Word Count: 11 994 Student Number: 630031027

State Responsibility: Tests of Attribution Applied in Cyberspace

1. Abstract

This dissertation will consider whether the Effective Control test for attribution of malicious conduct of an Entity to a State is too strict a test of attribution for Entities operating in cyberspace. Attribution under Article 8 and Article 4 of the International Law Commission's Draft Articles on State Responsibility is infamously problematic as the tests of Instructions and Control demand satisfaction of an exceptionally high evidential burden. Indeed, some authors have asserted the nature of cyberspace makes it so easy for States to evade their responsibility by setting up proxy cyber armies that alternative tests should be applied instead. The three main chapters of this dissertation will focus on the Entities rumoured to be conducting cyber attacks on behalf of States, and the extent to which each contemporary test of attribution can tackle these situations. In this context, the dissertation will argue that while the tests are indeed extraordinarily difficult to apply in cyberspace, there is nothing specific about the Entities, or their conduct, that would merit derogation from the test of Effective Control.

2. Table of Contents

3. Acknowledgements

I wish to express my sincere thanks to Dr. Kubo Mačák, my dissertation supervisor, for all the feedback and support he has provided me with.

I am also grateful to my family, Anastasia Vrublevská and my friends, for supporting me throughout my degree.

4. Introduction

The Draft Article on the Responsibility of States for Internationally Wrongful Acts, formulates the international law concerning State Responsibility for internationally wrongful acts.[1] Two articles in particular are interesting for the purposes of attributing cyber-attacks. Article 4, because it covers both the conduct of the *de jure* as well as the *de facto* organs of a State,[2] and Article 8, which covers the conduct of the Entities under the instructions, the directions or control of a State.[3] Both Articles provide an exception to the general rule under which the conduct of a non-State Entity is not attributable to a State.[4]

The attribution under Article 8[5] has always been a contentious area of academic discourse.[6] Not only is the number of tests under the Article contended,[7] but also much of their contents lack clarity. Such confusion is amplified in the context of cyberspace, where some authors asserted the circumstances are so different from traditional spaces of land, air and sea,

[1] James Crawford, *The International Law Commission's Articles on State Responsibility* (Cambridge University Press 2002).
[2] ibid, 94.
[3] ibid, 110.
[4] ibid.
[5] ibid.
[6] Scott J. Shackelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem" (2010) 42(4) GJIL 971, 984; Antonio Cassese, "The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia" (2007) 18(4) EJIL 649, 652; Marco Roscini, "World Wide Warfare – Jus ad bellum and the use of Cyber Force" (2010) 14 YBUNL 85, 96.
[7] Stefan Talmon, "The Responsibility of Outside Powers for Acts of Secessionist Entities" (2009) 58(3) ILQ 493, 493.

that cyber merits different tests of attribution.[8] While the Tallinn Manual considered the law contained in the ILC draft articles applicable in cyberspace without a change,[9] the question remains as to whether the conduct of cyber attacks demands amendments to the existing tests, and what those potential amendments should be. Despite these wide-ranging uncertainties, the discussion has so far been mostly limited to the question of whether the Effective Control test[10] or the Overall Control test[11] should be used to attribute conduct of non-State Entities.[12] While Article 8 considers three circumstances in which attribution of the conduct can arise, the instructions, control and directions,[13] such a limited view of the Effective Control test is insufficient in determining whether the tests are too strict to be usable. This dissertation will evaluate the strictness of the Effective Control test not only in the context of its fellow tests of control, including the Strict Control test[14] under Article 4[15] but also its fellow tests of attribution under Article 8. In each chapter, the test for attribution will be first established and then applied to an example of a cyber attack to examine the scope and limits of each legal test.

[8] Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility" (2013) 14(2) MJIL 496, 501. See also Shackelford, "State Responsibility for Cyber Attacks" (n 6) 987; Roscini, *"World Wide Warfare"* (2010) (n 6) 100.
[9] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 29.
[10] *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America) (Merits) [1986] ICJ Rep 14, [115].
[11] *Prosecutor v. Duško Tadić* (Judgment of the Appeals Chamber) ICTY-99-IT-94-1-A (15 July 1999), [137].
[12] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 987; Roscini, "World Wide Warfare" (n 6) 100.
[13] Crawford, *Articles on State Responsibility* (n 1) 110.
[14] *Nicaragua* (n 10) [110].
[15] Crawford, *Articles on State Responsibility* (n 1) 94.

There are three layers of State interference at which the tests of attribution operate, corresponding to the three tests of attribution and the three main chapters of this dissertation. The fifth chapter of the dissertation focuses on the test of Instructions. In this chapter it is argued that while the test of Instructions is a workable test in cyberspace for attribution of the Distributed Denial of Service (DDoS) attacks, with the use of botnets and more complex attacks it is unlikely States will instruct citizens to conduct DDoS attacks on their behalf.

The sixth chapter focuses on the test of Strict Control and submits that despite what the court in Tadic[16] argued, the Overall Control test is competing with the Strict Control test rather than the Effective Control test.[17] It will be argued the legally sound test is the Strict Control test. Finally, the chapter submits that while the Strict Control test is difficult to satisfy with regards to cyber attacks, the Overall Control test would not make the attribution any easier as it still demands evidence of an exercise of control.[18]

In the seventh chapter, it is argued, the Effective Control test is unsuitable not only for attribution of cyber attacks but any attack due to its focus on control during an operation, particularly when evidence is extremely difficult to discover. It is also submitted the third way of attribution under Article 8, Directions,[19] cannot be constructed without infringing on the already established tests of Instructions, Strict Control and Effective Control.

---

[16] *Tadić* (n 11) [124].
[17] Talmon (n 7) 506.
[18] Prosecutor v Kordic and Cerkez (Judgment) ICTY-95-14/2-A (17 December 2004), [361].
[19] Crawford, *Articles on State Responsibility* (n 1) 110.

5. Attribution under the Instructions

Instructions are the first circumstance in which attribution of the conduct of non-State actors is permitted under Article 8.[20] The test for Instructions and its possible application in the cases of international political DDoS attacks will be considered in this chapter. There are two changes in State practice of a particular relevance to the test of Instructions. First, the change of State attitude towards DDoS attacks between the early 2001 attacks on USA[21] and 2007 attacks on Estonia.[22] Second, the development in complexity of such attacks between 2001 and 2015. This chapter will look at whether the contemporary DDoS attacks could, in light of these developments, still engage with Article 8 or whether such attack would merit a change of the existing test instead.

a. Test for Instructions

In the case of instructions, a State is responsible for wrongful conduct if it instructs an Entity to act in a way that breaches the primary rules of the international law.[23] The Article is engaged when an Entity is recruited or instigated as an auxiliary of a State and operates under the State

[20] Crawford, *Articles on State Responsibility* (n 1) 110.
[21] Josef Nazario, "Politically Motivated Denial of Service Attacks" in Christian Czosseck and Kenneth Geers (eds), *The Virtual Battlefied: Perspectives on Cyber Warfare* (IOS Press 2009), 165.
[22] ibid.
[23] ibid.

instructions. At that point it is no longer the Entity but the State who is responsible for the wrongful conduct.[24]

However as both Crawford and Tonkin observe, problems arise in the application of this test.[25] In the Genocide case, the court stated in an attempt to clarify the situation, that the instructions must be given in respect of each operation in which alleged violation occurs, not generally in respect of the overall actions taken by the Entity having committed the violations.[26] Tonkin raises two questions; how narrow is the definition of an operation and how specific the instructions must be.[27] She imagines a gray zone *"where a State gave overly vague or ambiguous instructions which, although not unlawful on their face, conveyed a lack of concern as to how the instructions were carried out and which could even be interpreted as implicitly authorizing a violation"*.[28] In light of the Bosnian Genocide case,[29] however such situation would probably fail to satisfy the criteria of Instructions because the authorization would be of an overall character, thereby clearing the State of responsibility for the instructions under the Article. Crawford takes a more substantive approach to such grey zones. In his view, the action of an Entity is either incidental to the mission and thus falls under the scenario of instructions, or goes beyond the mission's scope and falls outside of the

[24] Hannah Tonkin, *State Control over Private Military and Security Companies in Armed Conflict* (Cambridge University Press 2011) 114.
[25] ibid; James Crawford, *State Responsibility: The General Part* (Cambridge University Press 2013) 145.
[26] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Judgement) [2007] ICJ Rep 43, [400].
[27] Tonkin (n 24) 114.
[28] ibid, 115.
[29] *Bosnian Genocide* (n 26) [400].

scope of instructions.[30] As Crawford states, the distinction between the instructions and control is that the former is testing the existence of instructions for a free agent and latter the sufficient level of control over the agent.[31]

The test for Instruction could be formulated in this way:

1. *The State must give instructions to the Entity.*
2. *The instructions must be given in respect of an operation during which the alleged breach of primary rules of international law occurs.*
3. *The breach must be the direct result of the instructions or at least incidental to the fulfilment of these instructions.*

b. Instructing Cyber Attacks

Commentators have sometimes ignored instructions when discussing attribution of cyber-attacks.[32] At first sight, because cyber operations are often conducted covertly and States do not openly authorize the conduct of the Entities they instruct,[33] this omission seems reasonable. However, in the case where the State would actually issue instructions, the test to satisfy is not as strict as the tests in the following chapters. For example, there is no

[30] Crawford, *State Responsibility* (n 25) 146.
[31] ibid.
[32] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 984. Roscini, "World Wide Warfare" (n 6) 101.
[33] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 90.

need for dependency or control to be weighed and identified, nor do the instructions need to be enforced.[34]

In the case of paramilitary operations, it seems unlikely the State would blatantly instruct the Entity to breach IHL, or at least such instruction could be easily hidden from the official documents in practice.[35] Moreover, it seems even less likely that in a top secret cyber operation such as Stuxnet,[36] aimed at slowing down the Iraqi nuclear program by covertly destroying the reactor centrifuges,[37] the State would leave evidence of instructions. However, cyber attacks come in so many different shapes and sizes that there is, at least, one situation that deserves closer attention.[38] The instructions and toolkits used to facilitate the DDoS attacks in the late 2000s seem to fit well within the scope of the Instructions.[39] The Tallinn Manual goes as far as to allude to these circumstances when it mentions that: *"reportedly the States have called upon private citizens to conduct cyber operations against other States or targets aboard*".[40]

