GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

www.cyberstability.org | info@cyberstability.org | cyber@hcss.nl | @theGCSC

REQUEST FOR PROPOSALS
RESEARCH ADVISORY GROUP

CONTRACTING AUTHORITY

***The Hague* Centre for Strategic Studies** on behalf of the Secretariat of the Global Commission on the Stability of Cyberspace (GCSC).

DEADLINE

Deadline for the submission of proposals is set at **19/01/2018 at 17:00 (local time The Hague).**

DELIVERABLE PRODUCTS

In this request for proposals, the Global Commission on the Stability of Cyberspace will commission four research projects. The deliverable product is a report that upholds to the standards of an academic journal to inform the deliberations of the Commission Meeting in May 2018. The researchers will be invited to present their work to the Commission at this meeting.

There are three kinds of reports in this request for proposals:

- A *briefing* is a facts-only summary of a particular topic. It functions as an overview and is limited in its own analytical contribution. It is around 5.000 words of length.
- A *memo* is a thought piece that is strong on the analytical side and openly normative in approach. It is around 5.000 words of length.
- A *working paper* is based on original research project and ideally combines elements of both a briefing and a memo. It is between 10.000 and 20.000 words of length.

REQUEST FOR PROPOSALS

1. **Adaptations to Enhance the Stability of Cyberspace**
2. **Impact of Technological Developments**
3. **Beyond the UN GGE**
4. **Defining Offensive Cyber Capabilities**

In addition to any commissioned research, unsolicited/unfunded submissions will also be accepted for review by the Research Advisory Group on behalf of the Commissioners.

TABLE OF CONTENTS

CONTRACTING AUTHORITY 1
DEADLINE 1
DELIVERABLE PRODUCTS 1
REQUEST FOR PROPOSALS 1

TABLE OF CONTENTS 2

1. REQUEST FOR PROPOSALS 3

2. GUIDELINES FOR GRANT APPLICANTS 12

2.1. SUBMISSION OF THE PROPOSAL 12
2.2. TIMELINE 12
2.3. COMPENSATION 12
2.4. INTELLECTUAL PROPERTY AND PUBLICATION 12
2.5. ABOUT THE GCSC AND THE RESEARCH ADVISORY GROUP 13
2.5.1. **INTERNATIONAL PEACE AND SECURITY OF CYBERSPACE (RAG-P):** RAG-P@CYBERSTABILITY.ORG 13
2.5.2. **INTERNET GOVERNANCE (RAG-I):** RAG-I@CYBERSTABILITY.ORG 13
2.5.3. **LAW (RAG-L):** RAG-L@CYBERSTABILITY.ORG 14
2.5.4. **TECHNICAL AND INFORMATION SECURITY (RAG-T):** RAG-T@CYBERSTABILITY.ORG 14

ANNEX: PROPOSAL TEMPLATE 15

1. REQUEST FOR PROPOSALS

Working Title:	**1. Adaptations to Enhance the Stability of Cyberspace**
Primary Lead:[1]	Internet Governance (RAG-I)
Secondary Support:[2]	Technical and Information Security Practice / Law / International Peace and Security
Deliverable Product(s):	"Working Paper"[3] (i.e.15.000 word in-depth study) with normative proposals
Period of Performance:	5 months
Target Start Date:	February 2018
Funding:	€5000

Key Research Question:
What technical and policy adaptations could be reasonably applied to the "Public Core" of the Internet to enhance its stability and security?

Scoping Questions:

1. What are currently known examples of threats to possible "Public Core" infrastructure and services? What are the historical case studies, and hypothetical threat scenarios?
2. What are the current protective measures, both implicit and explicit, that apply to the "public core" of the Internet? To what extent does this apply to identifiable infrastructures (such as the root zone), core protocols and their development (such as DNSSEC, BGPSEC, etc.), and the security of physical hardware and installations?
3. What are the current shortfalls in those protective measures, both in technical and policy terms? How could higher technical Internet security standards negatively impact geopolitical and/or economic stability, or significantly threaten the data protection or human rights of the individual? Which potential measures (either already existing, proposed, or proposed here for the first time) could best ensure the continued stability and security of the global Internet under different adverse scenarios, including the importance of human rights in cyberspace, and taking into account different security and political concerns of states?
4. What is the state of the discussions regarding possible new measures in different state and non-state fora? What prospects exist of interpreting existing international law, formulating new law (and treaties), or otherwise encouraging actors to abstain from harmful conduct towards the Public Core? What are the implications of these new measures, both in policy terms (multi-stakeholder vs intergovernmental approach) and within the human rights discussions?
5. Looking ahead, what are the most salient developments that will impact the near future (5-15 years) of the Internet? What hypothetical adaptions to the Public Core and other critical information infrastructures could become necessary to ensure the security and stability of the Internet as a whole?

