to a Cyber Stability "Quick Essentials Guide"

2. Site Navigation

The screenshot shows the 'Cyber Stability Resource' website. The top left features the UNIDIR logo and the text 'Cyber Stability Resource'. A 'Sign in' link is in the top right. A navigation menu is open on the left, listing 'Home', 'I AM PREPARING FOR', 'Event', 'Process', 'Forum', 'I AM INTERESTED IN', 'Cyber Stability Topic Briefs', 'COUNTRY PROFILES', 'Country Directory', and 'Regional Directory'. The main content area has a dark blue header with the title 'Cyber Stability Policy Tool' and a subtitle 'for policymakers and diplomats to prepare for briefings, discussions and negotiations related to Cyber Stability policy'. Below this, there is a section titled 'Key features of this tool' with three items: 'Cyber stability topic briefs', 'Cyber stability conferences', and 'Cyber stability country profiles'. A green box at the bottom right contains the text 'Download our Cyber Stability Quick Essentials Guide' and a 'DOWNLOAD NOW' button. The footer includes '© UNIDIR - 2014' and a 'Contact us' link.

Needs Supported:

"Help me prepare quickly and efficiently."

"Help me prepare for my upcoming cyber stability related tasks."

"Help me figure out where to begin."

Functions Delivered: Identify Knowledge

- situates information inquiry in professional activities
- organizes information around key Cyber Stability categories
- provides rapid identification and location of relevant information based on professional practice

Page Features:

- pop-up navigation menu (present on all pages)
- navigation organized around key policymaking activities and practices
- direct access to curated topic briefs and country profiles

3. Forum Pages

Sign in

Cyber stability and the OSCE

The OSCE plays an important role in cyber stability regionally and internationally. The Organisation has put a significant focus on building confidence among participating states in order that the risk of conflict can be reduced and cyber/ ICT security enhanced in the entire OSCE region. The OSCE views that this is especially relevant in the cyber arena where the potential for misperception and escalation remains a growing concern. The OSCE views efforts to build confidence as particularly important as they can prevent misunderstandings and stop an attack from potentially escalating.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim.

[READ MORE](#)

Key Activities

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

[READ MORE](#)

Cyber stability issues at the OSCE

[CRITICAL INFRASTRUCTURE](#) [DATA CONTROL](#) [IHL](#)

© UNIDIR - 2014 [Contact us](#)

osce

<http://www.osce.org/>

Useful links and conference reports

- [Lorem ipsum dolor sit amet](#)
June 2013
- [Lorem ipsum dolor sit amet](#)
August 2012
- [Lorem ipsum dolor sit amet](#)
August 2012

Needs Supported:

“Help me understand the role of regional and international fora in cyber stability issues.”

“Help me prioritize top tier issues.”

“Help me apply a Cyber Stability lens to my inquiry.”


Functions Delivered: [Get Informed](#)

- presents background and analysis of key organizations from a Cyber Stability perspective
- identifies the relevant cyber stability issues policymakers need to know about

Page Features:

- overview of selected Forum with respect to its activities concerning Cyber Stability issues and policy
- quick-links to further site content (topic briefs) directly related to the Forum’s Cyber Stability activities
- links/downloads to reports covering the Forum’s Cyber Stability activities

4. Topic Briefs



Sign in

Topic Brief:

Critical Infrastructure

Abstract

Most countries around the world today rely on critical infrastructure that is increasingly at risk from a variety of hazards, including attacks via the Internet. We are dependent on broadband and wireless networks for the utility plants that pump water to cities, and the energy grids that provide for industry and individual consumers' needs alike. The security and resilience of these assets, systems, networks, and functions from cyber threats is rapidly increasing. Understanding vulnerabilities of these key national resources to cyber attack, and the destabilizing impacts an attack on them could have, is a crucial part of today's security environment.

Guiding Questions

- 1 What impacts would an attack on critical infrastructure have on geopolitical stability?
- 2 What confidence-building measures are currently in place to address cyber threats to critical infrastructure?
- 3 Have there been cases of successful cyber attack on critical infrastructure to date?