The DDoS attacks are on the opposite side of Stuxnet in terms of complexity and thus are perfectly suitable for such cyber operation. On the one hand, there are powerful cyber weapons such as Stuxnet, but these require specific

[34] Crawford, *Articles on State Responsibility* (n 1) 110.
[35] Tonkin (n 24) 114.
[36] European Union Agency for Network and Information Security, "Stuxnet Analysis" (7 October 2010) <https://www.enisa.europa.eu/media/press-releases/stuxnet-analysis> accessed 27 April 2016
[37] ibid.
[38] UK Government Communications Headquarters "Common Cyber Attacks: Reducing the Impact" (19 February 2016) <*https://www.cesg.gov.uk/white-papers/common-cyber-attacks-reducing-impact*> accessed 27 April 2016
[39] Nazario (n 21) 165.
[40] Schmitt (n 9) 32.

targeting and substantial support to be created.[41] Thomas Rid explains such a cyber weapon as Stuxnet is *"a highly sophisticated rocket that can only be fired against one single target and at nothing else, even if some of its components may be reused".*[42] They are developed in secrecy as they exploit newly discovered vulnerabilities in the systems they target, so-called zero-day vulnerabilities.[43] Given the secrecy of execution is the main appeal of such attack, compared to traditional attack with a similar effect, it seems very unlikely that a State would openly admit to using them.[44] There are also DDoS attacks in which anyone with a computer and internet connection can participate.[45] The more participating computers, the more effective the attack, thus rendering instruction to citizens to join the attack appealing. The strength of such attacks is the ease with which they can be conducted.[46]

DDoS attacks first appeared in the summer of 1999 as a new breed of the Denial of Service (DoS) attack. The aim of traditional DoS attacks is to overflow the targeted system with requests, exhausting its ability to handle them and therefore rendering it unresponsive.[47] The DDoS attack uses the same method but distributes the source of the attack across multiple machines and locations which are remotely controlled by a single client.[48]

---

[41] Thomas Rid, "Cyber War Will Not Take Place" (2012) 35(1) JSS 5, 28.
[42] ibid.
[43] Liam O. Murchu, "Stuxnet Using Three Additional Zero-Day Vulnerabilities" (14 September 2010) <http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities> accessed 27 April 2016
[44] Lech Janczewski (ed.), *Cyber Warfare and Cyber Terrorism* (Idea Group Publishing 2007) 109.
[45] Nazario (n 21) 165.
[46] James Graham and others, *Cyber Fraud: Tactics, Techniques and Procedures* (Auerbach Publications 2009) 303.
[47] ibid.
[48] Stefanie Hoffman, "DDoS a Brief History" (25 March 2013) <https://blog.fortinet.com/post/ddos-a-brief-history> accessed 27 April 2016

DDoS attacks are nowadays conducted through toolkits; a few of these early toolkits included Trin00, Tribe Flood Network and Stacheldraht, a software designed to help the user to attack with less original code or even none at all.[49] The toolkits have been rapidly modified for political purposes and have begun to be used in international conflicts.[50]

By 2001, the first DDoS attack had been used in an international dispute between China and the US.[51] The dispute itself started with a crash between a US Navy spy plane and a Chinese fighter plane off the coast of China.[52] The Chinese plane and its pilot were lost, while the US Navy plane and its crew were detained on the Hainan Island where they had to make an emergency landing.[53] During this period of strained relations between the US and China, DDoS attacks targeting US military Internet sites took place.[54] Toolkits to attack US websites were distributed online through internet forums so that individual hackers could join in.[55] The US reaction to this was surprisingly tame. The National Infrastructure Protection Center have analyzed this and a number of other incidents leading to 2001 as forms of hacktivism and the proponents of it as pro-government groups.[56] Even the press, while using bombastic headlines forecasting cyberwar, did not

[49] Jelena Mirkovic, Peter Reiher, "A Taxonomy of DDoS attack and DDoS Defense Mechanisms" (2004) 34(2) ACM SIGCOMM Computer Communication Review 39, 40.
[50] Shweta Tripathi and others, "Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks" (2013) 4(3) Journal of Information Security 150, 164.
[51] Nazario (n 21) 165.
[52] ibid.
[53] ibid.
[54] ibid.
[55] Roscini, "World Wide Warfare" (n 6) 101.
[56] National Infrastructure Protection Center, "Cyber Protests: The Threat to the U.S. Information Infrastructure" (October 2001) <http://www.au.af.mil/au/awc/awcgate/nipc/cyberprotests.pdf> accessed 27 April 2016

speculate as to the connection between the hackers and the government.[57] This attitude changed completely after the attacks on Estonia in 2007.[58] Just as China had done 6 years earlier, the attackers recruited help through internet forums, providing the tools and instructions necessary to facilitate the attack.[59] However, this time, the attacks were of a much larger magnitude and scale and Estonia accused Russia of being responsible for the attacks.[60] In these circumstances, the Article could theoretically be engaged to establish the responsibility.

The instructions provided in the attacks above have been confused with mere incitement yet there are two ways in which we can distinguish instructions under the Article from mere incitement. Despite Roscini's analysis of the Chinese attacks in 2001 and the 2008 attacks on Georgia during the Russo-Georgian war,[61] these attacks could fall under the Instructions. Roscini imagines the State agents *"offered instructions to hackers on how to incapacitate United States government computers",* but concludes this would only amount to an incitement, which is not covered by the Article.[62] This seems unsubstantiated. Incitement is defined by the Oxford Dictionary as *"the action of provoking unlawful behavior or urging someone*

[57] Sarah Left, "Chinese and American hackers declare 'cyberwar'" (4 May 2001) <http://www.theguardian.com/technology/2001/may/04/china.internationalnews> accessed 27 April 2016
[58] Nazario (n 21) 165.
[59] Nazario (n 21) 165.
[60] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia" (17 May 2007) <http://www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 27 April 2016
[61] Nazario (n 21) 165.
[62] Roscini, "World Wide Warfare" (n 6), 101.

to behave unlawfully",[63] whereas instructions are defined as *"a direction or order".*[64] While mere incitement is focused on changing someone's mind, instructions are concerned on the issue of guidance. Although there is no notion of incitement in the law of attribution, there is a practice of direct and public incitement to genocide in the international law.[65] However, it seems that incitement, like its dictionary definition, is applicable in situations where masses or individuals are encouraged to act against individuals or groups by means of propaganda, or other forms of persuasion affecting their mental state. Despite the political agenda behind both of the 2001 and 2008 attacks, the instructions went beyond incitement in two major respects. Firstly, the instructions did not aim to sway the mind of the attackers, but simply gave a guide to achieving a predetermined outcome, and secondly, the instructions were very precise in who, when and how the prospective attackers are to target, resembling a plan of an operation rather than an argument for undertaking the operation itself.[66] We can distinguish the incitement from the instructions on Tonkin's example of private military and security companies (PMSC's). Incitement would be persuading the PMSC's to work for the State, most likely by paying for its services. This on its own is not covered by the Article. In the case of the hackers, this would be creating what we can assume to be the nationalistic feeling that led them to the attacks. But, chronologically-speaking, instructions come later to cause the already

[63] *'incitement'* (Oxford Dictionaries online) <oxforddictionaries.com/us/definition/american_english/incitement> accessed 1 February 2016
[64] *'instructions'* (Oxford Dictionaries online) <oxforddictionaries.com/us/definition/american_english/incitement> accessed 1 February 2016
[65] Wibke K. Timmermann, "Incitement in International Criminal Law" (2006) 88 IRRC 823, 831.
[66] Nazario (n 21) 165.

persuaded Entity to act. Or, as the Manual itself states, acts of hacktivists who are merely encouraged by the State does not amount to an attribution; an attribution is only engaged if instructions are issued.[67]

Providing weapons necessary for an attack and instructions on how to use them and on whom, do therefore go well beyond the scope of incitement, and they do satisfy the test of Instructions above, at least in the case of Estonia in 2007.[68] Instructions were given thorough internet forums (1) in respect of an operation to attack websites of the government and significant private industries in Estonia (2) and the results, defacements and crashes of the websites were incidental to the instructions (3). Surely if there would be a proof of a State posting instructions for attack and the targets online, the State would be held responsible for such attacks. There is no requirement for the State to instruct a specific Entity,[69] indeed with the advent of the internet such a requirement would significantly limit attribution of simple cyber weapons such as DDoS attacks. Both States have also considered the possibility of attribution for these instructions without a single direct recipient. The Estonian Prime Minister accused the Russian government of being responsible for the attacks,[70] and the Russian officials responded that *"it's a serious allegation that has to be substantiated"*.[71] Virtually the same circumstances arose after the Georgia Cyber attacks in 2008. NATO Cooperative Cyber Defence Center of Excellence in its report concluded that

[67] Schmitt (n 9) 33.
[68] Nazario (n 21) 165.
[69] Schmitt (n 9) 29.
[70] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia" (17 May 2007) <http://www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 27 April 2016
[71] ibid.

no evidence was found of Russian officials posting instructions online, *"be it because there was none, because the collection efforts were not far-reaching or deep enough to identify these connections, or because involvement by state organisations was conducted in a way to purposefully avoid attribution",*[72] and so indirectly acknowledged the possibility of attribution if appropriate evidence should become available.