Explanatory Discussion:
This research project is intended to build on the findings the previously commissioned research on the wider question of the "Public Core" as well as introduce additional elements of its own foundational research. It will be based on a fulsome understanding of the critical Internet infrastructures (policy, logical, hardware, or other interpretations), the associated risks (malicious, and non-malicious), the vulnerabilities, proposed and existing measures in state and non-state bodies including the existing community and industry response mechanisms, such as the root zone rollover procedures, routing norms or similar, the long-term standard technical standards setting role, and the prospect of future technological change as well as the political reality and expressed state

[1] The Primary Lead refers to the key subject matter of the Request for Proposal, and the cluster of the Research Advisory Group. Researchers and institutions
with expertise relevant to this cluster are advised to respond to the Request for Proposal.
[2] The Secondary Support refers to the supporting cluster(s) of the Research Advisory Group.
[3] A *working paper* is based on original research project and ideally combines elements of both a briefing and a memo. It is between 10.000 and 20.000 words of length.

interests. Further, it will use examples of past breaches of the Public Core as well as propose hypothetical threat scenarios, while using their own interpretation of exactly what assets and services are considered part of the Public Core (for an indication please see the GCSC Call to Protect the Public Core of the Internet.

Successful proposals shall above all concentrate on the effects on the end-user (data protection and human rights concerns), economic benefits, and lastly the security concerns of states. The proposal will ideally already outline if the intended outcome will be an institutional innovation (new framework or institution), institutional evolution (building on existing initiatives), or a principles-based document that lays out specific recommendations and action points. The proposal should be clear from the outset who the principle audience(s) for the recommendations would be, and therefore where it should be applied or implemented. Finally, special considerations will be given to proposals that show a keen understanding of intergovernmental and/or multi-stakeholder processes, and that can facilitate an easy translation of the papers technical and policy recommendations into the appropriate format (e.g. governmental non-paper, or RFC).

Recommended Methodology:
Unlike other RFPs, this RFP goes beyond the scope of the smaller projects (memos or briefings) and requests a more in-depth treatment of the subject. Successful proposals for commissioned research on this project could adopt a range of methodologies, including but not limited to:

a. historical analysis of prior Internet governance debates and their relationship to interstate conflicts; as well past and potentially future threats to the Public Core;
b. critical analysis of existing or proposed technical and policy practices (root zone procedures, register and registrar practices, routing frameworks, laws and treaties pertaining to communication infrastructures, etc.) and which have the largest impact on the Public Core;
c. original proposals for new normative policy measures supported by a technical discussion of Internet architectures; etc.

Researchers would be expected to conduct interviews with relevant experts, conduct original research, study the findings of other GCSC research, apply social science research methodologies, and put forward novel policy recommendations supported by detailed reasoning.

Intended Researchers:
This request for proposals (RFP) will be open to all researchers from NGOs, academia, and industry. In addition to any commissioned research, unsolicited/unfunded submissions will also be accepted for review by the Research Advisory Group on behalf of – and for further distribution to – the Commissioners. All products delivered pursuant to this RFP must principally address the Key Research Question as elaborated by the Explanatory Discussion above. Proposals for funded research should also identify how each of the Scoping Questions will be explicitly covered by the proposed research.

Reference Documents:
GCSC Call to Protect the Public Core of the Internet, GCSC Memos and Briefings from the Research Advisory Group on the Public Core of the Internet (to be published in the beginning of January 2018), Cyber ”scenarios” reports by the Atlantic Council, US National Intelligence Council (i.e. Global Trends reports), Australian Office of Net Assessments, and other institutions.

