Summary

This dissertation constitutes an inquiry into legal knowledge construction in the academic discourse on cyberwar and international law. It takes a grassroots approach towards the ‘how’ of legal knowledge construction in this discourse, and emphasizes the particular, singularly spoken and written word, as well as the part played by the individual scholar who utters it: what exactly is said in this academic discourse, and who is doing the saying? This means that the main question asked in this dissertation is understood as comprising two distinct subquestions: what do scholars do, to come to their legal answers, and who has a seat at the table in bringing these answers about?

From the mid-1990s onwards, international legal scholars have been concerned with the issue of how international law can and should respond to cyberattacks. The word ‘cyberattack’ as used in ordinary language, can mean different things: for example, it can refer to the hacking of personal bank accounts, or economic espionage into corporate affairs. In this dissertation, however, the focus lies on disruptive and/or destructive cyberattacks, with the involvement of at least one state. In other words, this dissertation deals with the international legal debate on hostile actions perpetrated in or by means of cyberspace.

There are several legal issues that arise as a consequence of the possibility of cyberwar: for example, scholars have considered the question of state responsibility for the acts of a non-state hacker group, or when a state can defend itself against a cyberattack. This dissertation primarily focuses on one specific part of the debate, namely the question how the prohibition on the use of force applies to cyberattacks.

The prohibition on the use of force can be found both in customary as well as treaty law, specifically in Article 2(4) of the UN Charter. Under this provision, states are prohibited from using force against other states; it similarly prohibits the threat to use force. Over the last few decades, the meaning of the word ‘force’ has time and again been subject to debate: the norm pertains to, at least, military, kinetic force, but the question is where its boundaries lie exactly. The extent of the prohibition was discussed in relation to the impermissibility of the use of biological and chemical weapons; similarly, in the 1970s the question arose whether the oil embargo imposed by OPEC on Western countries violated the prohibition on the use of force. Recently, the same question has been asked with regard to cyberattacks: does the prohibition allow for an extension towards attacks perpetrated by means of zeroes and ones, with a possible non-physical impact – or is the prohibition limited to those attacks that have a physical result?
In applying the prohibition to cyberattacks in their writing international legal scholars make several assumptions. First, in order to apply the norm it has to be clear where the attack originated; in other words, the cyberattack in question has to be attributed to a particular source. Given the characteristics of cyberattacks attribution is by no means a given; the assumption has to be made, however, in applying Article 2(4). Secondly, in applying the norm the assumption has to be made that the attack can be attributed specifically to a state. The prohibition on the use of force, at least as far as the treaty norm is concerned, only pertains to the relations between states: it prohibits the ‘members of the United Nations’ from using force against each other. As only states can be members of the UN, the prohibition similarly applies only between them. This also implies that the prohibition is meaningless when the cyberattack is perpetrated by a non-state actor: in that case, Article 2(4) is simply irrelevant. This is particularly problematic in the case of cyberattacks, as these are often perpetrated by non-state actors. Unless a relation to a state can be ascertained on the basis of the Articles on State Responsibility, Article 2(4) has nothing to say about the attack in question.

The reason for focusing in this dissertation on the prohibition on the use of force lies both in the nature of the norm itself, as well as in one of the main characteristics of cyberattacks. Once referred to by the International Court of Justice as the “cornerstone” of the UN Charter, the prohibition on the use of force had, in 1945, a profound impact on the way international relations are perceived from the perspective of international law. The aim was not just to outlaw the waging of war, but the use of force as such – a much broader category than warfare. To use force, from 1945 onwards, meant to violate the ‘normal state of affairs’, i.e., peace. Given the importance of the norm for the international legal system, the construction of its meaning in the cyberwar debate is likewise of particular importance.

The second reason for the primary focus in this dissertation on the prohibition on the use of force, lies in one of the characteristics of cyberattacks. Cyberattacks can be both disruptive as well as highly destructive: they can disturb online banking systems for a couple of hours, but they can also aim at the air traffic control systems of a major airport. What emerges, is a huge grey area of activities that are difficult to classify either as ‘force’, or as ‘non-force’. In other words, what international legal scholars attempt to do in their writing, is assess the threshold for violating the prohibition: when does the cyberattack in question reach the level of ‘force’, prohibited under Article 2(4)? Given the focus on knowledge construction in this dissertation (see below), as well as the difficulty in assessing the meaning of the norm in this particular case, the question as to how these legal answers are nonetheless constructed becomes particularly interesting.

