Institution: University of Exeter		
Unit of Assessment: UoA 18 Law		
Title of case study: Improving global cybersecurity: the implementation of the Tallinn Manual 2.0 on the International Law applicable to Cyber Operations		
Period when the underpinning research was undertaken: October 2013 – April 2020		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s): Professor Michael Schmitt	**Role(s) (e.g. job title):** Professor of Public International Law	**Period(s) employed by submitting HEI:** 1 Oct 2013 to April 2020
Period when the claimed impact occurred: 2017 to April 2020		
Is this case study continued from a case study submitted in 2014? No		

1. Summary of the impact

Just as the world becomes ever-more dependent upon secure digital systems, hostile cyber operations are increasing in frequency and severity, with targets including elections, critical infrastructure and even covid-19 vaccine research. Governments have been hampered in responding to these new threats by the lack of a clear international legal framework underpinning cyber operations.

Professor Michael Schmitt's work to develop the *Tallinn Manual 2.0* in 2017 has reduced that legal uncertainty by establishing a new legal framework for cyber operations. That legal framework has shaped the practice of NATO and governments around the world as they now use the Manual and its rules daily to inform their cyber operations, their responses to those directed against them, their national cyber strategies and policies, and their stance in multilateral negotiations. Implementation of the framework and compliance with international law has been facilitated by Schmitt's training of those approving and conducting cyber operations. The upshot is that in reducing legal uncertainty, Schmitt's research has reduced the risks to the cybersecurity of nation states and their populations internationally.

2. Underpinning research

Professor Schmitt is an internationally recognized scholar specializing in international conflict and security. He was a judge advocate specializing in operational and international law for the United States Air Force for twenty years. He holds Distinguished Scholar posts at both West Point and the US Naval War College and is Senior Fellow at the NATO Cyber Defence Centre of Excellence. He was Professor of International Law at Exeter University between 2013 and 2020.

Schmitt's recent work (e.g. 3.1, 3.5, 3.6) has focused on hybrid threats (i.e. unconventional methods of intervention including disinformation, proxies and insurgencies) and grey zone conflict (i.e. interventions by states that fall below the use of force threshold). In 2013 the Tallinn Manual 1.0, directed by Schmitt, had established that international law *does* apply in cyberspace during periods of conflict, now a universally accepted conclusion. However, there was no consensus on *how* the law applied in specific circumstances, including during peacetime. The international community desperately needed to know the rules of the game in order to protect their populations and critical infrastructure against hostile operations.

The result was an entirely new project and a new text – the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [3.1]. As with the original Tallinn Manual, this was a NATO Cyber Defence Center of Excellence (NATO CCD COE) commissioned project. Schmitt again led the effort as Director and General Editor. He was supported by a global team of 19 experts representing 12 nations (including Professor Akande from Oxford University and Dr Hernandez of Durham University) with 73 peer reviewers assessing the team's conclusions. Schmitt led all sessions of the team, wrote most of the text, and revised the draft based on peer review and State input. In recognition of his specific contribution, the President of Estonia awarded Professor Schmitt the Order of the Cross of Terra Mariana for his "work in promoting cyber defence cooperation" [5.1]

The research for Tallinn 2.0 identified 154 rules of law applicable to cyber operations in practice, with extensive commentary explaining the basis for each and describing its application [3.1]. The 154 rules cover the full array of international law rules that regulate events in cyberspace and cyber operations, from peacetime legal regimes to the law of armed conflict. Some pertain to general international law, such as the principle of sovereignty and the exercise of jurisdiction; others relate to specialised regimes, including human rights law, air and space law, the law of the sea, and diplomatic and consular law.

The new research also identified aspects of international law upon which the experts could not agree. The commentary catalogues all reasonable views, thereby enabling States to assess which best reflects their national interests.