Working Title:	**2. Impact of Technological Developments**
Primary Lead: [4]	Technical and Information Security Practice (RAG-T)
Secondary Support: [5]	International Peace and Security (RAG-P)
Deliverable:	"Briefing"[6] (i.e. 5.000 word report): analysis of emerging technologies
Period of Performance:	3 months
Target Start Date:	February 2018
Funding:	€3000

Key Research Question:
What are the anticipated implications of technological developments – especially the Internet of Things (IoT) and artificial intelligence (AI) – in the near future on international security as it pertains to cyber stability?

Scoping Questions:
1. How is the move to "hardened" Internet protocols such as DNSSEC, BGPSec, and IPv6 progressing? What other emerging issues are there in regard to core Internet protocols and infrastructure?
2. How is IoT being implemented and what are the main security concerns and solutions for its adoption? Are common standards and principles being established for IoT in the public Internet?
3. How will other ascendant technologies such as AI, quantum computing, quantum encryption, blockchain, etc. potentially impact the security and stability of the Internet? What are the trade-offs between functionality and security for each of those technologies?
4. What are other areas where future technological development could have an impact of the same magnitude, and why?
5. What are the geo-political implications of adopting those new technologies? Will they make military and intelligence operation in cyberspace, and offensive cyber activity in general, more or less effective?

Explanatory Discussion:
The incorporation of emerging technologies into global ICT networks will likely have broad implications for science, commerce, and government. This project is intended to identify and assess those technologies for how they will effect (a) the stability and vulnerability of critical infrastructures, and (b) the conduct of future hostilities. Will they make it easier or more difficult to conduct malicious activity in cyberspace? Will they mitigate or exacerbate the potential uncertainty and volatility associated with international relations? Conversely, what are the areas where future technological developments are likely to have the largest impact on overall security in cyberspace, and why?

Recommended Methodology:
Successful proposals will have two main components:
1. A literature review of technology R&D that specifically includes assessments of the points raised in 1-3 above, including subchapters on the specific technology in question. An overall temporal timeframe (e.g. by the year 2025, or 2030, as chosen by the authors) should be applied and streamlined throughout.
2. An analysis of the political, military, law enforcement and intelligence implications of adopting those and other new ICT, calibrated to a specific common date scenario (or multiple scenarios, as appropriate).

"Future technology" should include newly invented technologies as well as those existing technologies that are not being fully implemented yet. Discussion of industry and governmental positions on the adoption of specific technologies may also be helpful.

Intended Researchers:
This request for proposals will be open to all researchers from international institutions, NGOs, academia, and industry. Successful applicants will be able to show that they have the ability to conduct both the literature

[4] The Primary Lead refers to the key subject matter of the Request for Proposal, and the cluster of the Research Advisory Group. Researchers and institutions with expertise relevant to this cluster are advised to respond to the Request for Proposal.
[5] The Secondary Support refers to the supporting cluster(s) of the Research Advisory Group.
[6] A *briefing* is a facts-only summary of a particular topic. It functions as an overview and is limited in its own analytical contribution.

review and to perform critical analysis of the ICT from a technical perspective. In addition to any commissioned research, unsolicited/unfunded submissions will also be accepted for review by the Research Advisory Group on behalf of the Commissioners.

Reference Documents:
McKinsey, World Economic Forum, Gartner, and several think tanks have all done prior technology studies and trend analysis reports.

Working Title:	**3. Beyond the UN GGE**
Primary Lead: [7]	International Peace and Security (RAG-P)
Secondary Support: [8]	Law (RAG-L), Technical and Information Security Practice (RAG-T)
Deliverable:	"Memo"[9] (i.e. 5,000 word report): normative recommendations for military, diplomatic, legal, and public policy measures
Period of Performance:	3 months
Target Start Date:	February 2018
Funding:	€3000

Key Research Question:
What other discussion formats could be explored to continue, widen, and deepen the work of the UN Group of Governmental Experts (UN GGE)?