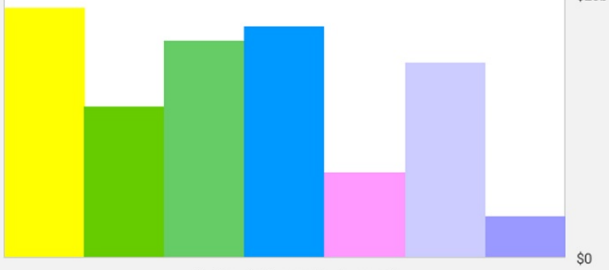
Related Topics

NETWORK VULNERABILITIES DATA CONTROL

IHL

Details and Analysis

Key Trends EXPENDITURE ▾



| Region | Expenditure (\$b) |
|----------|-------------------|
| Region 1 | 18 |
| Region 2 | 12 |
| Region 3 | 15 |
| Region 4 | 17 |
| Region 5 | 8 |
| Region 6 | 14 |

Regions (rollover or tap to reveal)

Critical Infrastructure and Cyber Stability

GOVERNANCE SOCIETY MILITARY CAPACITY

Overview

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

 System Vulnerabilities
June 2013

© UNIDIR - 2014

Contact us

Needs Supported:

"Help me get informed about Cyber Stability issues quickly and efficiently."

"Guide me in applying a cyber stability lens to my inquiry."

"Help guide further inquiry."

Functions Delivered: Get Informed + Make Sense of Information


- organizes and provides topic information according to categories of a Cyber Stability Framework
- provides questions to help guide the user's inquiry from a Cyber Stability perspective
- features a range of relevant information such as technical, legal, economic, political
- directs the user to other, closely related topic areas
- supports comparison of data and information

Page Features:

- summary of topic area including technical information and relevance to Cyber Security threat(s)
- guiding questions to focus the user on the relevant aspects of Cyber Stability policy debate in this area
- quick-links to related topic briefs
- visualizations (ex. graphs) of key data informing the topic area
- tabbed section for quick access to topic content, organized within the Cyber Stability framework categories (categories TBD)
- (curated) links to reports and other sources of supporting information
- modular organization of content supports rapid and clear communication of complex issues
- consistent presentation/layout of topic briefs makes them comparable and easy to navigate


5. Country Profiles

☰
Sign in



Country Profile:

China



Abstract
 Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

- SIGNATORY TO +
- POLICIES IN PLACE +
- STATED POSITIONS +
- VOTING RECORDS +

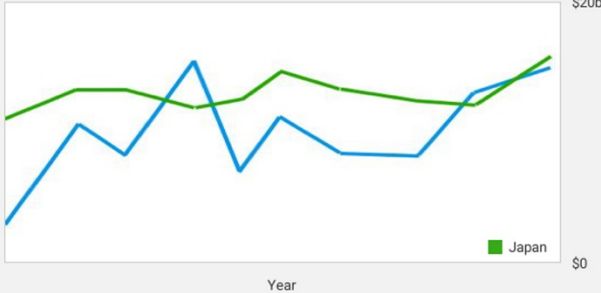
Key Contacts

Xu Yansong
 xyansong@unog.ch
 Tel. +41 (0)22 917 15 83


Xu Yansong
 xyansong@unog.ch
 Tel. +41 (0)22 917 15 83


Details and Analysis


Key Trends CAPACITY EXPENDITURE ▼ compared to JAPAN ▼




China and Cyber Stability



 GOVERNANCE


 SOCIETY


 MILITARY


 CAPACITY

Overview
 Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

 **System Vulnerabilities**
 June 2013

© UNIDIR - 2014
[Contact us](#)

Needs Supported:

“Help me get informed about country activities from a Cyber Stability perspective.”

“Help me identify trends.”

“Help me compare information.”

Functions Delivered: [Get Informed + Make Sense of Information](#)

- organizes and presents national level information according to categories of Cyber Stability activity
- supports comparison of data across states/regions

Site Features:

- summary of country activities and positions from a Cyber Stability perspective
- quick-views to key indicators such as relevant voting records and signatory commitments
- visualizations of key data informing the country profile, including cross-country comparison
- tabbed section for quick access to country information, organized within the Cyber Stability framework categories (categories TBD)
- (curated) links to reports and other sources of supporting information
- modular organization of content supports rapid and clear communication of complex issues
- consistent presentation/layout of topic briefs makes them comparable and easy to navigate

6. Dossier Function

NEW DOSSIER

My OSCE conference dossier

"Most countries around the world today rely on critical infrastructure that is increasingly at risk from a variety of hazards, including attacks via the Internet. We are dependent on broadband and wireless networks for the utility plants that pump water to cities, and the energy grids that provide for industry and individual consumers' needs alike. The security and resilience of these assets, systems, networks, and functions from cyber threats is rapidly increasing. Understanding vulnerabilities of these key national resources to cyber attack, and the destabilizing impacts an attack on them could have, is a crucial part of today's security environment."

