ASSER INSTITUTE

Centre for International & European Law

The International Law of Peacetime Cyber Operations - The Hague Launch of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations and a Panel Discussion

On 13 February 2017, the Asser Institute, together with the Ministry of Foreign Affairs of the Netherlands and the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) held a meeting and panel discussion to celebrate the launch of the "**Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**". The panel brought together **Prof. Michael Schmitt**, Director of the Tallinn Manual project; **Ms. Marina Kaljurand**, former Estonian Minister of Foreign Affairs and current Representative to the United Nations Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security; **Mr. Steven Hill**, Legal Advisor and Director of the Office of Legal Affairs of NATO; and **Dr. Marten Zwanenburg**, Legal Counsel to the Netherlands Ministry of Foreign Affairs.

Welcome speeches

Prof. Ernst Hirsch Ballin, President of the T.M.C. Asser Instituut, commenced by welcoming the participants and the audience. He was followed by **Mr. Sven Sakkov**, Director of NATO CCD COE, who emphasised the role of the Centre of Excellence in supporting the drafting and publication of the Manual, underlining that it is not an official NATO policy or doctrine.

Bert Koenders

In his keynote speech, **Mr. Bert Koenders**, Netherlands Minister of Foreign Affairs, addressed the new challenges stemming from so-called "cyber-attacks": he underlined that while such attacks often give rise to discussions on technical issues, it is equally important to address the question of behaviour. He stressed the need for work at the policy, legal and diplomatic levels to understand and change behaviour in cyberspace. Recalling recent events, including the attempts by hackers to influence the outcomes of national elections, he highlighted that international law helps determine how we can and should respond. He recalled that the answer to the question of how particular rules of international law can be applied to cyber operations is not always straightforward and that the role of the Tallinn Manual lies in helping to find that answer. In this regard, he welcomed the fact that the updated Tallinn Manual deals with a broad array of principles and rules that apply in peacetime, including the law of state responsibility and international human rights law.

He also praised the geographical diversity of the International Group of Experts (IGE) that drafted the Tallinn Manual 2.0, which included Chinese and Belarussian experts, to tackle an ever-more global concern.

Minister Koenders also mentioned a number of efforts by the Netherlands aimed at strengthening international stability in the cyber realm. These include the facilitation of dialogue between experts drafting the Tallinn Manual and legal advisors of states through "The Hague Process", and the establishment of the Global Commission on the Stability of Cyberspace. In doing so he underlined that we are now in a new era – not a World War III nor a new Cold War – in which new technologies and new behaviour require new tools and new thinking. He concluded by calling for pursuing the discussion on how international law applies to cyber operations.

Liis Vihul

Ms. Liis Vihul, Project Manager and Managing Editor of the Tallinn Manual 2.0, gave an overview of the new edition of the Tallinn Manual and its drafting process. Recalling the long-time partnership with the Asser Institute, Ms. Vihul also highlighted the role of Estonia at the forefront for issues related to cyber defence and security. While the Tallinn Manual 1.0 primarily addressed cyber operations that occur in armed conflicts, this new edition examines the law applicable to cyber operations that remain below that threshold.
She insisted on the status of this Manual as not a negotiation document nor a treaty proposal, but rather as a reference tool developed to **support national legal advisers**, which was further supported by the panellists.
She mentioned the rigour of the process, from The Hague Process to the peer review, both of which helped ensure a high quality document.

She concluded on the substance, clarifying what the Manual is: a comprehensive interpretation of public international law in the cyber context, presented in the form of 154 **black letter rules,** representing the consensus of the IGE, accompanied with sets of **commentaries**, that provide the legal basis for each rule, as well as nuances in application and points of disaccord among the experts. The last four chapters concern the *ad bellum* and *in bello* rules applicable to cyber operations (in other words: the Tallinn Manual 1.0), whereas the rest of the document relates to cyber operations in *peacetime.*

Panel Discussion

Following these introductory speeches, **Prof. Larissa van den Herik** from Leiden University, the moderator, formally initiated the panel discussion and introduced the speakers. The panel took place in a Q&A format, first within the panel, and during the second part the floor was given to the audience.

Prof. Van den Herik began by asking the panellists how they appreciated the value and legal status of the Tallinn Manual from their respective perspectives, and she asked Prof. Schmitt specifically to elaborate on the status of the Manual as the product of an expert process from a legal perspective.

Prof. Schmitt expressed his contentment with the traction gained by the Manual when presented to States, despite the strong independence of the IGE. He insisted on the importance of the document as an advisory tool and mentioned that he considered the book's strongest asset to be the fact that disagreements of the authors have been set out in the commentaries. He also stressed the importance of states engaging in cyberspace-related international law discussions.

