

# Cyber Diplomacy

## Research project proposal



<b>GFCE Theme/Topic</b>	CBMs, Norms Implementation and Cyber Diplomacy
<b>Research Idea</b>	Cyber Diplomacy Gaps Analysis
<b>Existing work/literature on the topic</b>	<p>The Task Force has produced a whitepaper on cyber diplomacy and a brochure overview of existing training initiatives relevant to cyber diplomacy.</p> <p>Existing tools/trainings can also be found on the Cybil Portal: <a href="https://cybilportal.org/themes/cyber-diplomacy/">https://cybilportal.org/themes/cyber-diplomacy/</a></p>
<b>Problem statement/Knowledge gap</b>	<p>Cyber diplomacy – the practice of diplomacy in support of better cybersecurity in the international system is a new and evolving area of practice. The challenges of cybersecurity are universal, and it is increasingly a topic of discussion and action in various international fora.</p> <p>Nevertheless, it can be hard for diplomats (especially from smaller and poorer countries) to follow and fully contribute to those engagements because of lack of information, expertise, or simply available personnel. The discussion requires understanding of international law, technology, as well as foreign affairs.</p> <p>There is, therefore, an opportunity to help build capacity within the diplomatic community, to help both improve the overall quality of the dialogue and to ensure that countries can fully benefit from the international discussions. The first step in that process need to be a survey of the community engaged in cyber diplomacy a better understand of what tools, training, and support are available (even if they are widely used), and what practice could be drawn from other fields of diplomacy.</p>
<b>Scope of Research and limitations</b>	The project should map existing tools/trainings/support for cyber diplomacy. Based on this mapping exercise, the project will identify possible gaps and make recommendations on addressing needs in this space. The mapping exercise should consider as wide a geographical spread as possible.
<b>Research question(s)</b>	<p>What tools exist that, if used, could improve the practice of cyber diplomacy?</p> <p>What are the tools/trainings/support that could, if developed, enhance the delivery of cyber diplomacy?</p>
<b>Research objectives</b>	<p>Primary objectives:</p> <ul style="list-style-type: none"> <li>• To identify what tools and support is available to support the practice of cyber diplomacy and how widely they are used.</li> <li>• To identify where it would be possible to make existing tools and support more widely available.</li> </ul>

# Cyber Diplomacy

## Research project proposal



	<ul style="list-style-type: none"> <li>• To identify, based on best practice in other diplomatic communities or other relevant communities of practice, what tools and services could be made available.</li> </ul> <p>Secondary objectives:</p> <ul style="list-style-type: none"> <li>• To identify – where possible – what level of additional resource could make a significant difference to the challenge of creating a knowledgeable and well-informed community of diplomats focused on cyber issues.</li> </ul>
<b>Suggested research approach (method)</b>	Interviews with Task Force members (including but not limited to government representatives) and desk research.
<b>Research output</b>	A report with recommendations (where applicable).
<b>Beneficiaries</b>	This research will support the work of the Task Force in understanding what future activity it should do in this area.
<b>Time estimate</b>	Estimate of 83 days, with the final output to be delivered within 5 months of signing the contract.
<b>Estimation of human resources needed</b>	1 Researcher with expertise or experience in a relevant area such as: international multilateral negotiations (i.e. UN), (cyber) diplomacy, capacity building, etc.
<b>Selection Criteria (of research supplier)</b>	In-depth understanding of (cyber) diplomacy demonstrated by publications, reports, and/or other written materials (including academic articles, blogs, policy briefs/papers, etc.) on international negotiations, cyber diplomacy and/or cyber policy. Good understanding of cyber capacity as a topic of research and a demonstrated ability to write for a broad non-expert audience is preferred.
<b>Budget</b>	50K USD