The attack on Estonia is an important milestone in two ways. First, instead of labeling the attacks as works of pro-State hacktivists (a State practice in the late nineties and early 2000's), Estonia has started the practice of seeking responsibility of the State from which the cyber attack originated. If the evidence had linked State officials with the instructions on Russian forums, this would most likely have been enough to attribute responsibility for at least a portion of the attacks to Russia. Second, the technology enabling participation in a DDoS attack has begun to liberalize, so that the average user could join in an attack. Since Estonia, many political DDoS attacks have taken place with software becoming increasingly simple to use.[73] The attacks from China on CNN even used a tool with only two buttons, *"Attack"* and *"Stop",* so that truly anyone willing could join.[74] According to the Manual, provision of hacking tools is not enough to establish control over the individual or the Entity, nor does it amount to instructions.[75] Yet a weapon of such predetermined purpose and simplicity to use would be an area in which the Tallinn Manual could perhaps expand the traditional rules of attribution

[72] Eneken Tikk, Kadri Kaska, Liis Vihul, *International Cyber Incidents: Legal Considerations* (CCD COE 2010) 75.
[73] Nazario (n 21) 165.
[74] ibid.
[75] Schmitt (n 9) 34.

adopted from ILC.

The toolkits have developed their capacity to cause damage and have lost the need for support from the public since 2001, given their increase in complexity. In the recent attack on Ukraine, the BlackEnergy toolkit, which has been developed since 2007,[76] has caused a blackout in Ivano-Frankivsk region of the country by attacking SCADA industrial control systems.[77] Unlike the early attacks on Estonia or Georgia, there were no instructions posted on the forums or easy to use tools distributed to the masses. It seems the attackers used botnets, large groups of enslaved computers, to orchestrate DDoS attacks instead of depending on patriotic nationals.[78] Although the group Anonymous notably still uses cyber volunteers,[79] with botnets becoming more sophisticated each year, the patriotic hacker seem to have lost her prominence *vis-à-vis* international cyber attacks.[80] However, it is easy to imagine a situation in which the new powerful toolkits such as BlackEnergy could become adapted for greater simplicity, making the test of Instructions relevant once more.

In conclusion, attribution under Instructions during the early days of cyber attacks would be possible. Although attributing acts of such attack was

[76] Rene Millman, "'Russian' DarkEnergy malware strikes at Ukrainian media and energy firms" (4 January 2016) <http://www.scmagazineuk.com/russian-darkenergy-malware-strikes-at-ukrainian-media-and-energy-firms/article/462778/> accessed 27 April 2016
[77] Hannah Kuchler, Neil Buckley, "Hackers shut down Ukraine power grid" (5 January 2016) <http://www.ft.com/cms/s/0/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.html#axzz3zmZD2bFJ> accessed 27 April 2016
[78] Robert Lipovsky, "BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry" (4 January 2016) <http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/> accessed 27 April 2016
[79] Sophie Curtis, "Anonymous recruits amateurs in cyber war against Isil" (18 November 2015) <http://www.telegraph.co.uk/technology/internet-security/12004025/Anonymous-recruits-amateurs-into-cyber-war-against-Isil.html> accessed 27 April 2016
[80] Imperva Cyber Security Blog, "The rise of DDoS Botnets" (2 April 2014) <http://blog.imperva.com/2014/04/the-rise-of-ddos-botnets.html> accessed 27 April 2016

unthinkable in 2001, with the predominant attitude among the States at the time being that such attacks are only conducted by hacktivists, this has changed dramatically in 2007 when the possible impact of such attacks was foreshadowed by the DDoS attacks on Estonia. However, the attacks have increased in complexity in recent years. It is unlikely a State would instruct its citizens to initiate a modern DDoS attack. Unless there are new toolkits designed for simplicity, or the ability of States to collect evidence on the communication of other States with hacker groups to discover instructions outside of the circumstances outlined above, is not improved, it is unlikely that Instructions will be discovered and used for attribution any time soon.

6. Attribution under the Strict Control test

The second set of circumstances under which attribution of the conduct of non-State actors under Article 8 is permitted are those of control. There are two tests of control established in the Nicaragua judgment,[81] each focusing on a different level of control. The famous test of Effective Control is formulated in paragraphs 109 and 110 of the judgment and focuses on control over actions during an operation.[82] The second, lesser known test, either called the Strict Control, the Complete Dependence or simply the Agency test,[83] is formulated in paragraph 115 and focuses on the control over the entire conduct of an Entity.[84] There is also another standard of control contained in the Tadic case,[85] the Overall Control test, which is often interpreted as challenging the Effective Control test.[86] The tests of Strict Control and Overall Control will be considered in this chapter, demonstrating firstly that the Overall Control test is challenging the Strict Control test, instead of the Effective Control test, and secondly that the Overall Control test, contrary to popular belief,[87] does not make the attribution easier to achieve. The test of Effective Control will be considered separately in the next chapter, as it is a subsidiary test applied when the Strict Control test is

[81] Talmon (n 7) 497.
[82] *Nicaragua* (n 10) [110].
[83] Talmon (n 7) 498.
[84] *Nicaragua* (n 10) [115].
[85] *Tadić* (n 11) [122].
[86] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 987; Roscini, "World Wide Warfare" (n 6) 100.
[87] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 987; Roscini, "World Wide Warfare" (n 6) 100.

not satisfied and demands control over the individual decisions of the Entity instead of its overall behavior.[88]

a. Strict Control test

To equate the Entity with an organ of a State the court will search for a relationship between the Entity and the State that is one of *"dependence on the one side and control on the other"*.[89] If the court finds such a relationship, the Entity, as the court in Bosnian Genocide concluded,[90] will become a *de facto* organ of the State under Article 4 and its conduct therefore becomes attributable to the State.[91] This development of Article 4 is stretching its original formulation significantly and the courts demand an exceptional situation with a proof of *"complete dependence"* and a *"particularly great degree"* of control to allow the attribution under the Strict Control test.[92] Although outside of the scope of Article 8, the attribution under the Strict Control test is relevant to cyber attacks for two reasons. Firstly, commentators often conflate the tests of Effective Control and Strict Control,[93] which hence calls for greater clarity in the application of each respective test. Secondly, the organized groups that the States allegedly use for attacks in cyberspace do in some cases seem strongly connected with the State over substantive periods of time,[94] indeed there seems to be a

[88] Talmon (n 7) 502.
[89] *Nicaragua* (n 10) [109].
[90] *Bosnian Genocide* (n 26) [393].
[91] Crawford, *Articles on State Responsibility* (n 1) 94.
[92] *Bosnian Genocide* (n 26) [393].
[93] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 987; Roscini, "World Wide Warfare" (n 6) 100.
[94] Frederic Lemieux, *Current and Emerging Trends in Cyber Operations; Strategy and Practice* (Palgrave Macmillan 2015) 105.

rising practice of creating, supporting and integrating cyber Entities by States.[95] As we have seen in the chapter above, the evidence of instructions from the State for the acts of such Entities or instructions for civilians are unlikely to be found. The attribution under the Strict Control test even extends to the acts of the Entity which were not authorized by the State.[96] As such the Strict Control is a particularly attractive tool for attribution of cyber attacks.

Perhaps the clearest formulation of the Strict Control test comes from Stefan Talmon. He formulates the Strict Control test in three steps:[97]

(1) The Entity must be completely dependent on the outside power.
(2) This complete dependence must extend to all fields of activity of the Entity.
(3) The outside power must actually have made use of the potential for control inherent in that complete dependence, ie. it must have actually exercised a particularly high degree of control.

Regarding the first step, there seems to be three main ways of inferring complete dependence. Firstly, the ICJ suggested in Nicaragua that if the State conceived, created and organized the Entity, then it creates a strong presumption of the Entity being completely dependent on it.[98] Secondly, if the assistance provided by the State is such that the Entity can't conduct its

[95] ibid, 99.
[96] Talmon (n 7) 501.
[97] ibid.
[98] ibid.

activities without the support of the State, to the extend that cessation of this support would terminate the activity of the Entity, then this suggests such dependence.[99] And thirdly, if the Entity is completely integrated into the administrative, military, educational, transportation and communication systems of the State, it will become annexed by the State and thus signify complete dependence.[100] This integration must not be legal, otherwise the Entity will simply be a *de jure* organ of the State.[101] Unfortunately the precise extent to which the presumption of complete dependence is sufficient to satisfy the first point is not clear from Talmon's article. The court in Nicaragua clearly demands complete, not partial, dependence; presuming dependence as complete seems easily satisfied, diluting the test. On a closer inspection however, all three ways of inferring complete dependence are merely creating only a presumption of complete dependence as this presumption is tested, when the dependence is exercised,[102] by the third step of the Strict Control test itself.

As for the second step, the complete dependence must also be shown to extend to all or the great majority of the Entity's activities.[103] The fact that only the most crucial activities are conducted under the complete dependence is not enough.[104] Unlike the Effective Control test, the entire conduct of the Entity is attributable to the State and therefore the dependence must extend

[99] ibid.
[100] ibid.
[101] Crawford, *Articles on State Responsibility* (n 1) 94.
[102] *Nicaragua* (n 10) [110].
[103] Talmon (n 7) 501.
[104] ibid, 498.

to at least the majority of its conduct.[105] However, as we will see below, each individual act of the Entity does not have to be controlled by the State. If the State created or annexed the Entity, the complete dependence will most likely be reaching over the entire conduct of the Entity. The only situation where the second step seems relevant is therefore when the support is provided by the State, after the Entity already came into existence, to such an extent that the Entity cannot conduct its activities without such support. The complete dependence inherent in this support must extend not only to a particular act but to at least a majority of the activities. This is one of the reasons attribution failed in Nicaragua, the proof of such extent of control was never established.[106]

We can go beyond Talmon's analysis; the Entity does not seem to have to be under the complete dependence for the entire duration of its existence. The court in Nicaragua established that although the Entity was not completely dependent on the State in its later years, it was so during the initial years at least. The court proceeded to attempt the attribution at least for these initial years.[107] It seems logical, then, that the extent of the complete dependence over the majority of the activities should not need to be present for the entire duration of the complete dependence. For the attribution to take place the two just need to exist simultaneously at any point during the Entities operation. Of course, it will then only be during that specific point of the conflict that the conduct of the Entity will be attributable to the State.

[105] *Nicaragua* (n 10) [109].
[106] ibid.
[107] ibid, [111].

