# Development of International Law on Cyber Operations: Contextualizing the Use of Force, the Law of Armed Conflict and Non-State Actors

パパワディ, タノドムデッ

氏　　名　：　パパワディ タノドムデッ

論文題名　：　**Development of International Law on Cyber Operations: Contextualizing the Use of Force, the Law of Armed Conflict and Non-State Actors**

(サイバー活動をめぐる国際法の展開 —武力行使、武力紛争法、非国家主体の文脈の中で—)

区　　分　：　甲

## 論　文　内　容　の　要　旨

Cyber operations directed at computer systems of powerplants can cause life-threatening dangers as any malfunction may possibly lead to explosions causing death and injury of persons. More generally, the effect of cyber operations on individuals' lives aggravates in proportion to the extent to which states and private sectors rely and depends on cyber technology.

Despite the UN GGE's confirmation that existing international law applies to cyber operations, states could not agree on how exactly it shall apply. The Tallinn Manual on the International Law Applicable to Cyber Warfare and the second version (2.0) on Cyber Operations (the Manuals), which are non-binding instruments drafted by legal scholars, attempted to fill this gap. Moreover, tech companies have asserted a law-making role by proposing the Digital Geneva Convention to be adopt by states and by obliging themselves under the Cybersecurity Tech Accord to protect themselves and individuals from the effects of cyber operations.

The assertiveness of these two groups of non-state actors justifies to reconsider whether their potential to contribute to the making of the international law on cyber operations is on par with states, which would have significant repercussions on the existing *lex lata* applicable to cyber operations. Therefore, this thesis commences with the identification of the *lex lata* by an assessment of the Manuals and respective legal scholarship stretching existing international law to cover cyber operations. Part I starts with Chapter II which elucidates the applicable law on cyber operations and discusses three flaws of the Tallinn Manuals: (1) the composition and (2) the authority of the International Group of Experts as well as (3) the drafting process. Chapter III examines different definitions related to cyber operations, including cyber attacks and information warfare, by taking into account the divergent perceptions of the North Atlantic Treaty Organization (NATO) and the Shanghai Cooperation Organization. Furthermore, it demarcates different kinds of cyber operations by utilizing the use of force threshold. Chapter IV examines possible interpretations of the UN Charter, in particular Article 2 (4) and chapter VII including the notion of an armed attack, with regard to cyber operations. The three approaches (instrument-based, target-based and effect-based) are discussed, and their respective partial or complete incompatibility with cyber operations is shown. The thesis proposes 'cyber causation' as an alternative approach, complementing the effect-based approach, in order to cover the destructive consequences of events originating from the launch of cyber operations in the first place. Cyber causation also contributes to the solution of the problem of distinguishing cyber operations amounting to an armed attack from those reaching the threshold of the use of force. Chapter V examines international legal rules applicable to cyber operations falling short of a use of force by exploring incidents of low-threshold cyber operations such as the interferences with the 2016 US presidential election and acts of disinformation. Chapter VI examines the applicability of the Law of Armed Conflict (LOAC) to cyber operations. It focuses on fundamental LOAC principles such as the distinction

between combatants and civilians, and military necessity. These selected issues are particularly problematic as to the use of cyber infrastructure for purposes of warfare. Part II explores the authority of non-state actors regarding the making of the international law on cyber operations. Despite the wide variety of possible non-state actors, the thesis focuses on tech companies and legal scholars as these are, besides states, outstanding with regard to cyber operations. Chapter VII discusses the status of states as subjects of international law that is associated with their capacity to make law. In particular, it addresses the theory which considers that there is no benefit in differentiating between subjects and objects of international law, regardless of whether states or non-state actors participate in the law-making process. The Chapter examines this phenomenon in cyberspace where the rise of non-state actors as both law-makers and major participants is particularly visible. In order to assess the actual potential of non-state actors to make the international law on cyber operations, Chapter VIII examines the essence of normativity in international law by distinguishing between law and non-law elements in propositions from tech companies such as the Digital Geneva Convention and the Cybersecurity Tech Accord. The role of legal scholars, in particular the International Group of Experts, is examined through the theory on communicative practice. The Chapter is completed with an assessment of the interaction between the products of non-state actors and traditional international law.

This thesis finds that not all rules in the Manuals are *lex lata* and that non-state actors are not able to directly make international law on cyber operations. Their outputs, rather, contribute to law-making indirectly as the final decision whether their outputs attain the status of international law remains with the states. The thesis thus inserts a caveat into the discourse supporting non-state actors' full authority to make international law and, instead, finds non-state actors to assume a subordinate role, particularly in the field of cyber operations.