Scoping Questions:

1. How can the work of the UN GGE best be continued, either expanded upon or reconfigured, in a way best suited to address the international peace and security (IPS) concerns of states? How should the future work on norms and CBMs, but also on capacity building and countering cybercrime, inter alia, be continued?
2. What are implications for the various mandates implied? What are the lessons learned (and the common criticisms) of the UN GGE process? What further options are there for continuing the dialogue initiated by the UN GGE outside of the UN First Committee (e.g. standing open Committee like the Human Rights Committee, Internet Ombudsman, etc.), or indeed outside of the UN? What are the known proposals (i.e. Code of Conduct, Geneva Convention, etc.) and their common pros and cons?
3. Are there new proposals that could be considered? What are the historical precedents from a security point of view (e.g. Helsinki Process, early Test Ban Treaty talks, etc.) but also from outside of security, for instance ecological or trade talks (e.g. Rio Earth Summit talks, GATT, etc.)?
4. What is the role of non-governmental organizations and the private sector in this new IPS process? Specifically, how could the Global Commission on the Stability of Cyberspace contribute to that process?

Explanatory Discussion:
In 2017, the latest UN GGE was unable to build on the success of the two previous reports, and reach a consensus on core issues – on the application of international law to cyberspace or how to achieve further progress towards implementing the previously stated norms. The future of these intergovernmental discussions is now uncertain, and new ideas are needed.

Overall, ideas to continue the UN GGE work fall into four categories:

1. inside process evolution, with a similar body set up within the UN (like the Human Rights Committee, or the UNSG Commission, etc.) or even in a similar body (such as the ITU);
2. outside institutional innovation, with a new international organization created with an uncertain but presumably massively extended mandate (e.g. "IAEA for cyber");
3. inside process innovation, with structured dialogues between various actors playing the lead (e.g. "FATF for Cyber", "IAEA for cyber", "Helsinki Process for Cyber");
4. Outside process evolution, with new ideas and formats (such as Code of Conduct, or Geneva Convention, etc.) effectively introducing an entirely new treaties or agreements between stakeholders outside of the existing IPS system.

This Request for Proposals (RFP) invites definitive analysis of the present landscape, as well making authoritative assessments of the various proposals and advocating novel concepts.

[7] The Primary Lead refers to the key subject matter of the Request for Proposal, and the cluster of the Research Advisory Group. Researchers and institutions with expertise relevant to this cluster are advised to respond to the Request for Proposal.
[8] The Secondary Support refers to the supporting cluster(s) of the Research Advisory Group.
[9] A *memo* is a thought piece that is strong on the analytical side and openly normative in approach

Recommended Methodology:
The RFP is intended to elicit original, normative suggestions as well as critique the feasibility of existing recommendations. Such prescriptive recommendations, however, should go well beyond the purely theoretical to illustrate specific paths to fruition as well as the basis for political support. Accordingly, successful proposals will not only incorporate a survey of the options already under consideration but also novel research on applying measures that have been successfully utilized in other instances (i.e. analogous case studies from arms control, trade, environment protection, etc.) to the cyber realm. When examining what alternatives exist to the currently defunct UN first committee process, the authors should provide examples from both within the UN as well as other multilateral discussion formats, and provide hypothetical solutions based on the historic record.

Intended Researchers:
This RFP will be open to all researchers from international institutions, NGOs, academia, and industry. Successful applicants will be able to show that thy have a strong knowledge of international law, international institutions, military doctrine, and/or public policy at the national government level in order to competently develop practical methodologies for actually incorporating the GGE principles into state practice. In addition to any commissioned research, unsolicited/unfunded submissions will also be accepted for review by the Research Advisory Group on behalf of the Commissioners.

Reference Documents:
The UN GGE reports from 2013 and 2015. OSCE permanent council decisions 1106 (December 2013) and 1202 (March 2016) on cyber confidence building measures (CBMs), the G20 statement against economic cyber espionage, and research previously done by Alex Grigsby on norms and CBMs for this Global Commission, as well as the UNIDIR report by Camino Kavanagh.

Working Title:	**4. Defining Offensive Cyber Capabilities**
Primary Lead: [10]	Law (RAG-L)
Secondary Support: [11]	International Peace and Security (RAG-P), Technical and Information Security Practice (RAG-T)
Deliverables:	"Memo"[12] (i.e. 5,000 word report): analysis of a survey of existing government and industry views plus any new normative proposals
Period of Performance:	3 months
Target Start Date:	February 2018
Funding:	€3000

Key Research Question:
To what extent is it possible to define and categorize offensive cyber capabilities, identify entities to be protected from attack, and/or determine "cyber weapons"?