Thirdly, the State must have *"made the use of the potential for control inherent in that complete dependence".*[108] This burden is both difficult to satisfy and difficult to underpin. For the use of the potential, Talmon argues *"the outside power must have wholly devised the strategy and tactics of the entity"* to exercise the control sufficiently.[109] Evidently, this is a great burden to satisfy. Yet, this must be distinguished from the requirement of the Effective Control test.[110] For Strict Control, it is only important that such control is exercised in general.[111] This is confusing particularly because of the terminology used. While the scope of the control must only be general and not in respect of each incident so that *"the state would accordingly be responsible for any acts committed by such a group, even if a specific act was committed ultra vires or against explicit instructions"*[112] the intensity of the control must be according to Talmon of a particularly high degree.[113] For example, it would not suffice to merely provide advisers, discuss strategy and tactics or *"provide funds coinciding with the launch of a new offensive or a certain activity".*[114] The confusion between the two concepts is not a new phenomenon. Griebel and Plücken have argued that the test of Strict Control would be hard to satisfy without the Entity in question being simultaneously under Effective Control under this same confusion.[115] Milanovic disproved

[108] ibid, [110].
[109] Talmon (n 7) 500.
[110] ibid, 501.
[111] Marko Milanovic, "State Responsibility for Genocide" (2006) 17(3) EJIL 553, 577.
[112] ibid.
[113] ibid.
[114] Talmon (n 7) 501.
[115] Marko Milanovic "State Responsibility for Acts of Non-State Actors: A Comment on Griebel and Plucken" (2009) 22(2) LJIL 307, 315.

this fallacy by distinguishing between the focus of each test.[116] The Strict Control test, unlike the Effective Control test, does not require control over each individual action of an Entity. The exercise of the potential control can be only over the general behavior of the Entity and is therefore at least in this respect less demanding than the Effective Control test. For example, if a State devises the strategy and tactics of the majority of missions of the Entity, it would most likely satisfy the requirement of the exercise of control. However, the same level of control would most likely not satisfy the Effective Control test as the State would lack sufficient control during each individual attack.

The intensity with which the control over the Entity needs to be exercised is nonetheless open to interpretation. On the one hand, Talmon suggests the very strict requirement; *"wholly devised strategy and tactics".*[117] Conversely, Milanovic, on the other hand, suggests the degree of control must be qualitatively only the same as the control a State exercises over its own organs, forces or territory.[118] This represents a less burdensome requirement since States do in fact exercise less control than that which Talmon suggests is necessary. Article 4, for example, considers that institutions are attributable *"even if regarded in internal law as autonomous and independent of the executive government"*.[119] Given that States seem to confer a lot of discretion to their own organs, why should Entities be subjected to the higher level of control than ordinary organs of the State? While Talmon's test

[116] ibid, 317.
[117] Talmon (n 7) 500.
[118] Milanovic, "State Responsibility for Genocide" (n 111) 577.
[119] Crawford, *Articles on State Responsibility* (n 1) 94.

definitely reaches the level of control necessary, it might go beyond what the courts intended.

It seems Milanovic's interpretation is preferable. The demand of strong dependence does not mandate the requirement of high control. The Strict Control test is predominantly focused on the dependence of an Entity. While Talmon borrows the line *"wholly devised strategy and tactics"*[120] from Nicaragua itself, the court does conclude that such control is not present before even beginning to consider the Strict Control test.[121] The court seems instead to be contemplating a test which does find the State responsible for the conduct of an Entity while not wholly devising the strategy and tactics. The court does imagine the possibility of an exercise of a control through the cessation of aid, which would be a much lower requirement to satisfy than wholly deciding the strategy, as contemplated by Talmon.[122] The focus here is again on necessary dependence rather than control. With regards to the level of control to satisfy the dependence and control relationship, the court in Nicaragua actually only states that whether the State devised the strategy of the Entity depends on *"the extent to which the State made use of the potential for control inherent in that dependence".*[123] The text in Nicaragua seems to suggest there is particular potential for control created by the complete dependence and that such potential needs to be exercised with regards to some unspecified, level as a proof of the control. Although the court in the Bosnian Genocide says it demands a particularly high degree of

[120] *Nicaragua* (n 10) [108].
[121] ibid.
[122] ibid, [110].
[123] ibid, [110].

control, it equates that level of control with the relationship of complete dependence:

"… However, so to equate persons or entities with State organs…requires proof of a particularly great degree of State control over them, a relationship which the Court's [Nicaragua] Judgment quoted above expressly described as "complete dependence"."[124]

It seems that this high level of control is created by the state of *"complete dependence"* and there certainly must be proof of such dependence. However, the exercise of such control is a separate burden from the high level of control inherent in complete dependence, and it does not have to be of a great degree.

If the Strict Control test is to be read as a test for attribution under Article 4, the exercise of control necessary to satisfy the third part of the test should be established in line with the Article's own interpretation of the State organ. The Article seeks to find, in the absence of a formal status under the municipal law, attribution on the *"basis of the role that they in fact perform within the structure of the State".*[125] The Article also states that *"in some systems the status and functions of various entities are determined not only by law but also by practice"*.[126] It should be the State practice in each case that we seek in determining whether sufficient control has been exercised,

[124] *Bosnian Genocide* (n 26) [393].
[125] Crawford, *Articles on State Responsibility* (n 1) 94.
[126] ibid.

rather than a universal burden of complete decision on the strategy and tactics. Both Article 4,[127] the court in Nicaragua[128] and the Bosnian Genocide judgment,[129] have left the exercise of control by the State over the Entity to be determined on a case by case basis. Talmon is wrong in suggesting that the third step of the Strict Control test can only be satisfied by *"strategy and tactics* wholly devised" by the State.[130] Complete dependence on one hand does not necessitate complete control on the other. Rather, as Milanovic suggests, the Entity should be controlled to the same standard any other organ of the State would be. Perhaps the preferable name for the test should be the Complete dependence test, as the level of dependence, rather than control, is its crucial ingredient.

b. Overall Control test

The Overall Control test has been developed in the Tadic case to cover attribution of conduct of organized and hierarchically structured groups. It is mistakenly understood by some commentators as an alternative to the Effective Control test.[131] This confusion is understandable as the Appeals Chamber in the Tadic judgement itself has constructed the test in this way under the belief the Effective Control test is the only test created in Nicaragua.[132] Unknowingly, as Talmon and Milanovic concluded, the court in

[127] ibid.
[128] *Nicaragua* (n 10) [110].
[129] *Bosnian Genocide* (n 26) [393].
[130] Talmon (n 7) 500.
[131] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 988; Roscini, "World Wide Warfare" (n 6) 100.
[132] *Tadić* (n 11) [124].

Tadic has offered an alternative not to the Effective Control test, but to the Strict Control test of Nicaragua.[133] The Appeals Chamber created the Overall Control test by misreading Nicaragua and conflating its two tests into one.[134] Since the two tests in Nicaragua were confirmed in the Bosnian Genocide case,[135] the initial mistake is now beyond any doubt. Talmon identifies the test as insufficient in the context of Article 4, lacking the requirement of complete dependence from the Strict Control test.[136]

There are two grounds on which the Appeals Chamber found the Nicaragua test to be unpersuasive.[137] Both of these grounds would be meritless if the court would have accepted that there are two tests in the Nicaragua. The two tests contained in Nicaragua offer a better solution to the problems the Appeals Chamber identified in Tadic. The first ground of disapproval in Tadic is that the degree of control may vary according to the factual circumstances of each case because a single private individual needs to be distinguished from a hierarchically structured group and while the former needs to receive instructions from the State for the latter it might suffice that an overall control is exercised by the State over the Entity.[138] The two tests in Nicaragua offer a very similar distinction, not between a private individual and a structured group, but between the attribution of the whole conduct of an Entity under the Strict Control test and attribution of an individual conduct under the Effective Control test. And while the focus of the distinction is on the level of

[133] Talmon (n 7) 506; Milanovic, "State Responsibility for Genocide" (n 111) 583.
[134] *Tadić* (n 11) [114].
[135] *Bosnian Genocide* (n 26) [393].
[136] Talmon (n 7) 507.
[137] *Tadić* (n 11) [115].
[138] ibid, [117].

control, the result has essentially the same effect as the distinction which the court in Tadic wanted to introduce. A single act can be attributed by a State exercising Effective Control over an Entity[139] and the whole conduct of the Entity can be attributed under the Strict Control test, without the need to attribute every single act.[140] The Nicaragua solution is therefore easier to satisfy in this respect, because it allows the conduct of hierarchically structured groups to be attributed both by the tests of Strict Control and Effective Control. Because the tests in Nicaragua do not focus on the structure of the Entity but rather the level of control, it is more flexible than the solution the court proposed in Tadic: it can be applied to both hierarchically structured and disorganized groups. The first ground of disapproval in Tadic is therefore not only wrong in its accusation, but ironically suggests a less flexible solution.

The second ground of disapproval in Tadic is that the Effective Control is the wrong level of control over the Entity for its attribution as a *de facto* organ of the State.[141] The court is correct in this conclusion, the Strict Control test is the appropriate level of control for the attribution of an Entity as a *de facto* organ of a State. The Appeals Chamber then determines the appropriate level of control over the group as Overall Control, a test not requiring the issue of specific instructions with regard to specific acts. The Overall Control test as formulated in the paragraphs 131 of the judgement and as separated into two parts by Talmon requires the State's:[142]

[139] *Nicaragua* (n 10) [115].
[140] Milanovic, "State Responsibility for Genocide" (n 111) 577.
[141] *Tadić* (n 11) [124].
[142] Talmon (n 7) 506.