Clipped from [Cyber stability and the OSCE](#)

Key Trends CAPACITY EXPENDITURE compared to JAPAN

| Year | Capacity Expenditure (unnamed) | Capacity Expenditure (Japan) |
|------|--------------------------------|------------------------------|
| 2008 | ~\$5b | ~\$10b |
| 2009 | ~\$10b | ~\$12b |
| 2010 | ~\$8b | ~\$11b |
| 2011 | ~\$15b | ~\$10b |
| 2012 | ~\$10b | ~\$12b |
| 2013 | ~\$15b | ~\$15b |

Clipped from [China country profile](#)

© UNIDIR - 2014 [Contact us](#)

Needs Supported

"Help me prepare for my particular tasks or activities."

"Help me to selectively organize information for the things I need to get done."

"Help me to manage large amounts of information productively and make my own connections."

"Help me apply a Cyber Stability lens to my analysis."

Functions Delivered: [Organize for Use](#)

- allows individual users to cross-reference and apply site content in different ways for different tasks
- supports personal, idiosyncratic processes of analysis for formulating, advising and representing policy

Site Features:

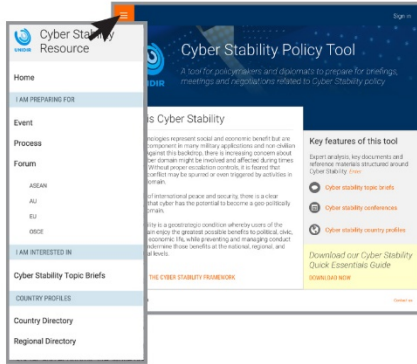
- personal workspace accessed via password log-in
- capability to create personal work folders (dossiers) around professional tasks and activities
- ability to selectively "clip" content from anywhere in the site and save to personal dossiers

Sample User Journey

The following re-presents the key site pages and features as a “user journey” to illustrate the tool through a hypothetical scenario of use. The journey helps bring the elements of the tool to life and convey not only the functions of the tool, but also the experience of using it.

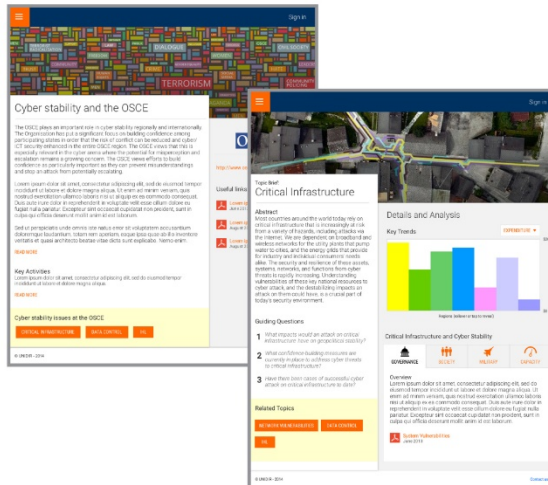
1. Identifies Relevant Information:

Mark, a senior policymaker is preparing for a meeting at the OSCE. Using the navigation, Mark identifies his starting point for inquiry by following the “I am preparing for” section of the menu to link to the OSCE page.



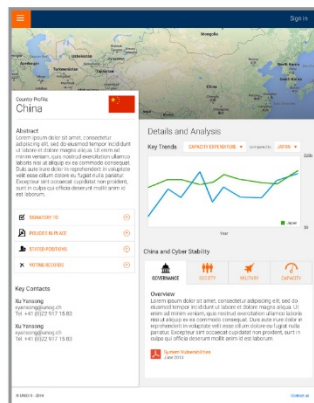
2. Gets Informed:

Mark learns about the cyber stability focus of the OSCE and reviews a recent conference report. From the topic links provided, he identifies “Critical Infrastructure” as a key focus of inquiry for the upcoming meeting he is preparing for. He clicks the link to review the brief.



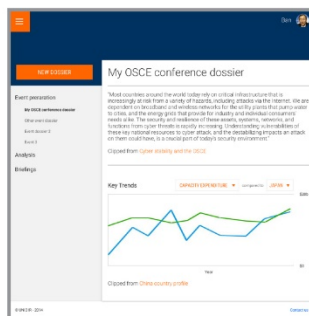
3. Makes Sense:

Having reviewed several topic briefs, Mark has a firm grasp on the key issues informing his upcoming meeting from a cyber stability perspective. He now reviews the country profiles of key states taking part in the meeting, to help him analyze their positions.