Scoping Questions:

1. What are the existing implicit and explicit definitions of offensive cyber capabilities in governmental and academic literature? Do these definitions lend themselves to segmentation of different levels of disruption/attack? What are the potential "use cases" and scenarios (e.g. within "battlefield cyber", "strategic strike", "strategic influencing" etc.) for offensive cyber capabilities? How do they reflect or develop on classic information security properties (like the ISO2700x and C-I-A triad)?
2. To what extent is it possible to define a "cyber weapon"? What role does the question of "data as an object" play in these deliberations? What examples are there from arms control history, including in particular the NPT, MTCR, BWC and similar attempts to deal with "dual use" technology? How would such a definition work with the nature of offensive tool sets (such as Metasploit) that are developed for legitimate purposes, and the free availability of which is considered an article of faith?
3. Should there be restrictions on offensive technologies that non-state bodies (e.g. defense contractors, researchers, etc.) are permitted to develop, possess, or use in their work such that these entities could not be used as proxies by state actors for the conduct of offensive cyber operations? Would it be practically feasible to implement restrictions on the development and/or use of cyber weapons? What would technical enforcement and verification of such a regime look like? Are there models of regulation that do not rely on enforcement and verification that could be applied?
4. What targets and/or effects of offensive cyber operations should be prohibited by the international community? What models have already been proposed on such "Internet safe zones", what are there perceived benefits and costs? Should those limitations vary between peacetime and armed conflict?
5. What are the relevant international law standards for attributing non-state actors' cyber activities to states, and what is the burden of proof? In particular, when would a state be in "effective control" over a non-state actor for the purposes of state responsibility? What level of due diligence should states exercise vis-à-vis non-state actors operating from their territory that have the potential to engage in offensive cyber operations? Would a state's unwillingness to accept foreign assistance, or to cooperate with transnational law enforcement investigations, constitute a breach of due diligence?

Explanatory Discussion:
First, the normative debate regarding cyber weapons and information operations has focused on the permissible targets and/or effects of cyber activity, and this request for proposals is intended to focus on that approach. There are therefore three potential approaches that proposals could take that are encapsulated in the initial question – focusing on the question of identifying *means* (i.e. identifying "cyber weapons"), focusing on the question of controlling *effects* (i.e. analyzing the question of protected zones), or a combination of the above or emphasis on *methods*. While all proposals will be entertained, particular value will be placed on those

[10] The Primary Lead refers to the key subject matter of the Request for Proposal, and the cluster of the Research Advisory Group. Researchers and institutions with expertise relevant to this cluster are advised to respond to the Request for Proposal.
[11] The Secondary Support refers to the supporting cluster(s) of the Research Advisory Group.
[12] A *memo* is a thought piece that is strong on the analytical side and openly normative in approach

proposals that compare and contrast the practical (political / technical) restraints of each of the above approaches, and attempt to propose workable solutions to the known challenges.

Questions that could be examined include: What types of entities are such vital infrastructures that they should be protected from all kinds of hostile cyber effects? What kinds of cyber effects, including both intended and collateral, should be proscribed? To a lesser degree, some attention has also been given to restricting the means themselves. Are there certain aspects of cyber conflict that should be considered akin to poison gas, "booby traps" (mines), or biological agents? This becomes especially relevant when states wish to find a basis to engage on arms control discussions on the subject, which make it key that the effects and capabilities are given a common definition. At the same time, a valid point has been made that the arms control approach in cyber may be futile, and instead efforts to constrain effects should be maximized. This project will therefore look holistically at targets, effects, weapons, and counter-proliferation efforts. The project will also look at potential restraints on offensive cyber operations that would be most likely to limit unintended consequences of cyber operations.