1. *[The] provision of financial and training assistance, military equipment and operational support. [Equipping and financing.]*
2. *Participation in the organisation, coordination or planning of military operations. [General planning.]*

This is a much lower standard than the Strict Control test. The court makes the mistake of conflating the scope and intensity required for the attribution. While the control needs to be exercised in general for an attribution under both Overall and Strict Control tests, there also must be a complete dependence of the Entity on the State under the Strict Control test.[143] The *de facto* State organ needs not to be instructed on each specific act.[144] As we discussed earlier, certainly at least in Milanovic's interpretation, the level of control exercised over the Entity can be inferred from the States practice *vis-à-vis* its own organs.[145] For example, if a State has particularly autonomous official organs, perhaps an army with autonomy to act more or less independently or a cyber army which is only a *de facto* organ of the State, it should not be subjected to a greater level of control. Perhaps general planning of the operation is sufficient to satisfy Talmon's third step of the Strict Control test. However, mere equipping and financing is insufficient to create a relationship of complete dependence, the first step of the Strict Control test, in any case.[146] The focus of the court is mistakenly placed on correcting perceived wrong, in this case, the burden of instruction to every

[143] ibid, 501.
[144] ibid.
[145] Milanovic, "State Responsibility for Genocide" (n 111) 577.
[146] Talmon (n 7) 499.

act, and thus fails to engage directly with the high burden of complete dependence the Strict Control test imposes. Because the control in both the Strict Control and Overall Control tests is over the general behaviour of the Entity as opposed to specific acts, the second ground of disapproval is again meritless. The test offered as a solution hence falls bellow the standard established in Nicaragua without any justification and it is, therefore, unpersuasive.[147]

Since the Overall Control test is an alternative to the Strict Control test, it is a competing test of attribution under Article 4, despite the court's intention in Tadic. Moreover, as we have established above, the exceptional nature[148] of the attribution of an Entity under Article 4 dictates the stringent nature of the Strict Control test, hence suggesting the Overall Control test is unsuitable. Perhaps the exercise of the control can be evidenced by a lower standard of control than wholly devising strategy and tactics, but either way the possibility of control certainly needs to emerge first from the complete level of dependence.[149] The complete omission of the requirement of dependence in the Overall Control test stretches the test *"almost to breaking point"*[150] and it cannot be considered good law for attribution of *de facto* organs of the State under Article 4. This is no surprise since the test was not intentionally concerned with Article 4 after all.

[147] Milanovic, "State Responsibility for Genocide" (n 111) 577.
[148] *Bosnian Genocide* (n 26) [393].
[149] *Nicaragua* (n 10) [110].
[150] Talmon (n 7) 507.

c. Control in Cyberspace

From the above discussion it is clear the legally sound test for the attribution of de facto organs of the State in cyberspace is that of Strict Control. However, much like the court in Tadic, the commentators on attribution in cyberspace have, on a number of occasions, considered the Overall Control test as an alternative, not to the Strict Control test, but to the Effective Control test.[151] We will first consider the interpretations of the law by Shackelford[152] and Roscini[153] and then evaluate whether the properly constructed Strict Control test should be lowered for attributing the conduct of the Entities in cyberspace.

Shackelford claims that if the Overall Control test would replace the Effective Control test, the *"Russian or Chinese incitement behind the cyber attacks on Estonia, Georgia, or the United States, if proven, would be sufficient to satisfy State attribution".*[154] It is important to note here that we have already established in the previous chapter that such attacks would most likely fall under Instructions if sufficient evidence could be discovered. Shackelford dilutes the test of Overall Control by explaining that *"sponsorship or support for cyber attacks would be sufficient"*[155] to satisfy the test. This is not true; even the less stringent Overall Control test requires on top of support, at least, some level of planning to be satisfied.[156] Mere sponsorship or

[151] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 988.
[152] ibid.
[153] Roscini, "World Wide Warfare" (n 6) 100.
[154] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 992.
[155] ibid, 1013.
[156] *Tadić* (n 11) [131].

incitement would not be enough. The advantages of Overall Control test put forward by Shackelford are therefore unsubstantiated even if the test would be available as an alternative to the Strict Control test.

Equally problematic are the opposing voices. Roscini dismisses the lower test on two grounds. For policy reasons, Roscini dismisses Shakelford's praise for the Overall Control test and concludes that the *"inherently clandestine nature of cyber activities and the technical difficulty of identifying the authors"*[157] is, on the contrary, a reason for a stricter test of control to prevent the States *"from being frivolously accused of cyber attacks"*.[158] This position seems dissatisfactory. The accusation and attribution are two distinct concepts. States seem to be accused of cyber attacks frivolously, no matter what the legal test of attribution is.[159] What needs to be considered instead is whether the State practice, in using proxy Entities for their cyber operations, demands a lower standard of control than Strict Control to be sufficiently encompassing, balanced with the risk of the test being too inclusive. Roscini then proceeds to criticize Shackelford for not failing to consider that the application of the Overall Control test extends only to *"organised and hierarchically structured groups, such as a military unit or, in case of war or civil strife, armed bands of irregulars or rebels"*[160] and concludes that there is of yet no such group operating in cyberspace. Again this position does not seem to reflect reality, we will consider at least two

[157] Roscini, "World Wide Warfare" (n 6) 100.
[158] ibid.
[159] Oliver Laughland, "FBI director stands by claim that North Korea was source of Sony cyber-attack" (7 January 2015) <http://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey> accessed 27 April 2016
[160] Roscini, "World Wide Warfare" (n 6) 100.

organized and hierarchically structured groups below. Even if the Overall Control would be available, Roscini's interpretation does not ultimately hold.

In the past decade, there has been an increase in organised groups conducting political cyber attacks. What used to be a novelty during the DDoS attacks on Estonia and Georgia is now an established practice.[161] Organized groups of cyber criminals such as Russian Business Network (RBN),[162] Honker Union[163], Emissary Panda[164], CyberBerkut[165] or Sandworm[166] operate from their respective countries with their attacks often coinciding with the interests of their host State. They can be divided into two general categories based on what seems to be their primary motivation. On the one hand, there are politically motivated hacker groups such as CyberBerkut or Syrian Electronic Army. On the other hand, there are cyber crime groups seeking profits such as Russian Business Network.[167] Both categories have been previously connected with political cyber attacks and suspected of working on behalf of a State.

---

[161] Nazario (n 21) 163.
[162] James Graham, *"The Russian Business Network: Rise and Fall of a Criminal ISP"* in James Graham and others, *Cyber Fraud: Tactics, Techniques and Procedures* (Auerbach Publications 2009) 171.
[163] Owen Fletcher, "Patriotic Chinese Hacking Group Reboots" (5 October 2011) <http://blogs.wsj.com/chinarealtime/2011/10/05/patriotic-chinese-hacking-group-reboots/> accessed 27 April 2016
[164] Fahmida Y. Rashid, "Emissary Panda Hackers Get Selective in Data Heists" (6 August 2015) <http://www.securityweek.com/emissary-panda-hackers-get-selective-data-heists> accessed 27 April 2016
[165] Jeff Stone, "Meet CyberBerkut, The Pro-Russian Hackers Waging Anonymous-Style Cyberwarfare Against Ukraine" (17 December 2015) <http://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902> accessed 27 April 2016
[166] Jim Finkle, "U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage" (7 January 2016) <http://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108> accessed 27 April 2016
[167] James Graham, *"The Russian Business Network: Rise and Fall of a Criminal ISP"* in James Graham and others, *Cyber Fraud: Tactics, Techniques and Procedures* (Auerbach Publications 2009) 171.

Let's first consider RBN which has been connected with the attacks on Georgia.[168] RBN is conducting its large scale illegal activity only thanks to the lack of interest from Russia.[169] It is speculated that the RBN is paying for this immunity to the Russian officials as a group *"as malicious and wealthy as RBN certainly has крыша, or "roof" (i.e., protection bought from corrupt politicians and organized criminal elements".*[170] If this protection would cease, all or the vast majority of the RBN operation could stop. In this sense, it could be argued the RBN is completely dependent on Russia. The question is whether the inversion of the cash flow we would expect to create complete dependence would prevent the Entity from being considered so dependent on the State. It does not seem reasonable to stretch the requirements of (1) complete dependence (2) extending to all or majority of operation over RBN. The Entity is benefiting from an omission rather than support of the State. It would be wrong to conclude that the Entity is completely dependent on the State as the Entity is in fact completely dependent on being ignored by it. The first two requirements of the Strict Control test would therefore not be met. The attribution could more likely be under Instructions as the Entity is operating as a hacker mercenary that can be hired by anyone, including the State, to act on their behalf.[171]

However, if the State would have created the Entity in the first place, thereby creating the presumption of being under its complete dependence,[172] the

[168] John Markoff, "Before the Gunfire, Cyberattacks" (12 August 2008) <http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0> accessed 27 April 2016
[169] Graham (n 167) 172.
[170] ibid.
[171] ibid.
[172] Talmon (n 7) 501.

situation could be different. There does not seem to be any obvious reason why the commercial nature of the Entity should make it less dependent on the State. While the commercial aspect of the Entity would make it less likely dependent on financial support from the State, it would not be sensible to, on this factor alone, consider it independent. However, the presumption of complete dependence could easily be rebutted here as RBN seems far from a *"mere instrument"* of Russia even in the broadest of terms.[173] Therefore, if it were proven that the RBN was in fact created by Russia it would still most likely not Satisfy Talmon's first two criteria.

The second question is whether the potential control inherent in the relationship of complete dependence could be sufficiently exercised in the case of RBN to satisfy the third criterion. If Milanovic's broader interpretation of the exercise of control, is the standard necessary, the dual nature of the Entity would not be problematic. Article 4 offers a broad construction of a State organ and explicitly states that the State organ *"may be classified as "commercial" or as acta iure gestionis*. As discussed earlier, whether the State exercise of control is to satisfy the third criterion would depend on whether the State control over its official organs would set the control necessary for attribution under Strict Control low enough so that the RBN could satisfy it. In the case of RBN, this would seem near impossible as it does not perform any apparent role within the structure of the State, operating instead as an independent criminal commercial enterprise.[174] It is

[173] Bosnian Genocide (n 26) [392].
[174] Talmon (n 7) 501.

unlikely Russia is controlling the RBN in any manner and thus RBN would not be attributable under the Strict Control test.