Schmitt has continued to examine unsettled issues of law identified by Tallinn 2.0. In [3.2], Schmitt proposed a policy approach to the law of cyber targeting during armed conflict that balances military necessity and humanitarian considerations; it is currently under discussion among states.

In [3.3], Schmitt & Vihul challenged the UK government's position that there is no rule of sovereignty applicable to cyberspace. Since then, every state that has publicly expressed its view (including 30 other NATO nations) has taken the Tallinn Manual 2.0 position, in part based on the analysis in [3.3].

Cyber election meddling presents unique international law challenges vis-à-vis the rules of sovereignty and intervention. Drawing on his Tallinn Manual work, Schmitt addressed the issue in [3.4] and is working with Microsoft and Oxford University to develop consensus norms on such malicious activity.

3. References to the research

3.1: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017) (Michael N. Schmitt, Project Director) https://doi.org/10.1017/9781316822524

3.2: Michael N. Schmitt, *Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations,* 101(1) International Review of the Red Cross 333-355 (2020) https://doi.org/10.1017/S1816383119000018

3.3: Michael N. Schmitt and Liis Vihul, *Respect for Sovereignty in Cyberspace,* 95 Texas Law Review 1639-1670 (2017) https://texaslawreview.org/respect-sovereignty-cyberspace/

3.4: Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International* Law, 19 Chicago Journal of International Law 30-67 (2018) https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1736&context=cjil

3.5: Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum,* 8 Harvard National Security Journal 239-282 (2017) https://harvardnsj.org/wp-content/uploads/sites/13/2017/02/Schmitt-NSJ-Vol-8.pdf

3.6: Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?,* 25 Stanford Law and Policy Review 269-99 (2014) https://law.stanford.edu/wp-content/uploads/2018/03/schmitt.pdf

4. Details of the impact

1. Creating a new legal framework for cyber operations. By identifying areas of consensus, the Tallinn Manual 2.0 established a legal framework governing cyber operations where none had existed before. The Manual sets out, for example, what legitimate measures or countermeasures a state may take in relation to hostile cyber operations on a range of areas that are critical to the functioning of democracies and economies, from conducting remote law

enforcement searches of data, to election meddling and how attacks may be conducted in cyberspace during wartime.

2. The Tallinn Manual rules have been quickly adopted by states to guide cyber operations. The legal framework established by consensus in Tallinn 2.0 has been adopted by multiple states globally as publicly available legal policies to guide cyber operations. Examples include the UK (other than on sovereignty) [5.2], the Netherlands in July 2019 [5.3], France in September 2019 [5.4] and the US in March 2020 [5.5].

Schmitt twice briefed the North Atlantic Council on cyber conflict and the law at the invitation of the NATO Secretary-General. The resulting Rules of Engagement are classified; however, the Legal Adviser to NATO confirmed that "NATO's work on cyber operations would not be the same without Professor Schmitt. This is the greatest statement of impact that I can imagine for an academic researcher" [5.7].

Tallinn Manual 2.0 also directly impacts operational cyber practices during warfare. The German and New Zealand law of armed conflict manuals, which govern their military operations on the virtual battlefield, refer directly to the Manual [5.6, 5.10]. Every rule set out is drawn from the Tallinn Manual, including those prohibiting cyber operations that affect medical care or the functionality of civilian computers.

The Legal Director of NATO confirms that the Manual has been transformative in the development of law and practice in cyber law: "it is almost impossible to overstate the impact that [Schmitt's] work on the Tallinn Manuals has had on the approach of NATO Allies and partners to the international law governing cyberspace. First, Professor Schmitt helped set the boundaries of the debate in a way that gave Allies the space and structure to begin their own thinking about these issues. Second, the positions that Professor Schmitt took, even where not adopted by Allies, helped spur States to be more explicit about their views of how international law applies to cyberspace. Major policy statements by States including Australia, France, The Netherlands, and the United Kingdom can be directly attributed to Professor Schmitt's advocacy work. This kind of impact is massive" [5.7].