The way these scholars approach this issue is what is referred to in this dissertation as ‘legal problem-solution’: the emergence of a new phenomenon – cyberwar – requires the development or application of (new, better) law to mitigate its possibly harmful consequences. The common denominator of the group of scholars whose work is considered here, can thus be described as a belief in the regulatory capacity of international law. In this understanding, moreover, this legal solution can be arrived at in a structured, rational fashion. The questions asked by these international legal scholars are, for example, ‘how can existing rules be applied to cyberwar? What does ‘force’ mean in the context of cyberattacks? How to draw the line between what is, and isn’t, ‘force’?’ This dissertation does not deal with these questions but instead, it considers
how the answers to these questions are constructed. In other words, how is legal knowledge constructed in the academic discourse on cyberwar and international law?

This dissertation considers the answers to these questions as the construction of particular disciplinary knowledge: these scholars are participating in the academic discipline of international law. This means it does not primarily approach international legal scholarship as involving ‘the application of law’, but rather, as a particular discipline within which scholars collectively construct (in this case legal) knowledge. Considered as such, legal scholars will act to some extent in a similar way as those academics involved in other disciplines, such as philosophy or linguistics. More concretely, the knowledge practices employed by international legal scholars – the way they refer to other academic work, or how academic authority is established in a particular discourse – may overlap with those employed by other scholars. In short, the attempt here is to not consider international legal scholarship as particular, but to allow for the possibility that it is not. Moreover, the assumption here is that, if we truly want to understand how legal knowledge comes about, we will have to look at what it is legal scholars ‘actually do’. The primary tool used here is description of these practices, where the main question is ‘how’ legal knowledge is constructed (rather than, for example, why certain answers prevail over others). Underlying this perspective is the assumption that (following the work of Ken Hyland) academic knowledge is socially constructed. This means that the emphasis lies on the interaction between academics, the language they use to come to their particular answers, and the construction of authority within particular (sub)disciplines.

At the same time the dissertation aims at balancing the internal (the doctrinal legal argument) and external (the reflection on how legal answers come about) perspective on these practices. The aim throughout this dissertation is to remain situated ‘in law’, all the while retaining the possibility of reflecting on the practices employed. What this sociological approach means for this dissertation, is that the arguments and practices scrutinized here are identifiable as legal ones to two sets of legal scholars: to those involved in the debate on cyberwar and international law, who maintain an internal perspective on it, but also to those (critically) reflecting on these practices.

The dissertation is structured as follows.

The first chapter introduces the cyberwar discourse; it clarifies the theoretical perspective taken in this dissertation and the methodology resulting from that perspective. This has been outlined, above.

The second chapter provides an overview of the cyberwar discourse, and functions as the framework for the three close-ups of the cyberwar discourse presented in chapters 3 to 5 of this dissertation. The aim of this chapter is to detail what it is international legal scholars are concerned with: what exactly do they mean by cyberattacks, for example; and what is the international legal framework within which they design their arguments? The chapter first presents the ‘reality’ of cyberwar: it gives a brief overview of the ‘actual’ cyberattacks states have engaged in up to this point, that would qualify for consideration under the jus ad bellum and the jus in bello, and shows how these attacks are discussed by legal scholars. It furthermore gives an overview of the emerging opinio juris, and proceeds by elaborating on the notion of ‘legal problem-solution’, already referred to, above. It explains what this phrase means exactly
and what it entails in terms of scholars’ expectations of what international law can do. It subsequently provides the background specifically for the discussion on the application of Article 2(4) to cyberattacks, and gives a taxonomy of cyberattacks. As a contrast to legal problem-solution the chapter furthermore discusses the work of those scholars who question the ability of international law to regulate this phenomenon in the first place.

Chapters 3, 4 and 5 subsequently present three close-ups of the cyberwar discourse: together they deal with the ‘what’ and ‘who’ of legal knowledge construction in the cyberwar discourse. Whereas the first close-up and the first half of the second, focus on the ‘what’ of legal knowledge construction, halfway through the second close-up the focus of this dissertation switches to the question of ‘who’ is doing the saying.