The second type of organized group is a more likely candidate to satisfy the criteria of the Strict Control test. The Sandworm hackers, for example, are believed to be responsible for the attacks on Ukrainian power grid in January 2016 and are solely political in their cyber activity.[175] While evidence confirming the link with Russia is missing, commentators have agreed the level of sophistication with which the attack has been conducted makes it very likely the group had support from Russia.[176] Mere support would not be enough to constitute complete dependence, however. With operations of this level of complexity the cessation of financial aid, or supply of expensive and rare zero day exploits, from the State would certainly stop the operation. It is therefore possible, that if there is a State involvement, the Entity will be completely dependent on the State's support and becomes *"mere instrument"* of the State.[177]

The burden of complete dependence, while strict, might be easier to achieve for the second type of organized groups than first expected. While evidence is missing to actually confirm the dependence of bodies above to their respective States, it is conceivable that such a link could be discovered. The difficult part of attribution, just like in the case of Nicaragua, is likely to be the

[175] John Hultquist, "Sandworm Team and the Ukrainian Power Authority Attacks" (7 January 2016) <http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/> accessed 27 April 2016
[176] ibid; Stephen Ward, "iSIGHT discovers zero-day vulnerability used in Russian cyber-espionage campaign" (14 October 2014) <http://www.isightpartners.com/2014/10/cve-2014-4114/> accessed 27 April 2016
[177] Bosnian Genocide (n 26) [392].

third part of the Strict Control test; the exercise of the inherent control. Therefore, even if the Overall Control test would replace the Strict Control test, the Entities above could still not be attributed. Furthermore, while the Overall Control test requires participation, coordination or planning of military operations and the exercise of control, the Strict Control test offers a flexible test which demands, at the least, the same level of control that the State exercises over its own official organs; potentially a lower standard to meet. It seems the Overall Control test does not make the attribution of a *de facto* organ any easier in practice.

The third part of the Strict Control test is certainly extremely difficult to satisfy, even under Milanovic's interpretation. An Entity such as Chinese Unit 61398, for example, which could be a *de jure* organ based on the evidence from the Mandiant report demonstrating its legal integration within the Peoples Liberation Army[178] and therefore fall under Article 4, would not be possible to attribute under the Strict Control test. While complete integration does create a presumption of complete dependence, to satisfy the Strict Control test the Entity would have to also satisfy its other two criteria. There is no indication the inherent control China has over the Unit 61398 has been exercised in any way. The Unit could therefore be a *de jure* organ of the State, but not satisfy the Strict Control test at the same time demonstrating how Milanovic's approach is more sensible.

Perhaps the Entities operating in cyberspace do deserve to be attributed on their complete dependence alone. Such relaxation would not go directly

[178] Mandiant *"Exposing One of China's Cyber Espionage Units"* < http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf > accessed 27 April 2016.

against the Strict Control test; it could develop in line with Milanovic's relaxed understanding of the exercise of control. If the Syrian Electronic Army,[179] Iranian Cyber Army[180] or Unit 61398 are found to be completely dependent on their respective States the lack of proof that the respective States exercise control over them should not let these States escape responsibilities for the actions of these proxy armies. Much like the police being considered independent by the State legislature and thus remains a State organ,[181] the level of control exercised necessary would become null, based on the State practice in regards to these Entities'.

In conclusion, many States have established unofficial organs for cyber espionage or sabotage. Some, like RBN, do not merit attribution as they seem to be cyber mercenaries that are not particularly dependent on any State. Other Entities, such as Sandworm, Unit 61398 and potentially the Syrian Electronic Army and Iranian Cyber Army seem more likely to be behaving on behalf of their respective State. These Entities cannot be attributed under the Strict Control test as it now stands. Replacing the Strict Control test with Overall Control test would not help the attribution because the Overall Control test still demands an evidence of the exercise of control. The use of these Entities would, therefore, merit relaxation of the last requirement of the Strict Control test.

[179] ibid, 99.
[180] ibid.
[181] Crawford, *Articles on State Responsibility* (n 1) 94.

7. Effective Control and the test of Directions

The most elusive of all of the tests under Article 8 of the ILC draft articles on State attribution is the Effective Control test. Articulated in paragraph 115 of the Nicaragua judgement the court has created a test to attribute the acts of Entities which are not under the Strict Control of a State.[182] It is, therefore, a subsidiary test to the Strict Control test but, despite its lower scope[183] and the opinion of commentators,[184] the test seems more difficult to apply, at least with respect to cyber attacks, than its parent test. The focus of this chapter is the clarification of this test. Later, the possibility of a distinct test of directions will be considered. Finally, I will try to evaluate whether the Effective Control test, as it stands in the context of the Strict Control test and test of Instructions, is too harsh of a test for attribution of cyber attacks.

a. Effective Control test

The first problem with attribution under the Effective Control test is the lack of clarity in its content. The interpretation of the test has prompted a wide variety of opinions between commentators. Unsurprisingly, the Effective Control test is often conflated with the Strict Control test or the test for Instructions.[185]

[182] *Nicaragua* (n 10) [115].
[183] Talmon (n 7) 502.
[184] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 987; Roscini, "World Wide Warfare" (n 6) 100.
[185] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 987; Roscini, "World Wide Warfare" (n 6) 100.

Shackelford, for example, demands complete dependence for the acts of the Entity to satisfy the Effective Control test.[186] From the discussion in the previous chapter, it is clear that complete dependence is required for the Strict Control test. Effective Control, however is distinguished from its parent test by requiring a lower threshold of dependence, namely the partial dependence which *"may be inferred, inter alia, from the provision of financial assistance, logistic and military support, supply of intelligence, and the selection and payment of the leadership of the entity by the outside power".*[187] The court makes this clear in paragraph 112, where it states that if no complete dependence can be found, a *"partial dependency"* may still entail responsibility *"for activities of the contras".*[188] Shackelford is, therefore, mistaken in demanding the threshold of dependence to be complete.

As was discussed in the previous chapter, Roscini has also conflated the tests of Strict Control and Effective Control. However, on top of not considering the tests separately, he has also concluded that the Effective Control test is *"i.e. the need to prove the issue of specific instructions concerning the commission of the illegal act or the state's public retroactive approval of the individual's actions".*[189] Although there is no reason why the tests in Article 8 could not overlap, each test is distinct.[190] Because Roscini's definition of the Effective Control is exactly the same as the test for Instructions, he cannot be correct. The first test is looking for the existence of

[186] Shackelford, "State Responsibility for Cyber Attacks" (n 6) 975.
[187] *Nicaragua* (n 10) [112].
[188] ibid, [113].
[189] Roscini, "World Wide Warfare" (n 6) 100.
[190] Crawford, *Articles on State Responsibility* (n 1) 94.

instruction while the second test is searching for a sufficient level of control.[191] Instructions on their own will not satisfy the Effective Control test. To conclude that instructions and control are the same is appealing, but does not reflect the position of the court in Nicaragua and Bosnian Genocide.[192] Roscini is, therefore, wrong in equating them; the test of Effective Control is not a test for Instructions.

Yet it is easy to conclude on a reading of the judgment that if the Effective Control test does not require instructions it must require enforcement by the State. Cassese, for example, analyses paragraph 115 in Nicaragua as demanding either:

"(1) the issuance of directions to the contras by the US concerning specific operations (indiscriminate killing of civilians, etc.), that is to say, the ordering of those operations by the US, or (2) the enforcement by the US of each specific operation of the contras, namely forcefully making the rebels carry out those specific operations."[193]

Cassese seems to be right in stating that enforcement of the operation would satisfy the Effective Control test. However, ordering or directing the operation seems to again be conflating the test for Instructions with the test of control. Talmon, in arguing that Effective Control must extend from the beginning of the operation, throughout its duration, until the end, seems to not only be

[191] Crawford, *State Responsibility* (n 25) 146.
[192] *Bosnian Genocide* (n 26) [400]; *Nicaragua* (n 10) [115].
[193] Cassese (n 6) 653.

describing the length of the control necessary but also bringing clarity as to what distinguishes Effective Control from Instructions.[194] Not all State involvement over the entire duration of the activity will be enough to reach the level of Effective Control. Instructions over the entire operation would fall outside the test as they would not necessary cover the beginning, middle and the end of the activity. Instead, the direction and control must be given in respect of each decision through the operation so that the Entity would not be able to conduct its activity without such State involvement.[195] The test of Effective Control is therefore very similar to its parent test and can be described in three steps like this:

1. *The Entity must be at least partially dependent on the State.*
2. *The control must extend over the entire duration of the operation.*
3. *The control must be such that the Entity would not be able to conduct its activity without the State control.*

However, unlike its parent test the major focus is on the level of control instead of the level of dependence.[196] Where the Strict Control test requires complete dependence and some level of control,[197] the Effective Control test requires partial dependence and effective level of control.[198] Interestingly complete dependence, where the dependence on State is such that the Entity can't conduct its activities without it, seems difficult to distinguish from

[194] Talmon (n 7) 503.
[195] *Nicaragua* (n 10) [115].
[196] Talmon (n 7) 503.
[197] *Nicaragua* (n 10) [110].
[198] ibid, [115].

the level of control where the Entity is not able to conduct its activity without State control. Of course, we can separate these easily from the context of their respective tests, because one test is attributing the entire conduct of the Entity as *de facto* organ of the State[199] the other only a specific action of the Entity.[200] However, the question still remains as to how, on a substantive level, is an effective level of control different from complete dependence.

There are notable differences in the way each arises. While complete dependence can be evidenced by the State creating or completely integrating the Entity, as well as providing such support that the Entity cannot conduct its activates without it,[201] only control over the Entity which is such that the Entity can not conduct its activities, is enough to satisfy the Effective Control test.[202] More importantly, while both control and dependence are created by support, dependence is only an Entity's passive state of reception, whereas, for control, the exercise of such by the State must be shown.[203] While the Strict Control test, arguably only seeks to find a level of control the State exercises over its own organs,[204] the Effective Control test requires exercise of control to the point where the State decides exactly what the Entity will do during any moment of the operation.[205] In other words, the test seeks a State that is in command of the Entity. We can distinguish this from Instructions as these are given in respect of each operation of the

[199] Crawford, *State Responsibility* (n 25) 148.
[200] ibid.
[201] Talmon (n 7) 501.
[202] *Nicaragua* (n 10) [115].
[203] ibid, [110].
[204] Milanovic, "State Responsibility for Genocide" (n 111) 577.
[205] Talmon (n 7) 503.