4. Organizes for Use:

During his research process, Mark clipped excerpts from the site content that were the most useful to the task at hand. Mark now reviews this aggregated material in his saved dossier, to help him use what he has learned and prepare his position for the meeting.



New Information Resources

Many of the functions proposed for the tool involve the provision of original information resources, designed to achieve something new—the application of a cyber stability lens to preparatory activities of policymakers. Therefore, the visual designs above encompass not only what the user interface would look like, to navigate from point A to B, but also present the first models for how the definition of cyber stability can be mobilized by states and organizations as an analytic category to report on, track, and analyse activities relevant to cyber stability.

These new resources, which feature in the illustrations above, include a **Cyber Stability Framework Document** (to help orient users of the tool), a **Cyber Stability Quick Essentials Guide**, **Forum Pages**, **Topic Briefs**, and a redesign of the **Country Profiles** that originated in the *Cyber Index*.

1. Cyber Stability Framework Document

While clear frameworks have been developed for some approaches (such as cyber maturity and cyber readiness), one does not yet exist for conducting an analysis of cyber stability¹³ that can be used to inform dialogue and decision-making at the regional and international level. This makes it difficult to specify what it means to turn a cyber stability lens to the range of policy discussions and concerns, or to teach others how to apply it.

For cyber stability to be more than mere political aspiration or a symbolic term, a structured framework is needed that is able to direct our attention to certain categories of information and not others, and that can help us to work in a productive manner towards some end. A framework on cyber stability enables us to ask: what are the characteristics and theory behind cyber stability that will allow us to learn from events and make determinations about them so that we can work towards our preferred goals?

Such a framework is a crucial underpinning of the Cyber Stability Policy Tool. Its implicit function is to provide the organizing principles to the site generally. But explicitly, it would serve to: 1) orient the user to the site, 2) provide the categories for the country profiles (as below), and 3) create an explicit basis for a research agenda that can give practical support to cyber stability as a policy agenda.

2. Cyber Stability Quick Essentials Guide

Policymakers cite the need for something like a “Cyber 101”: an introductory resource that could help people new to the cyber stability sphere become sufficiently informed in order to begin to engage effectively.

¹³ Such frameworks are being developed at the national level, however. During the course of this project (2014), the International Security Advisory Board of the US Department of State published its *Report on a Framework for International Cyber Stability*, laying out “existing and potential threats in cyberspace, realities associated with cyberspace that must be taken into account, and the role of deterrence in enhancing cyber stability. The report then offers a number of recommendations for the Department of State to undertake or support” (p. i).

The tool should provide a “quick guide” that gives an overview of the areas (briefly indicating key topics, agreements, historical events, etc.), and linking this to the other resources available in the tool. This provides support to the policymaker who may need additional orientation and context, and can help those completely new to the cyber stability sphere determine where to begin.

3. Forum Pages

Profile pages for regional international forums and organizations help to bring regional and international developments and perspectives into view. Given the fact that much of the current dynamism in policymaking is taking place in the context of regional organizations, such as the Organization for Security and Co-operation in Europe (OSCE) or the Association of Southeast Asian Nations (ASEAN) Regional Forum, understanding both the organizational mandate and approach, and how they apply to cyber issues, is highly useful. Additionally, given that many regional organizations have processes that may not be specifically focused on cyber-related issues, understanding positions and structure of cyber-issue engagement within these organizations is of importance to government actors representing at the respective regional organizations, national level actors looking to create national policy, and those working on international peace and security issues at the global level.

4. Topic Briefs

Topic Briefs are a quick-access resource providing brief context and background. As explicit applications of a cyber stability lens, produced by experts in the field, they help to inform users about key topics relevant to discussions of cyber stability. The briefs can be updated as needed, and linked to other relevant information resources on the site, or to a set of curated external links, facilitating the practical navigation of information. In addition, briefs are accompanied with guiding questions to help users learn how to apply a cyber stability lens to a range of issues and topics. The briefs themselves represent an evolving resource that can make use of an evolving network.

5. Country Profiles

Policymakers are clear in their need for state-level information that can help them to assess threats and risks in the cyber sphere in order to make informed and well-considered decisions. It is therefore crucial that information of this nature be included in the tool.

UNIDIR’s original *Cyber Index* responded to this need by creating a study using open-source information to illustrate state-level cyber capacity, development, and orientation in both the civilian and military domains.