The first close-up of this dissertation, in chapter 3, is titled “Not ‘armed force’ in the literal sense.” The title is taken from one of the articles written on Article 2(4) and cyberattacks, and it signifies how scholars reconstruct the meaning of ‘force’ in light of the “novel features” of cyberwar. The chapter starts with a more general introduction into how the prohibition is given meaning through legal reasoning, subsequently zooming in on how precisely its boundaries are constructed. Given the range of effects potentially caused by cyberattacks, the question these scholars struggle with is where to draw the boundary of the prohibition on the use of force. By juxtaposing the different arguments scholars make in this “gray area” of law, the first close-up shows what legal knowledge construction at the boundaries of Article 2(4) looks like. It does so by identifying two argumentative turns scholars take in legal reasoning. The first pertains explicitly to the boundaries of the norm. This part of the chapter shows how both the sufficiency, as well as the over- or underinclusiveness of the prohibition are contingent on a previous decision – made as part of the argument presented to the reader – as to the ‘inside’ and ‘outside’ of force. Whether existing law ‘allows’ for an expansive reading to include cyberattacks or whether it is insufficient in covering the wide range of effects caused by them, is demonstrated to be the outcome of legal reasoning, and not a quality inherent to the rules themselves. The second junction identified in these pieces, is the classification of the threat presented by cyberattacks. Whereas to some scholars cyberattacks constitute simply a new means to wage war or exercise coercion, to others the change is much more fundamental. Whether a scholar, in his/her article or chapter, opts for the first label or the second, matters to how the legal analysis proceeds towards a diagnosis of the (in)sufficiency of the norm. Through the identification of these junctions this chapter shows how ‘force’ receives its boundaries through legal argument, and that these boundaries are not pre-set. This is the first close-up of the cyberwar discourse.

The second close-up, in chapter 4, is titled “The greater part of jurisconsults.” It remains with scholarly interpretations of Article 2(4), but focuses on the use of one particular argument: consensus claims. With ‘consensus claim’ I refer to, e.g., appeals to majority opinion, generally accepted interpretations, or unanimity: phrases such as “the generally accepted interpretation is that the term force within Article 2(4) is limited to armed force.” These kinds of claims are found throughout scholarly writing on the prohibition on the use of force, and the fourth chapter starts by examining what these claims purport to do in a scholar’s argument about the meaning of ‘force’. It first posits that the function of these claims is to present a fixed reference point for the legal argument: once claimed, the scholar concerned has to relate his or her argument to this stated consensus. The chapter takes a further step, however, in explaining how consensus claims
are also claims to authority: after all, one can disagree with a particular interpretation of a norm, but it is much more difficult to disagree with the majority interpretation of that norm. This majority, the chapter claims, has the character of a somewhat mystical ‘out there’ – which may be precisely where its strength in the argument lies. Consensus evades capture; and this may be the reason it ‘works’ in an argument.

This does raise the question, however, whether consensus claims are ‘false’. After all, if everyone claims it is there, one might wonder whether as a result something emerges which may best be described as ‘meta-consensus’, where consensus follows from the mass of claims that consensus exists (or: the performativity of consensus claims). However, if we trace the use of consensus claims, we find that they are made very early after the creation of the norm in 1945. This suggests that consensus does not just follow from its repeated invocation, but also precedes its postulation in the discourse on Article 2(4).

The second half of chapter 4 subsequently considers how these claims are substantiated in legal writing. For example, the phrase “the prevailing and commonly accepted view” put forward by scholars is that the force referred to in Article 2(4) is limited to armed force”, is followed by a footnote. The ‘sources’ listed in this footnote seemingly function to substantiate the claim that this is, indeed, ‘the prevailing and commonly accepted view’. However, as shown in the appendix of this chapter the footnotes following these consensus claims most of the time consist of references to largely the same, limited set of scholars. Simply put, in order to support their consensus claims, scholars largely refer to the same publicists; something referred to in the chapter as ‘self-referentiality’. Making use of the notion of “concept symbols” as developed by Henry Small in the sociology of science, this chapter shows how these ‘most cited scholars’ turn into the ‘bearers’ of majority opinion; they are ‘symbols’ for the ‘concept’ of consensus. From this also follows that a convincing substantiation of the consensus claim can only follow from a reference to a scholar others will recognize as authoritative. In other words, we do not just cite randomly to support these claims; we cite so others will recognize. The chapter concludes that even though in an individual piece a singular reference can appear to be quite harmless, when considered as a more widespread practice of ‘self-referentiality’ it seriously impacts who gets a say – and thus, ultimately, what we know – in international law.