As a corollary, the international community has noted that many adverse cyber activities are conducted by non-state actors (e.g. corporate contractors, criminals, hacktivists, etc.) whose operations are often instigated, encouraged, and/or condoned by national authorities. The legal question of the standards of attribution is critical for unmasking proxy actors and imputing their actions to sovereign governments. Of the attribution standards, that of "effective control" has been examined in depth. Other standards, however, have received less attention. This project aims at building a more robust understanding of all the international law standards for attributing non-state actors' cyber activities to states. Related considerations include the technical evidentiary requirements for establishing attribution; calls for a multi-stakeholder "cyber attribution council"; the conduct expected of a "diligent state" in situations in which the non-state actors' cyber activities are not attributable to the territorial state as a matter of law; and the potential impact of increased domestic monitoring – that may be needed to comply with state responsibility and due diligence requirements – on human rights.

Recommended Methodology:
Successful proposals for commissioned research on this project will include:

1. a literature review of existing government, NGO, and industry views that have been published on these topics, and;
2. an original analysis of the strategic, legal, and technical implications that argue in favor of or against trying to implement any such restrictions.

The literature review will survey different approaches to defining and classifying "cyber weapons", "cyber operations", and "cyber effects" to discuss the relative advantages and disadvantages of proposed limitations. It may also consider what constitute "defensive" versus "offensive" cyber actions in terms of "active response", "hack back", or countermeasures. The purpose would be to identify existing frameworks and then provide critical analysis that builds upon those taxonomies. The majority of this Memo should, however, explore the desirability and identifying workable proposals to proposing whether the international peace and security discussion should focus on regulating "means", proscribing "effects" or a combination of the two.

Intended Researchers:
This request for proposals (RFP) will be open to all researchers from international institutions, NGOs, academia, and industry. Successful applicants will be able to show that they have the ability to conduct both the literature review and to perform critical analysis of proposed limitations from strategic, legal, and/or technical perspectives. Applicants should also show that they have experience in, or aptitude for, understanding the procedures of international institutions and the application of international law. A law degree or professional certification is not required but would certainly prove useful in conducting this research. Alternatively, professional military experience with rules of engagement and the laws of armed conflict would also prove useful. In addition to any commissioned research, unsolicited/unfunded submissions will also be accepted for review by the Research Advisory Group on behalf of the Commissioners. Position papers from government organizations will also be accepted on an unfunded basis.

Reference Documents:
UN GGE reports, SCO Code of Conduct, Wassenaar Arrangement, recent national cyber strategies with discussions of offensive doctrines (e.g. France and Australia), and normative proposals by Microsoft, Carnegie Endowment for International Peace, and other non-governmental organizations. Cyber related legal analysis can be found in the Tallinn Manual 2.0, and further academic commentary can also be found in the CCD COE's published volume from CyCon in June 2017. See also, Kubo Macak, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors", Journal of Conflict & Security Law, Vol. 21 No. 3, 405–428 (2016).

Non-cyber-related case law can be found in the decisions of the International Court of Justice (e.g. the Nicaragua case), the International Criminal Court, and other ad hoc tribunals like the International Criminal Tribunal for the former Yugoslavia (e.g. the Tadic case).

Further, attention should be made to other strategic arms control discussions, including the Biological Weapons Convention, the Non-Proliferation Treaty, the Missile Technology Control Regime and other attempts to define "weapons"; offensive capabilities, and limit their spread and employment. Attention should be paid to those documents that try to segment and define cyber capabilities (such as the Air Force Science Advisory Board report etc).

2. GUIDELINES FOR GRANT APPLICANTS

2.1. SUBMISSION OF THE PROPOSAL

Legal entities that are a member of the Research Advisory Group can respond to these RFPs with proposals. The subscription procedure for the Research Advisory Group is explained here.

Proposals should be submitted as a single Word file with the following information:

1. Proposal (see the Annex for the proposal template): institutions can respond to only one or all lots. Each lot requires a separate proposal.
2. Supporting Documents (see the Annex on what constitutes a Supporting Document)

Proposers will be evaluated by the Chairs of the Research Advisory Group, the Secretariat and the Commissioners. Evaluations are based upon the content of the submitted proposal and further evaluated on the basis of the applicant's experience in the subject area, understanding of the work, and prior relevant publications.

There is no limitation on the number of proposals each party is allowed to submit. Therefore the same party can submit proposals on all RFPs if desired. Each proposal will be considered on its own merits.

Proposals should be submitted electronically to cyber@hcss.nl by 17:00 (local time The Hague) on **19/01/2018** entitled: "Proposal: GCSC Research Lot X [specify the lot number and title]".