Entity,[206] not in respect of each decision during the operation. So instead of ordering the Entity to commit the activity in breach of primary rules, the command of the Entity is supplied by the State. While this can be done by enforcement, it can also arise, for example, while placing the State officers in command of the Entity, or alternatively by instructing the Entity on each individual decision it makes during the operation. The Effective Control test is therefore far more difficult to satisfy than its parent and the test for Instructions.

b. Test of Directions

As originally constructed, Article 8 contemplates directions along instructions and control as a third way of attributing an act of an Entity.[207] The directions have however became conflated with the test of control by the academic commentators.[208] Very few do consider directions a separate method of attribution under the Article. And those who do, like Crawford, claim the courts have, since the adoption of the ILC articles, merged the two together and direction simply does not exist anymore.[209] However, the court in the Genocide case clearly separates them, and declares that the State will be responsible for the acts under the *"instructions or directions of the State or under its Effective Control".*[210] The direction and control, have therefore been kept explicitly separate by both the courts and the ILC draft articles.

---

[206] *Bosnian Genocide* (n 26) [400].
[207] Crawford, *Articles on State Responsibility* (n 1) 110.
[208] ibid.
[209] Crawford, *State Responsibility* (n 25) 146.
[210] *Bosnian Genocide* (n 26) [401].

Nonetheless the direction and control are conflated conceptually, by the way in which the courts have established the Effective Control test. The direction of each individual move of the Entity is one of the two ways the court establishes control, enforcement is the other.[211] Even if directions were to be established as a separate test, it is hard to conceive of such a test that does not infringe on the already established tests of instruction and control. Any sensible interpretation of directions would infringe on one of these tests. If directions were to be issued in respect of a single operation, they would be replacing the test of Instructions. If directions were to be issued in respect of the entire conduct of the Entity, they would be infringing on the Strict Control test. And if they were to be issued during the operation, they would infringe on the Effective Control test. If the courts will not construct the test for directions as an exception to one of these tests, it seems unlikely we will ever need to consider directions outside of the Effective Control test. Despite this, the courts have retained the directions as a possible third test under Article 8.

c. Effective Control over Cyber Attacks

The Effective Control test is, therefore, the hardest test to satisfy in Article 8. This is partly because of its focus on the most intimate level of control. All three tests of the attribution, the Instructions, Strict Control test and Effective Control test approach the question of responsibility from a slightly different angle. The most general test of Strict Control looks at the conduct of the

[211] Cassese (n 6) 653.

Entity as a whole. Instructions look at an individual operation of the Entity as a whole. The Effective Control test on the other hand, looks at the interactions during such operation. The test is focusing on control arising at an already obscured level to begin with. Unfortunately, because the test is created as a subsidiary of the rhetoric of its parent, the Strict Control test, it also falls victim to its logic. In Nicaragua, the court starts examining how much dependence is necessary for attribution.[212] When the court decides the dependence needs to be complete in order to justify a lower threshold of control for Strict Control test, it makes sense in that it does so in creating the subsidiary test of Effective Control. In a situation where the dependence is not complete, they compensate by requiring an extraordinarily high level of control. The evidential burden for the Effective Control test is the highest of all of the tests, as the focus on State involvement is at a micro level within each operation of the Entity.

Because the Effective Control test is constructed as a subsidiary test, it is incredibly difficult to satisfy it in the cyberspace. The courts will consider the Effective Control test when the Entity is not completely dependent on the State.[213] In practice, the less the Entity is dependent on the State, the lower the control of the State over the Entity is. The control over the Entity is, as the court in Nicaragua itself recognized, inherent in the level of dependence.[214] The greater the dependence the greater the possibility of control. The more the Entity is dependent, the more likely it is that the State

[212] *Nicaragua* (n 10) [109].
[213] *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v Uganda) (Judgement) [2005] ICJ Rep 168, [160].
[214] *Nicaragua* (n 10) [109].

will enforce the individual actions or micromanage individual operations. We can see this in the development of cyber strategies in Iran and Syria.[215] Both the Syrian Electronic Army and Iranian Ashiyane Digital Security Group have been originally created as *"loosely formed organizations based upon nationalistic leanings"*[216] and slowly graduated to allegedly becoming a part of their respective State as part of government inclusion of *"cyber security as a national imperative"*.[217] Both Entities went through a similar process of State assimilation, becoming more and more dependent on their respective State. But even when the Entity becomes a *de jure* organ, as the Chinese Unit 61398 most likely is,[218] there will still be no evidence of any exercise of any control. Such evidence is either difficult to find or impossible to find as the, organs of the State (as they are at this point) enjoy far greater autonomy to conduct their activities than envisioned by the court in Nicaragua. If the court in Nicaragua could not find any exercise of control over the contras even in a situation where complete dependence has at some point arisen, how can it expect the test looking solely at such control will ever be satisfied if the required level of control is raised?

Cameron and Chetail would disagree with the above as in their interpretation, the court has found sufficient evidence to satisfy the Effective Control test in Nicaragua at least in respect of the UCLA's.[219] This interpretation is misleading as the court states that the UCLA's have been:

[215] Lemieux (n 94) 99.
[216] ibid.
[217] ibid.
[218] Mandiant (n 178).
[219] Lindsey Cameron, Vincent Chetail, *Privatizing War* (Cambridge University Press 2013) 213.

"acting on the direct instructions of, United States military or intelligence personnel"[220]

Because the UCLA's were acting under the instructions, the court was able to hold them to a different test, the test of Instructions. Cameron and Chetail are therefore wrong in concluding the planning, directing, and supporting ofUCLA's satisfied the Effective Control test. Indeed, mere planning, directing, and supporting of the Entity is not enough to satisfy the Effective Control test, as was discussed above.

Should the Effective Control test be lowered? That depends on how we answer the question Griebel and Plucken famously considered.[221] Do the tests of attribution meet the present needs of the international community?[222] And if not, would lowering the Effective Control test help to resolve this inadequacy? The relevant tests of attribution of cyber attacks have been outlined above and it seems that in the past only Instructions could attribute acts of an Entity acting on behalf of the State. Of course, this on its own does not mean the standards of control are too high. However, the test for control under Article 8 is constrained unnecessarily by its construction as a subsidiary to the Strict Control test of Article 4. Instead of covering the situations that do not satisfy the Strict Control test, the Effective Control test should try to consider the question of when the control over an individual act

[220] *Nicaragua* (n 10) [75].
[221] Jorn Griebel, Milan Plucken, "New Developments Regarding the Rules of Attribution? The International Court of Justice's Decision in Bosnia v. Serbia" (2008) 21 LJIL 601.
[222] Milanovic, "State Responsibility for Acts of Non-State Actors" (n 115), 319.

of an Entity, amounts to an attribution of responsibility for that act. Why should, for example, an act of an Entity which is completely dependent on a State in respect of a single attack, be impossible to attribute to the State? As I have argued in the previous chapter it might be possible to attribute acts within a relatively short period of time under Milanovic's interpretation of Strict Control test. However, dependence, no matter of what degree, which seems far easier to find evidence for, will never satisfy a test of Effective Control. If complete dependence over the majority of acts requires an exercise of control inferred from the practice of the States in question, a test to cover a situation of complete dependence over a single operation could be a more sensible alternative to the Effective Control test. Such test would still set a very high burden, but it might be able to engage with the State support of the proxy cyber armies. A test looking for a finer control over an Entity which is purposefully distanced from the State will never have enough grip to satisfy the needs for attribution of the international community. Such test could be defined as:

(1) The Entity must be completely dependent on the outside power.
(2) This complete dependence must be present during the entirety of a specific operation.

The cyber attacks themselves are nonetheless not specific in any way which would justify derogation from the Effective Control test, or any other traditional attribution test for that matter. While it seems to be more difficult to find evidence in the cyberspace, although, by no means impossible, the

problem of technical attribution should not be an argument for lowering the legal test of attribution.[223] Such practice would most likely result in unsubstantiated attribution of cyber attacks and aggravation of cyber conflicts.[224] It also seems that the problem of technical attribution is solved proportionately to the emerging threat of such attacks anyway. Peter Margulies's argument of attribution asymmetry, the asymmetry between the ease with which cyber attack can be conducted, and the difficulty to detect it, does not seems persuasive.[225] While the cyber attack itself can be easier to control for the Entity deploying it, it is a programmed set of actions after all; the State control over the Entity does not focus on the State control over the weapon, but instead over the people deploying it. The fact that cyber attacks can be conducted from a great distance with a small group of people does not mean, as professor Marguiles asserts, that *"a state has a far greater capacity to control such groups".*[226] The State certainly has a greater capacity to control any group thanks to the advancement of communication technologies over the years, but this is not specific for control over Entities conducting cyber operations. In looking at cyber attack we need to distinguish the technical attribution of an attack to the Entity itself, which is a separate issue, and the legal attribution of the responsibility for the attack to the State. There is no attribution asymmetry at this side of the problem. A State does not have any better means of controlling a group of hackers than it has for controlling a group of contras, although the hacker group will most likely have better internet connection. It can thus be argued that attribution is

[223] Thomas Rid, Ben Buchanan, "Attributing Cyber Attacks" (2015) 38 JSS 4, 7.
[224] Roscini, "World Wide Warfare" (n 6) 100.
[225] Margulies (n 8) 513.
[226] ibid, 514.

primarily a legal and not a technical problem, or at least it will slowly become primarily a legal problem as the methods of physical attribution become more sophisticated.[227]

In conclusion, the Effective Control test is focusing on the entire duration of a single operation, where it demands the highest form of control and only partial dependence of the Entity. The test is unsuitable for attribution not only of cyberattacks but of any attack, due to its construction as a subsidiary to the Strict Control test and of its focus on a control during an operation where evidence is either impossible or at least extremely difficult to discover. An alternative test focusing on dependence during an attack would be preferable as it would be still sufficiently narrow, but perhaps possible to satisfy.