This was regarded as a valuable contribution by many policy actors—despite the known problems and risks of reliability associated with open-source reporting on military capabilities and developments—since it put information at their fingertips that was crucial to their tasks. Recognizing this need, a number of other organizations and

entities (both in the public and private sectors) have also developed resources to make different kinds of information about state-level cyber capabilities available.¹⁴

However, given the particular needs of policymakers, information at the state level will be even more useful when it is:

- Both *current* (updated on a regular basis) and *archived* (information from the past is still available): Policymakers need both the most current information available, but they sometimes also need to evaluate developments over time.
- *Comparable*: Comparative analysis is a key building block in the development of the situational intelligence that is central to policy work. Information that facilitates comparison (for example, across states, over time, and across issues) is of value.
- *Consistent*: In order to be reliably comparable, information needs to be produced according to analytic categories that are consistently and transparently operationalized. Further, consistent categories help the reader develop a more rapid overview of their focal concern.

Given these particular needs, we developed a model for a digital Country Profile page that provides these features. Country Profiles should be a quick-access resource. They should be organized according to the key categories of a cyber stability framework, give a real-time (or close to real-time) snapshot of state-level capabilities or developments in these key domains, give information about useful areas of state-level activity (like United Nations voting records), facilitate trend analysis, and be comparable.

There is no easy solution for managing the risks and challenges that derive from working with open-source information about sensitive topics that has not been verified through formal method. However, the risk can be managed and progress be made through two techniques. First, information collection and presentation can be systematized in cyber profiles through consistent and comparative categories thereby creating a new level of transparency through comparative data. Second, efforts can be made (through the establishment of criteria, coding mechanisms, and other techniques) to differentiate verified and unverified information thereby flagging areas of concern for policymakers so that the information can be used judiciously. An added benefit is that the use of such coding systems across the newly comparable cyber profiles will result in very clear maps showing who and what is transparent in a variety of critical areas allowing for decisions to be made on how to improve the state of affairs.

¹⁴ Examples include, among others, the Global Cyber Security Index (International Telecommunication Union), the National Cyber Security Strategies publication (European Network and Information Security Agency), the Cyber Maturity in South East Asia report (Australian Strategic Policy Institute), the Cyber Readiness Index (Harvard University), the Cyber Power Index (The Economist Magazine Intelligence Unit and Booz Allen Hamilton), and the Global Cyber Risk Assessment Index (Alvarez and Marsal Management Consulting Firm). Each of these resources provides information for different target audiences, towards different ends, and using different methods, techniques, and data.

Summary: Added Value of the Tool

These illustrations help demonstrate how a tool developed in this way can facilitate the application of a cyber stability framework to policy practices at four key junctures (identifying task-relevant information, locating information, analysing information, and organizing it for use).

In being animated by a cyber stability framework from the first instance, the tool serves several purposes, including:

- helping users to develop a clearer picture of cyber stability as a set of conditions to work towards,
- teaching users what key aspects of decision-making and public life to pay attention to in order to advance towards that goal, and
- providing a common basis (which can be developed over time) from which to engage these activities and goals.

Supporting individuals in these ways would make a direct contribution to improving the capacity of policy actors working in the cyber domain. In addition, this sort of tool adds value in several other ways.

- It can help users to identify and prioritize information relevant to their tasks.
- It can provide the first real orientation to a cyber stability approach and help users apply this in their analysis and policy activities.
- It can serve a wide range of users and needs, from the expert who needs quick information at their fingertips, to the novice who needs guidance on what to know and to ask when applying a cyber stability perspective.
- It can help users to make the best use of existing information resources, rather than just contribute to the ever-growing supply of information and data that must be digested.

6. Next Steps

There are several stages involved in progressing from an initial prototype to a digital tool. While the level of development in each stage can be scoped according to resources, each stage must be conducted in order to produce a digital tool. Further, the sophistication of the resulting tool will be a reflection the degree of development engaged.

1. Validate and refine the tool concept

“Test” the proposed prototype and design direction for the tool (as presented in this document) with users to validate (or adapt) our conclusions about functions and our propositions for how the tool can address them, and refine and develop the concept further, based on test findings.

2. Conduct the technical, content, and design development process

Including:

- site map development;
- design of navigation;
- design of interactive elements design;
- design of key template pages;
- development of key content areas (including but not limited to the Cyber Stability Framework, Country Profiles, Topic Briefs, Forum Pages, and the Quick Guide for users);
- technical programming;
- content development and testing;
- preliminary prototype testing; and
- finalization of design direction.

This stage results in the initial assembly of all the tool functions together, into a complete tool design with ready templates and structures for adding context.