2.2. TIMELINE

22 December 2017	The Secretariat publishes the Request for Proposals (RFP)
19 January 2018	Deadline submission proposals
1 February 2018	The applicants awarded with the grants are informed by the Secretariat. Start date of the of the research projects.
19 February 2018	Submission of detailed chapter outline
2 March 2017	Feedback from the Secretariat and Research Advisory Group Chairs
4 May 2018	Submission of final report

This timeline refers to the *briefings* and *memos*. The timeline for the *working paper* will be subject to special rules.

2.3. COMPENSATION

The grant for each research project is specified for each Request for Proposal (RFP). Applicants will not be compensated for the writing of a proposal.

2.4. INTELLECTUAL PROPERTY AND PUBLICATION

For all the resulting reports, the ***intellectual property rights*** remain with the author(s) of the work. Citations of the report referring to the GCSC is only allowed if agreed upon by the Commission. This means that the author(s) are free to use the work otherwise, i.e. publish the report if they wish to do so. However, only if the Commission agrees to explicitly endorse the final report, will the reference to the "Global Commission on the Stability of Cyberspace" (GCSC) be permitted.

The reports can be made available on www.cyberstability.org as briefing material from the Research Advisory Group for additional feedback. The Commissioners may also decide to consider using the report as a basis for a non-paper, RFC, or similar official report. In that case, the report can be converted into an actionable document for governments or other stakeholders by the Secretariat (in conjunction with the original author(s)). The original authors will be given full credit in the final report.

2.5. ABOUT THE GCSC AND THE RESEARCH ADVISORY GROUP

The Global Commission on the Stability of Cyberspace (GCSC) develops proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace. The GCSC engages the full range of stakeholders to develop shared understandings and its work will advance cyber stability by (i) supporting information exchange and capacity building, (ii) research, and (iii) advocacy.

In the margins of the GCCS2017 in New Delhi, the GCSC released a Call to Protect the Public Core of the Internet by all Internet stakeholders to safeguard the general availability and integrity of the Internet. The commissioned research briefings and memos for Project 1 on the Public Core informed the deliberations of the GCSC Meeting in New Delhi and will be published in the beginning of January 2018. The experts of the Research Advisory Group that executed the commissioned research were invited to present their findings to the Commission in New Delhi.

The deciding element of the GCSC are the Commissioners, distinguished individuals who have worked on different aspects of the security and stability of cyberspace. The Commission is a self-nominated volunteer body that sets its own agenda and work schedule. The Commission is supported by a Secretariat – led by The Hague Centre of Strategic Studies (which started the initiative with support of the Ministry of Foreign Affairs of the Netherlands, ISOC and Microsoft) and the EastWest Institute. Key financial supporters are included in the Management Board, which, however, does not have an agenda setting function. More information about the Commission, its mission and members is available on https://cyberstability.org.

The Research Advisory Group (RAG) fulfills a critical research and execution element of the Commission. It functions as the Commission's academic backbone and links the latter to the wider research community. The RAG engages in scientific research to support the deliberations and publications of the Commissioners and, through its outreach and community engagement, also fulfills a crucial advocacy mission of the Commission.

The core interaction of the Research Advisory Group occurs in four email lists that correlate to the key subject areas that the Commission focuses its work on. Find out how to join the lists here. Each list is moderated by a RAG Deputy Chair.

2.5.1. INTERNATIONAL PEACE AND SECURITY OF CYBERSPACE (RAG-P): RAG-P@CYBERSTABILITY.ORG

This cluster covers the (geo)political and military dimensions that affect the stability on and of cyberspace. It will mostly focus on responsible state behavior – examples can include systemic threats from international conflict to the stability of cyberspace, espionage and preparation of the battlefield, the stockpiling of zero-days, matters of attribution, political norms of behavior, and confidence-building measures. The impact of non-state actors and the private sector as relevant for International Peace and Security (IPS) issues will also be included when considered relevant - examples can include data protection frameworks, encryption issues as well as international cooperation between the public and the private sector. IPS issues (related to the UN First Committee on disarmament and international security) are a primary focus of the Commission, so this cluster will be further supported by the Chair of RAG, Sean Kanuck. The Deputy Chair and moderator of the list is Hugo Zylberberg, Cyber Fellow at Columbia University's School of International and Public Affairs and a member of the Castex Chair of Cyber Strategy in Paris.