[227] Rid, Buchanan (n 223) 30.

8. Conclusion

Despite what the Tallinn Manual asserts,[228] to attribute the conduct of the Entities operating in cyberspace would merit some amendments to the tests of attribution. Because of the customary nature of the law of State responsibility,[229] such change could materialize from the practice of the States themselves. In the first chapter I have argued that test of Instructions, although workable test for attribution of the DDoS attacks is a test which should extend over toolkits with self-contained instructions. I have also argued that State practice has shifted from perceiving DDoS attacks as mere acts of cyber activism to a threat worth attributing, demonstrating the change in this attitude from the late 2000's.

However, in majority of the examples considered in this dissertation, the means of the attack had no effect on the attribution. For the tests of control, the type of a weapon, whether traditional or cyber, is simply irrelevant to the attribution of the Entity. The test of Instructions is the only test that was theoretically possible to satisfy in the circumstances of a DDoS attack. Yet, even this test is very unlikely to be satisfied in the future, if espionage in this area does not improve, as States have been, even during the early days of DDoS attacks, very careful to distance themselves from any instructions posted on the internet and even more so not to circulate any instructions they may have given to the Entities.

[228] Schmitt (n 9) 29.
[229] Anthony D'Amato, *The Concept of Custom in International Law* (Cornell University Press 1971).

As for the tests of control, I have argued in the second chapter, that the Strict Control test would merit a softer interpretation of the requirement of an exercise of the control, so that the *de facto* organs of a State do not have to be subjected to a stricter level of State control than their official counterparts to satisfy the test. With such amendment, as accepted already by Milanovic,[230] the Strict Control test could be a workable test for attribution in cyberspace.

Finally, in the third chapter I submitted that the Effective Control test is, because of its construction as a subsidiary of the Strict Control test,[231] unsuitable for an attribution of the conduct of an Entity in cyberspace. The level of control it seeks during an operation is extremely difficult to discover, if it was ever present. Rather, a test seeking complete dependence during a single mission would be a better alternative. I have further argued the test for directions has been conflated conceptually as any sensible interpretation of it would infringe upon an already established test of attribution.

As for the question of whether the cyber attacks or the Entities conducting these attacks, are so different from their traditional counterparts to merit such derogation from the Effective Control test? My answer is no. There is no attribution asymmetry, as it does not matter whether the group in question conducts an attack by shooting bullets or bytes of data. In both cases, the focus of the test of control under Article 8 is on the connection between the

[230] Milanovic, "State Responsibility for Genocide" (n 111) 577.
[231] Talmon (n 7) 502.

Entity and the State; a connection which does not change with the space in which the Entity operates.

9. Bibliography

a. Books

- Cameron L, Chetail V*, Privatizing War* (Cambridge University Press 2013).
- Crawford J, *The International Law Commission's Articles on State Responsibility* (Cambridge University Press 2002).

  -- *State Responsibility: The General Part* (Cambridge University Press 2013).
- Czosseck C, Geers K. (eds.), *The Virtual Battlefied: Perspectives on Cyber Warfare* (IOS Press 2009).
- D'Amato A, *The Concept of Custom in International Law* (Cornell University Press 1971).
- Graham J and others, *Cyber Fraud: Tactics, Techniques and Procedures* (Auerbach Publications 2009).
- Janczewski L. (ed.), *Cyber Warfare and Cyber Terrorism* (Idea Group Publishing 2007).
- Lemieux F, *Current and Emerging Trends in Cyber Operations; Strategy and Practice* (Palgrave Macmillan 2015).
- Rid T, *Cyber War Will Not Take Place* (Oxford University Press 2013).
- Roscini M, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014).
- Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).
- Tikk E, Kaska K, Vihul L, *International Cyber Incidents: Legal Considerations* (CCD COE 2010).

- Tonkin H, *State Control over Private Military and Security Companies in Armed Conflict* (Cambridge University Press 2011).

b. Journal Articles

- Buchanan B, Rid T, “Attributing Cyber Attacks” (2015) 38 JSS 4.
- Cassese A, “The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia” (2007) 18(4) EJIL 649.
- Griebel J, Plucken M, “New Developments Regarding the Rules of Attribution? The International Court of Justice’s Decision in Bosnia v. Serbia” (2008) 21 LJIL 601.
- Margulies P, “Sovereignty and Cyber Attacks: Technology’s Challenge to the Law of State Responsibility” (2013) 14 MJIL 496.
- Milanovic M, “State Responsibility for Genocide” (2006) 17(3) EJIL 553.

  -- “State Responsibility for Acts of Non-State Actors: A Comment on Griebel and Plücken” (2009) 22(2) LJIL 307.
- Mirkovic J, Reiher P, “A Taxonomy of DDoS attack and DDoS Defense Mechanisms” (2004) 34(2) ACM SIGCOMM Computer Communication Review 39.
- Rid T, “Cyber War Will Not Take Place” (2012) 35(1) JSS 5.
- Roscini M, “World Wide Warfare – Jus ad bellum and the use of Cyber Force” (2010) 14 YBUNL 86.
- Shackelford S, “State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem” (2010) 42(4) GJIL 971.

- Talmon S, “The Responsibility of Outside Powers for Acts of Secessionist Entities” (2009) 58(3) ILQ 493.
- Timmermann K, “Incitement in International Criminal Law” (2006) 88 IRRC 823.
- Tripathi S and others, “Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks” (2013) 4(3) Journal of Information Security 150.

10. Table of Cases and Websites

a. Table of Cases

- Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Judgement) [2005] ICJ Rep 168.
- Case Concerning Application of the Convention on the Prevention and Punishment of the crime of Genocide (Judgment) [2007] ICJ Rep 43.
- Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) (Merits) [1986] ICJ Rep 14.
- Prosecutor v. Duško Tadić (Judgment of the Appeals Chamber) ICTY-99-IT-94-1-A (15 July 1999).
- Prosecutor v Kordic and Cerkez (Judgment) ICTY-95-14/2-A (17 December 2004).

b. Websites and blogs

- Sarah Left, “Chinese and American hackers declare 'cyberwar'” (4 May 2001) <http://www.theguardian.com/technology/2001/may/04/china.internationalnews> accessed 27 April 2016
- Ian Traynor, “Russia accused of unleashing cyberwar to disable Estonia” (17 May 2007) <http://www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 27 April 2016

- John Markoff, “Before the Gunfire, Cyberattacks” (12 August 2008) <http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0> accessed 27 April 2016
- Marko Milanovic, “What Exactly Internationalizes an Internal Armed Conflict?” (7 May 2010) <http://www.ejiltalk.org/what-exactly-internationalizes-an-internal-armed-conflict/> accessed 27 April 2016
- Liam O Murchu, “Stuxnet Using Three Additional Zero-Day Vulnerabilities” (14 September 2010) <http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities> accessed 27 April 2016
- European Union Agency for Network and Information Security, “Stuxnet Analysis” (7 October 2010) <https://www.enisa.europa.eu/media/press-releases/stuxnet-analysis> accessed 27 April 2016
- Owen Fletcher, “Patriotic Chinese Hacking Group Reboots” (5 October 2011) <http://blogs.wsj.com/chinarealtime/2011/10/05/patriotic-chinese-hacking-group-reboots/> accessed 27 April 2016
- Stefanie Hoffman, “DDoS a Brief History” (25 March 2013) <https://blog.fortinet.com/post/ddos-a-brief-history> accessed 27 April 2016
- Imperva Cyber Security Blog, “The rise of DDoS Botnets” (2 April 2014) <http://blog.imperva.com/2014/04/the-rise-of-ddos-botnets.html> accessed 27 April 2016

- Stephen Ward, “iSIGHT discovers zero-day vulnerability used in Russian cyber-espionage campaign” (14 October 2014) <http://www.isightpartners.com/2014/10/cve-2014-4114/> accessed 27 April 2016
- Oliver Laughland, “FBI director stands by claim that North Korea was source of Sony cyber-attack” (7 January 2015) <http://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey> accessed 27 April 2016
- Fahmida Y. Rashid, “Emissary Panda Hackers Get Selective in Data Heists” (6 August 2015) <http://www.securityweek.com/emissary-panda-hackers-get-selective-data-heists> accessed 27 April 2016
- Sophie Curtis, “Anonymous recruits amateurs in cyber war against Isil” (18 November 2015) <http://www.telegraph.co.uk/technology/internet-security/12004025/Anonymous-recruits-amateurs-into-cyber-war-against-Isil.html> accessed 27 April 2016
- Jeff Stone, “Meet CyberBerkut, The Pro-Russian Hackers Waging Anonymous-Style Cyberwarfare Against Ukraine” (17 December 2015) <http://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902> accessed 27 April 2016
- Rene Millman, “’Russian’ DarkEnergy malware strikes at Ukrainian media and energy firms” (4 January 2016) <http://www.scmagazineuk.com/russian-darkenergy-malware-strikes-

at-ukrainian-media-and-energy-firms/article/462778/> accessed 27 April 2016

- Robert Lipovsky, “BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry” (4 January 2016) <http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/> accessed 27 April 2016
- Hannah Kuchler, Neil Buckley, “Hackers shut down Ukraine power grid” (5 January 2016) <http://www.ft.com/cms/s/0/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.html#axzz3zmZD2bFJ> accessed 27 April 2016
- Jim Finkle, “U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage” (7 January 2016) <http://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108> accessed 27 April 2016
- John Hultquist, “Sandworm Team and the Ukrainian Power Authority Attacks” (7 January 2016) <http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/> accessed 27 April 2016
- UK Government Communications Headquarters, “Common Cyber Attacks: Reducing the Impact” (19 February 2016) <*https://www.cesg.gov.uk/white-papers/common-cyber-attacks-reducing-impact*> accessed 27 April 2016

- Mandiant *“Exposing One of China’s Cyber Espionage Units”* < *http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf* > accessed 27 April 2016