International Cyber Law in Practice
Workshop Report

Friday 8 February 2019, 9:00-16:30

Exeter, United Kingdom

Introduction

The purpose of this workshop was to discuss the progress of the project and its outputs in depth with experts in the field and with potential users of the relevant outputs. The project has so far resulted in the co-creation of the first draft of an interactive toolkit on international cyber law in practice (available online). The present workshop followed after the pilot workshop held in Tallinn, Estonia, on 29 May 2018 (workshop report is available here).

The workshop was convened by Dr Kubo Mačák (University of Exeter) and Mr Tomáš Minárik (NATO CCD COE). Attendees included legal practitioners, cyber law experts, and researchers from armed forces, government bodies, and academic institutions in Europe, North and South Americas, and the Middle East. The workshop was held under the Chatham House rule,[1] resulting in a fruitful and vibrant discussion during the workshop.

Workshop participants

Opening plenary

The day started with a presentation delivered by Dr Mačák on the progress of the project since the first workshop in Tallinn. As noted, the project aims to produce an interactive toolkit, which will contribute towards bridging the existing gap between academia and practice in the cyber law domain. The core of the Toolkit consists of detailed scenarios drafted by the project team. The team was guided by input received at the previous workshop and then engaged in several months of independent research and drafting. In the next stage, the scenarios were sent off to external peer reviewers. Each peer reviewer was given at least two scenarios, which ensured that each scenario was reviewed by, on

[1] The following version of the Rule was used: "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed". See <www.chathamhouse.org/chatham-house-rule> (accessed 8 February 2019).

average, two or three peer reviewers. On the day of the Workshop, the Toolkit contained 13 peer-reviewed scenarios, 38 content pages and 161 pages in total.

The next part of the plenary was led by Mr Minárik who walked the participants through the Toolkit from a user's perspective, using the example of a government legal advisor who consults the Toolkit when tasked to provide legal advice concerning a massive DDoS attack against targets in that State's territory. The participants were shown a number of possible ways how to obtain the necessary information – such as exploring directly the relevant Toolkit scenarios or searching through real-world examples analysed in the Toolkit and selecting those that involved a DDoS attack.

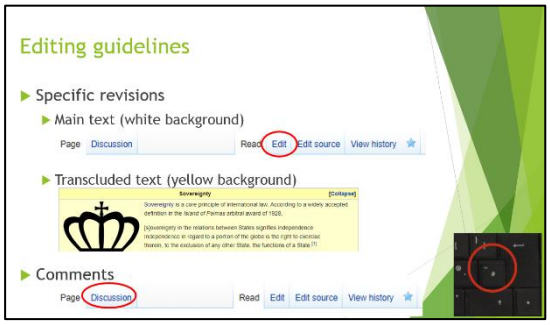
Toolkit at a glance: Screenshot of the front page

The participants contributed with a number of useful observations on the possible enhancements of the search functionalities, such as narrowing the search by labels or limiting the search to certain categories only. Another suggestion that was made in this session was to include a reference to each individual scenario that uses a certain legal concept at the bottom of the page dedicated to that legal concept.

The plenary further discussed the intended target group of the Toolkit, with a number of suggestions made by the participants. Some considered that the Toolkit would be best used as a training resource, while others saw it as suitable for the provision of operational advice. Although no clear consensus emerged through the discussion, the participants were in agreement that the Toolkit should be disseminated as broadly as possible in order to make it available to different kinds of audiences, which may include legal advisors, decision makers, academics, and students.

Another point that was discussed was the scope of issues covered by the Toolkit. Several additional topics were suggested by individual participants. These were welcomed by the project team who confirmed that their aim was to continue developing the Toolkit in the future and to keep adding new scenarios. It was noted that the current topics were chosen based on the expertise of the core team, as well as on the basis of the suggestions made at the first workshop.

Breakout sessions

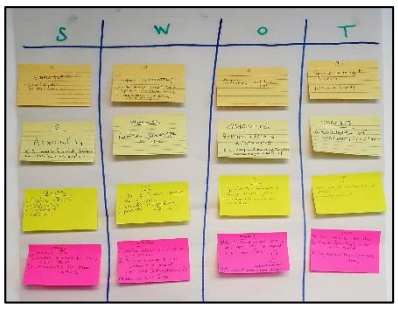


Editing guidelines for the breakout sessions

In the second part of the day, the attendees were split into pairs. Each pair of participants was tasked with the detailed review of two scenarios each. The participants used the editing functionality of the Toolkit to propose specific changes and modifications directly in the online text. Dr Mačák and Mr Minárik provided facilitation and guidance during these sessions. The sessions resulted in significant improvements of several of the scenarios and also served as a proof of concept as to the ease of further development and online review of the Toolkit content.

Closing plenary

During the closing plenary, the participants were asked to engage in a "SWOT analysis" of the Toolkit, i.e., to identify its potential strengths, weaknesses, opportunities, and threats. The contributions made by the participants have included the following:



SWOT chart co-created at the workshop

- **Strengths**: strikes the right balance between law and cyber and operations and academia; it is accessible in terms of the applicability of the law to practical scenarios, the format and the target audience; it is practice driven; its collaborative nature; it is comprehensive and scenario-based; it creates structure for thinking about the key issues.
- **Weaknesses:** not sufficiently visually appealing and user friendly; without knowing about the process behind it users might see it as "just another wiki page"; somewhat limited coverage of topics; narrow use of sources; for some it may require further interpretation.
- **Opportunities:** scalability and the fact that it is not fixed in time; responsivity; possibility for further interactivity through discussions; could incorporate a broader resource database; opportunity to expand into new areas.
- **Threats:** needs a patron; issues with maintenance and keeping currency/coverage; resources for its continuation; quality control of the content.

Each group then made overall recommendations for the project based on the SWOT analysis and previous discussions. These included the following suggestions: add new cyber and non-cyber topics to the Toolkit; strengthen the bibliography with primary sources as well as more geographically-diverse sources; keep the Toolkit interactive; establish a feedback mechanism for users; emphasize the credibility of the toolkit by expressly noting the contribution of the peer-reviewers and content-creators; and improve the external appearance of the project.

Continuity

The majority of the participants expressed their interest to remain involved in the next stages of the project. The project will continue with the finalization of the Toolkit over the months of February and March 2019. In parallel, a professional designer will be commissioned to polish the final appearance of the Toolkit. Finally, the Toolkit will be formally launched at CyCon 2019 in Tallinn, Estonia.

The organizers are grateful to the Economic and Social Research Council for its generous support of the project; to Exeter Law School for providing the venue for the workshop; to Exeter Centre for International Law for organizational support; to Kate Wannell for administrative support; and to students Matt Kuningas and Jana Šikorská for assistance on the day of the workshop.