2.5.2. INTERNET GOVERNANCE (RAG-I): RAG-I@CYBERSTABILITY.ORG

This cluster covers the issues and development pertaining to Internet governance and the evolution of the Internet. The GCSC aims to influence international peace and security, not Internet governance – the focus of the initiative is on work generally conducted in the First Committee of the UN, so-called "international cybersecurity". Internet governance has its independent processes with its own goals and institutions (i.e. ICANN, ISOC, etc), but at the same time the field can provide vital input into the wider IPS discussion. Also, some states addressing international cybersecurity issues routinely attempt to bring in questions of Internet governance, and often introduce uncertainty among the IPS actors as to the role and responsibility of the different institutions in technical and policy Internet governance. This cluster is mainly intended for the Internet

governance community to help better communicate and interact with the IPS community, and is moderated by Marilia Maciel, Digital Policy Senior Researcher at DiploFoundation.

2.5.3. LAW (RAG-L): RAG-L@CYBERSTABILITY.ORG

The Law cluster considers various legal issues pertaining to the stability and security of cyberspace. It deals with matters of both domestic and international law. Topics that are of relevance include understanding how existing law applies to cyberspace; identifying areas that demand legal regulation; ascertaining national and regional differences in domestic law as well as in approaches to international law; examining possible conflicts and synergies between domestic and international legal regimes; and determining mechanisms for improving compliance with the law. Moreover, the identification of legal norms will help focus and conserve efforts by avoiding the need to develop political norms regarding which legal norms already exist. Ultimately, the cluster will help to both sensitize the Commission to the range of legal opinion on various issues in cyberspace and support its efforts to advance international peace, security and stability in cyberspace through domestic and international law. The Law cluster is primarily intended for legal experts and is moderated by Liis Vihul, founder of Cyber Law International, the managing editor of the Tallinn Manual 2.0, and Ambassador of the NATO Cooperative Cyber Defence Centre of Excellence.

2.5.4. TECHNICAL AND INFORMATION SECURITY (RAG-T): RAG-T@CYBERSTABILITY.ORG

This cluster covers the technical aspects of cyberstability – examples can include the technical core protocols and standards of the internet, management and protection of critical information infrastructures and essential web services, threats, risks and their vectors, and any matters pertaining to network and information security. Technical RAG members are particularly encouraged to help explain the structure and contribution of the wider security community to combating all types of cyber-threats, and help ensure that the IPS community is appraised of some of these existing community features, their strengths and limitations. It is mainly intended for the InfoSec and technical community, and is moderated by Koichiro Komiyama, Deputy Director of the Global Coordination Division at JPCERT/CC.

ANNEX: PROPOSAL TEMPLATE

The proposal should be no longer than 2 pages (excl. supporting documents), and should be written in Arial, font size 10, single spacing.

[insert Working Title as shown on the project statement RFP]

1. DESCRIPTION OF THE APPLICANT (MAX. ½ PAGE)

Lead applicant	(Name of institution that will appear on contract; include address and phone number)
Legal Status:	(legal status of Lead applicant and Chamber of Commerce reference)
Person Submitting Proposal	(Name, title, telephone number and e-mail address)
Proposal Written by	(Name, title and affiliation of involved scholars)
Proposal Date:	(dd-mm-yyyy)
Principal Investigator:	(Name and title, and e-mail address)
Administrative Officer:	(Name and title, and e-mail address)

In case of a **joint submission** by two institutions, please provide the name, legal status, and contact information of the co-applicant(s), as well as the involved experts.

2. OBJECTIVES, RESULTS AND METHODOLOGY (MAX. 1,5 PAGES)

Title	(if the proposed project uses another title as shown on the RFP)
Objectives of the report	(overall and specific objective(s) of the project)
Estimated results / deliverables	(briefly outline the estimated result(s))
Activities and summary of Approach	(briefly outline the methodology and how it relates to the objectives and results)

3. SUPPORTING DOCUMENTS

- Resumes of key team members along with a description of responsibilities;
- A list of relevant prior publications of the (co-)applicant (you may enclose one or two samples).