Ms. Kaljurand encouraged states and governments to look into the Tallinn Manual, because lawyers can provide their understanding of international law and it is up to states to interpret and apply international law in practice. This means also political decisions which are not always easy. In 2007 Estonia applied national laws and international law in attributing the cyber attacks against Estonia and in taking retorsion measures. She also introduced the relevance of the **private sector**, which will be crucial in developing norms together with governments.

Mr. Hill highlighted the role and function of NATO as a place of consensus aimed at helping Allies to build cooperative defence capabilities and, regarding cyberspace, conducting cyber exercises, developing reaction teams, and coordinating efforts. Indeed, at the Wales and Warsaw Summits the NATO Allies underscored the applicability of international law in cyberspace. The legal domain within the Alliance is heavily influenced by the Member States who must reach a consensus on the various policies and decisions. Nonetheless, he suggested that the Alliance is well-suited as one forum for open discussion between the Member States of NATO on the future of collective defence in cyberspace.

Dr. Zwanenburg, in agreement with his colleagues, added that states would have to produce strong arguments to take an interpretation contrary to that of the Tallinn Manual, given the extensive research underpinning the document and the authority of its drafters.

***

Second, ***Prof. Van den Herik*** *asked the panellists to elaborate on what they regarded as crucial aspects* ***addressed by the 2.0-version of the Manual*** *and also* ***how States should implement or follow up on its propositions****.*

Prof. Schmitt addressed the challenge of **State sovereignty** when it comes to the implementation and interpretation of the law, citing the example of determining how to categorise a cyber operation that does not cause physical damage or injury but does result in a deprivation of functionality. He stressed the work to be done in these areas for a functioning framework. Secondly, he gave the example of the Democratic National Convention hack, asking whether such acts amounted to a breach of the prohibition of intervention in the internal affairs of other states – he took the position that they do so. Thirdly, he insisted on the importance of the principle of **due diligence** of states in cyberspace, concluding that this principle needed to be upheld also in the cyber domain. In particular, application of the principle of due diligence may open a door for action against non-state actors by pursuing actions against the state that failed to take sufficient measures to put an end to the non-state actor's harmful cyber operations. He added, when talking about the actions states could undertake to respond to cyber operations, that the question of **pre-emptive countermeasures** had not been agreed upon as it is a sensitive issue.

Ms. Kaljurand re-affirmed that the applicability of international law to cyber space is **internationally agreed and recognised**. She highlighted that the same ideological division that exists in the real world is mirrored in the cyber sphere: on the one hand there are states that support the peaceful use of ICTs for the benefits of their societies and people, and on the other, there are states that try to limit freedom of Internet and the use of ICTs. This is also reflected in the way different states approach international law. Applicability of international law has to be a subject that is addressed by all states – developed and developing states.

Asked to specifically address the **stance and role of NATO, Mr. Hill** answered that the "grey areas" of the Manual could be used by injecting them into their discussion and training processes of the Alliance in order to see the results. However, he remarked, NATO is rather focused on practical and military cooperation. And while the Manual is primarily directed at states, he said that the document was also **very relevant for international organisations**, which can provide a venue for states to express their positions on the law, more specifically on how international law applies.

When the same question was raised regarding the position and perspectives of the ***Netherlands***, **Dr. Zwanenburg** stated that the Manual will be useful in two ways.

Although their state's international obligations and interpretations of those obligations that have been given previously will be the starting point for state legal advisers, the Manual serves as an authoritative source of reference that they can draw on.

In this regard it is particularly useful that the Manual often describes different possible interpretations, and why experts considered these to be the better view or not. He added that the second way in which the Manual can be useful is as a platform for discussion between state legal advisers among themselves and with others. He concluded that therefore, The Hague Process was not yet over.

***

Prof. Van den Herik *subsequently asked the panellists* ***whether, given the non-binding status of the manual, a new treaty on cyber operations would be a logical next step,*** *and, complementarily,* ***what the role of private actors would or should be in the further elaboration of norms and in their implementation****.*

Prof. Schmitt admitted he was **pessimistic** on the idea of a treaty, due to the complexity of such a process when factoring in national policy elements. Nonetheless, he claimed he was **optimistic** regarding how the Manual as well as actions taken by the UN Group of Governmental Experts (GGE) will affect states at the operative level. He stated the importance of state practice and *opinio juris*, hoping that strong reactions will occur when a state crosses a red line and that they would go further by creating **ground for normative discourse.**

Ms. Kaljurand explained that there are different views on the need to write new international law, e.g. the Code of Conduct proposed by Russia, China and some other states. She supported the need to analyse existing international law before reaching conclusions about drafting additional international law. She did not exclude completely that at some point there might be a need for additional international law, but at this stage it is too early to make any final conclusions. Today it is crucial to analyse, interpret and apply existing international law.

Mr. Hill pointed out that, under certain conditions, a cyber incident **could trigger Article 5** of the Washington Treaty and allow for collective defence between the Allies. Nonetheless, it would all depend on the specifics of the incident and the decision of the Alliance.