Introduction

Introduction to Special Issue on Nordic Perspectives on the International Legal Regulation of Cyberspace

Smaller liberal nations like the Nordic countries have a clear and vested interest in maintaining a rules-based international order. This general statement holds no less true when it comes to threats emanating from the cyber domain. While the vast majority of States now generally agree that the rules of international law apply also in the cyber context, there is still much disagreement about the specific understanding and application of a number of key rules. Indeed, several recent conflicts, including notably the war in Ukraine, have made it obvious that the lack of clarity with regard to the international legal regulation of cyberspace continues to provide fertile ground for abuse by hostile States, while simultaneously making it difficult for allied nations to lay down common cyber security strategies and policies. In other words, there are plenty of reasons for the Nordic countries to take an active role in the ongoing debate on and development of international law in the context of the cyber domain. The question is, of course, which interests the Nordics should promote – and how? These issues were addressed at a conference ‘Nordic Perspectives on the regulation of cyberspace under international law’ held at the University of Copenhagen on the 28th and 29th September 2022. Over the course of the two days of the conference, legal scholars and civil servants discussed both the state of the law within the cyber domain and the role that the Nordic nations play – or might choose to play – in the ongoing international debate. The present special issue of the Nordic Journal of International Law has its origins in this conference.

The special issue comprises two types of contributions: Firstly, it includes official statements – ‘position papers’ – by the governments of Denmark,
Finland, Norway, and Sweden on the application of international law in cyberspace. Denmark’s position paper is published for the first time, whereas the Finnish, Norwegian and Swedish statements, which were originally published in 2020, 2021, and 2022 respectively, are reprinted with new introductions. As such, the special issue collects the available official Nordic perspectives on the state of international law in cyberspace.

Secondly, the special issue includes five academic articles that each address aspects of the lack of clarity we are experiencing on the interpretation and application of key rules of international law in cyberspace. In the first article entitled ‘Virtual Groups and the Triggering of Armed Conflicts’, Marie Thøgersen considers how virtual groups can trigger armed conflicts and thus the application of international humanitarian law (IHL). Thøgersen contends that the rise of non-State actors in cyberspace and the growing use of cyber operations in conflicts make regulating these actors an increasingly pressing concern. Specifically, the article analyzes the organization requirements in IHL’s triggering provisions for non-State groups and identifies their underlying rationales. Thøgersen ultimately concludes that these provisions do not currently permit reinterpretation to accommodate the unique structures of virtual groups, thus making it difficult for such groups to actually trigger an armed conflict.

In the second article entitled ‘Attacking Data: Moving beyond the Interpretative Quagmire of the ‘Data as an Object’-debate’, Marc Schack & Katrine Lund-Hansen explore a key contemporary IHL problem in regulating cyber operations: How to apply the law on ‘attacks’ under IHL when the target is neither a person nor a physical object in the traditional sense but rather purely (digital) data. Schack and Lund-Hansen consider the current state of this – long-standing – legal debate and explore ways of moving the debate forward. Thus, while critiquing the standard interpretative approach of either focusing on the ‘ordinary meaning’ of the term ‘object’, or on the ‘object and purpose’ of the rules, the authors argue that the debate could be advanced by adding an additional, contextual analysis. Doing so, the authors argue, would make it is possible to achieve a more coherent and meaningful outcome for this complex debate.

Pia Hüsch’s contribution, ‘Non-Intervention Thresholds in Cyberspace – In the Shadow of the Sovereignty Debate?’ explains that important questions about the functions and effects of the legal principle of non-intervention in the cyber domain have been overshadowed by debates about the application of the principle of sovereignty. On this basis, Hüsch takes the reader through
the two parallel debates and considers how these have progressed. From here, Hüsch sets out the implications of the one-sided focus of the debate, noting for example that questions of the relevant legal thresholds have not been treated in the same level of detail by States, which could create problems as States begin to grapple more with the non-intervention principle. Given the need for clearer red lines, Hüsch emphasizes why Nordic countries in particular should have an interest in advancing these discussions, and she notes that they could advance such interests either through more detailed state pronouncements on the matter, or through collective statements e.g., by the Nordic countries.

Going somewhat in the other direction, Peter Pijpers argues, in his contribution entitled ‘Careful What You Wish For: Tackling Legal Uncertainty in Cyberspace’, that the increase in the number of State’s expressions of legal opinions does not, as is commonly assumed, necessarily increase the level of legal certainty – rather it decreases it. Pijpers explains that while it is widely acknowledged that international law applies to cyberspace, there is an ongoing dispute about ‘how’ it applies, and the hope, he argues, that once we get more opinio juris and State practice, we will be able to clarify the rules, is ill-founded. Rather, Pijpers notes that the recent increase in the number of legal opinions has led to more differences and thus greater legal uncertainty, and that this may even result in a kind of legal asymmetry, where some States chose to comply with international law while others exploit the ambiguity to support their own strategic goals. Therefore, one should – as an international lawyer – in Peter Pijpers’ words be ‘careful what you wish for’.

Finally, Henning Lahmann’s ‘The Plea of Necessity in Cyber Emergencies: Unresolved Doctrinal Questions’ rounds off the academic contributions. While an increasing number of States recognize the plea of necessity in cyber emergencies, many important doctrinal questions remain underexplored. Lahmann focuses on three key issues: 1) the ‘only way’ requirement, 2) the non-contribution condition, and 3) the question of assistance by unaffected states in emergencies. He concludes that the necessity defense continues to present a range of problems in relation to all three of the issues considered. Specifically, Lahmann finds that it is still unclear, in regard to the first requirement, if the dominant, strict understanding of the ‘only way’-criterion could be softened, which makes reliance on the necessity defense difficult. On the non-contribution condition, he concludes that emerging norms obliging States to observe a certain standard of ‘cyber hygiene’ in regard to domestic cyber infrastructures could influence legal assessments. Finally, in considering the question of assistance, Lahmann does not find clear guidance in the law.
Thus, he notes several relevant policy perspectives and argues that it would be preferable if States would strive for more legal clarity.

Marc Schack  
Associate Professor in International Law and National Security, Faculty of Law, University of Copenhagen, Copenhagen, Denmark  
marc.schack@jur.ku.dk

Astrid Kjeldgaard-Pedersen  
Professor in International Law and Vice Dean for Research, Faculty of Law, University of Copenhagen, Copenhagen, Denmark  
astrid.kjeldgaard-pedersen@jur.ku.dk