3. Conduct user testing and refinement

Test the usability of the tool prototype in the target user group to determine whether the tool can be used in the ways intended and will produce the experience and results intended, and to identify crucial design problems and gaps before moving into production. Findings from this test cycle will be used to adapt, correct, and otherwise refine the tool.

4. Produce beta version

Produce the technical and content elements of the tool. This stage involves the programming required to create a functioning website ready for beta testing.

5. Conduct beta testing

Conduct the final test stage, involving limited release of the tool to a sample of the target user group, in order to allow for technical troubleshooting and adjustments if needed.

6. Launch

Make the tool “live” for online use, including debugging and refinement of interface design, and conduct a formal launch event of the tool.

In addition to these practical steps, UNIDIR plans to carry out further intellectual refinement of the concept of cyber stability that can be effectively operationalized for tool categories. The definition provided here gives a point of orientation for the practical use of the new tool. However, there is a wider challenge worth engaging to build a widely accepted definition—whether this one or another—throughout the policymaking community for the benefit of cooperative action.

UNIDIR initially suggests a meeting of a group of policy experts to begin a professional discussion of cyber stability that would later evolve into a process-oriented approach towards creating a shared international concept.

In a similar vein, it is also crucial that the international cyber community be introduced to the value of the new tool in order to facilitate its use and acceptance within personal and organizational practice. We therefore also propose creating an awareness-raising and capacity-building component to future work that assists stakeholders (donors, potential users, etc.) and others whose political support will be needed at the organizational and administrative levels to bring the tool to fruition and better ensure its application and uptake.

7. Conclusions

The task given to this project team was to develop the foundations for a digital tool to support policymakers working on matters of international peace and security in the cyber domain. A common response to this kind of call is to focus on addressing users' information needs with different kinds of information products (journals, reports, databases, etc.). However, we believe that the increase in the volume of information policymakers have access to has paradoxically made using information harder; it is more difficult to know what is relevant, what is authoritative, what is valid, what is appropriate, and how any of it can be used to improve job performance aside from "staying informed".

Guided by both the EBD approach and findings from research within this project, UNIDIR has instead focused on understanding the concrete needs of policymakers, and has created a response that addresses the ways in which they use information to do their jobs—not just how they get it. In this, we have not only moved away from a study to an online resource, but from an information resource to a policy design tool.

This represents both a new way of using technology to support the work of policymakers, as well as a specific effort to explicitly support the appropriate and effective use of information in policy design.

UNIDIR's decision to move from a research publication to a policy tool is a substantive move that fundamentally directs attention away from the analysts' views of what people should know, to a user-driven perspective that is oriented towards helping the users of information achieve greater performance in their own duties and objectives in the context of daily work.

In this way, this framework for a Cyber Stability Policy Tool addresses and provides a solution to a key problem: namely, that information is too often being "pushed" at decision-makers, rather than creating conditions for it to be "pulled" into their work as a better means of achieving it. The value, in other words, is in making information (and evidence) an asset in the crafting of real-world solutions to real-world problems.

The development of a tool—based on an analytically sound model—to make information useful for advancing international cooperative action, is not an advocacy activity but a design activity. Stakeholders to the process will benefit from a new recognition of possibilities created by new dynamics among expert design methods, evidence-based approaches to design, political cooperation, and the need to focus on user experience to anchor utilitarian solutions.

In being impact-driven, user-oriented, and practice-based, the Evidence-Based Design process we applied to develop this tool provided a new basis from which to understand the impact goals for cyber stability policy, the challenges that policymakers face in identifying and mobilizing information for use in advancing cyber stability, and the daily practices they engage in to use information in the absence of specific tools to support it.

The Cyber Stability Policy Tool is more than a sum of its parts. It results in a user experience that is holistically responsive to user needs. It holds promise—if developed, tested, and employed—to not only serve the specific need of building user competence in attending to cyber stability, but could in fact be a new model for empowering a wider community of key policy actors to effectively participate in policy discourse in new, fast moving and highly complex subject matter areas.

We believe that this tool could represent a new and effective method of policy support. In the cyber context, given the pace of change and the proliferation of processes and capabilities, we consider that this tool can make a small, but vital, contribution in achieve greater international understanding of cyber stability issues, and by supporting more considered and informed policymaking can assist in working towards improved security and stability in the cyber domain.



UNIDIR

Towards Cyber Stability
A User-Centred Tool for Policymakers

Lisa Rudnick and Derek B. Miller
with Leeor Levy