Similarly, the CEO of Cyber Law International noted "It is extremely rare for an international law textbook to have such a far-reaching effect on the legal policies of nation states" [5.8].

3. Facilitating implementation of the framework and compliance with international law through training for those approving and conducting cyber operations. Government legal advisers across the world now use Tallinn 2.0 on a daily basis to identify cyber operations that clearly do not violate international law and those that unambiguously do, as well as those operations about which legal uncertainty persists. This allows States to craft lawful operations, publicly condemn those that are not and assess legal-political risks associated with cyber operations of unsettled legality.

Schmitt has played a critical role in ensuring that those charged with approving or conducting cyber operations understand and comply with the legal framework set out in Tallin 2.0. As of March 2020, about 800 governmental officials have attended 25 training courses held across four continents [5.8].

In 2018, Schmitt trained all NATO generals and admirals assigned to Headquarters on cyber law. The Tallinn based program included training on targets that cannot be the object of cyber-attacks during armed conflict, including civil defence facilities and civilian food and water supplies. [5.7]

4. Improving the cybersecurity of individual states and thereby protecting populations and economies internationally. The Legal Director of NATO stated that the Manual and Schmitt's research had directly improved the cybersecurity of NATO members: "Although I am not at

liberty to go into the details, these have led to new policy developments that help improve the cybersecurity of our Alliance" [5.7].

It is difficult to overstate the significance of improved cybersecurity in a digitally-dependent world. As the CEO of Cyber Law International noted, the legal policies shaped by Tallinn "do not only exist on paper; on the contrary, they determine the types of cyber operations countries will engage in, the effects they will pursue in cyberspace, and ultimately, how individual users, corporations and societies will be affected by nation state activities in this domain" [5.8]. This is at its starkest with Schmitt's evidence-based training for generals and admirals, with life and death consequences for civilian populations across continents.

Above all, the Manual has ushered in a new legal regime that has moved cyberspace away from an ungoverned 'Wild West'. It has extended and enhanced the rule of law internationally and offered greater protection to smaller states dependent upon the protection offered by international law. As the Dutch Minister of Foreign Affairs emphasized, "[t]he Tallinn Manual reduces ambiguity and uncertainty. It reduces malicious actors' room for manoeuvre. The manual shows that cyberspace is not simply a jungle, where the strong do what they want and the weak suffer what they must" [5.9].

5. Sources to corroborate the impact

5.1 Order of the Cross of Terra Mariana: awarded for Schmitt's "work in promoting cyber defence cooperation"
https://web.archive.org/web/20201120112627/https://www.president.ee/en/estonia/decorations/bearer/19560/michael-n-schmitt

5.2 Speech at Chatham House by UK Attorney General, 23rd May 2018:
https://web.archive.org/web/20201120112810/https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

5.3 Dutch Ministry of Foreign Affairs Letter to Parliament (2019) (copy on file)
https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/05/kamerbrief-over-internationale-rechtsorde-in-het-digitale-domein

5.4 France, International Law Applied to Cyberspace (2019) (copy on file)
https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf

5.5 United States Department of Defense General Counsel (2020):
https://web.archive.org/web/20201120113246/https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

5.6 German Law of Armed Conflict Manual:
https://web.archive.org/web/20201123080011/https://usnwc.libguides.com/ld.php?content_id=5616055

5.7 Letter from Legal Adviser and Director, Office of Legal Affairs, NATO (copy on file)

5.8 Letter from CEO of Cyber Law International (copy on file)

5.9 Netherlands Minister of Foreign Affairs Speech, 20th June 2018:
https://web.archive.org/web/20201123080328/https://www.government.nl/documents/speeches/2018/06/20/speech-by-minister-blok-on-first-anniversary-tallinn-manual-2.0

5.10 New Zealand, Manual of Armed Forces Law:
https://web.archive.org/web/20201123080113/https://usnwc.libguides.com/ld.php?content_id=47364407