In this manner, halfway through the dissertation focus changes from the ‘what’ of legal knowledge construction to an inquiry into ‘who is doing the saying’ in the cyberwar discourse. Whereas the third chapter and the first half of the fourth focus on what it is scholars say exactly, halfway through chapter 4 emphasis shifts to the ‘who’ of legal knowledge construction. The third and final close-up of the cyberwar discourse, in chapter 5, continues the focus on the ‘who’ of legal knowledge construction.

Chapter 5 focuses on the academic presentations of Michael Schmitt, professor of international law in the US and one of the foremost authorities on cyberwar and international law. It asks how, by means of these presentations, he positions himself at the heart of the cyberwar discourse. The title of this chapter, “Call me again if you’re ever ready to begin answering the questions”, is taken from one of the presentations given by Schmitt about the Tallinn Manual on the International Law Applicable to Cyber Warfare – an international legal handbook, written by legal scholars on the application of the jus ad bellum and jus in bello to cyberwar. The Tallinn
project was directed by Michael Schmitt, and, given its position in the cyberwar debate, further affirmed his status as one of the most important figures in this discourse. What the Tallinn Manual represents in the cyberwar debate, is an ‘authoritative reference point’ (following Venzke) to those involved in it: when writing a piece about cyberwar and international law, it is almost impossible not to mention the Tallinn Manual.

The fifth chapter considers Schmitt’s presentations on the Tallinn Manual specifically, and on cyberwar and international generally, to entail a kind of map-drawing of the professional world he inhabits. By means of linguistic analysis it seeks to show how his construction of authority happens exactly. The first part of the chapter shows how Schmitt relates to ‘time’ and international legal thinking; the second, how he constructs a spatial map of the field within which he functions. With regard to ‘time’, Schmitt positions himself as well as the Tallinn Manual squarely within the history of international legal thinking; secondly, he has a strong sense of certainty about the substance of existing law, and, lastly, he proclaims the possible futures of international law on cyber. The second part of the chapter shows how Schmitt discursively positions himself in relation to several ‘others’, including, non-lawyers; other(s) (lawyers) who, in his view, misinterpret international law as well as those he refers to as “pure academics”; third, the group of experts, involved in the composition of the Manual; and, finally, himself in the third person. Following the construal of all these relations, what is left at the heart of the discursive map is Schmitt himself, holding the key to, not only, what we know to be the law, but what is more, to who is eligible for making these claims.

In its sixth, concluding chapter, this dissertation reflects on the implications of this research for international legal scholarship generally, and sets out an agenda for future research.

First, it calls for reflective scholarship, entailing an awareness of the effect of the knowledge practices we employ – and this applies both to doctrinal as well as critical legal scholarship. Our practices, it posits, are the same across the board, in terms of the effect they have on ‘what we know’ within our own (sub)discipline. This also entails the responsibility for reflective scholarship, and implies, inter alia, that the possibility for resistance against authority claims lies precisely in scholars’ individual contributions.

The chapter furthermore suggests two avenues for further research. First, research could be done specifically into legal knowledge construction in international humanitarian law: who exactly is involved in the production of knowledge here, and how is the knowledge produced – in particular in the form of international legal handbooks such as the Tallinn Manual – used by state legal advisers? This project would entail, first, a mapping of the affiliations of the people involved (e.g. the ICRC, Ministries of Foreign Affairs, academia), and second, interviews with state legal advisers as to how they construct or draft their legal advice.

Secondly, the chapter suggests further research should be done into knowledge production in critical legal scholarship; specifically, how ‘the other’ is constructed here. The question asked here is how this ‘other’ serves to construct, sustain, and solidify the identity of the critical researcher, as critical. After all, ‘the other’ is presumed to be – and needs to be – flawed and political in order for critical scholarship to be able to do its work. An inquiry into how this works exactly, would similarly employ the tools of precise description to scrutinize the manifestation of this “image of other” in critical legal scholarship.
The dissertation concludes with a call for more descriptive (critical) legal scholarship, with greater attention being placed on the individual contributions and participants in legal discourse. The claim made here is that many things happen that, if we do not take the trouble of looking this closely, run the risk of being overlooked. Such an approach is key to understanding what happens on the grassroots level of legal scholarship, and, moreover, to grasp how these individual contributions bring about international law as we know it.