Cyber Attacks and the Use of Force in International Law

Janne Valo
Master's Thesis
University of Helsinki
Faculty of Law
International Law
Supervisor: LL.D. Jarna Petman

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiedekunta/Osasto Fakultet/Sektion – Faculty	Laitos/Institution– Department	
Faculty of Law		
Tekijä/Författare – Author		
Janne Valo		
Työn nimi / Arbetets titel – Title		
Cyber Attacks and the Use of Force in International Law		
Oppiaine /Läroämne – Subject		
International Law		
Työn laji/Arbetets art – Level	Aika/Datum – Month and year	Sivumäärä/ Sidoantal – Number of pages
Master's Thesis	January 2014	XIV + 85 p.

Tiivistelmä/Referat – Abstract

The thesis reviews the issue of cyber attacks and international law in terms of jus ad bellum, the law concerning the recourse to force by states. The thesis takes the view that the existing rules on the use of force, namely Articles 2(4) and 51 of the United Nations Charter and the corresponding rules of customary international law apply to attacks regardless of the way they are carried out and thus, they apply to cyber attacks as well. Two central examples of different kinds of cyber attacks are presented to illustrate the issue: the attacks against Estonia in 2007 and Stuxnet, the malware that targeted Iranian nuclear facilities and was discovered in 2010.

Before covering the main question of if and when cyber attacks may constitute uses of force or armed attacks, the thesis takes a brief historical look at how the just war doctrine and the regulation of war have evolved to their current state. The thesis argues that while cyber attacks are a new phenomenon with certain unique aspects, they are a part of the evolution and continuum of armed conflict.

The thesis takes a look at the different approaches (instrument-based, target-based and effects-based) to assessing the question of whether or not a cyber attack crosses the threshold of a use of force or an armed attack. The effects-based view is found to be most appropriate one. It is argued that particularly cyber attacks that cause death, injury, damage or destruction qualify as uses of force. As cyber operations make it possible to cause severe economic consequences without the use of physical force, the question of economic force is discussed as well. The thesis argues that while the prevailing view is that Article 2(4) does not cover the use of economic force, the question may arise in the context of cyber attacks, and an attack with such consequences may result in a reappraisal of the issue in state practice.

Turning to armed attacks, the thesis argues that cyber operations may also qualify as armed attacks. Accepting the prevailing view that distinguishes between uses of force and armed attacks, the thesis claims that for a cyber operation to rise to the level of an armed attack, the consequences must be sufficiently grave. It is argued that for example a denial-of-service attack does not fulfil the criteria of an armed attack, but an attack that causes fatalities or severe damage or destruction would cross the threshold and justify self-defence. The thesis also discusses the question of pre-emptive self-defence in the context of cyber attacks.

Avainsanat – Nyckelord – Keywords
international law, cyber attacks, use of force, jus ad bellum, armed conflict, self-defence

Säilytyspaikka – Förvaringställe – Where deposited
University of Helsinki Library

Muita tietoja – Övriga uppgifter – Additional information

Table of Contents

1 Introduction....1
1.1 Introduction to the Issue....1
1.2 Terminology....4
1.3 Applicability of the Existing Rules....7
2 Evolvement of War and Cyber Attacks....10
2.1 Evolvement of the Notion of War....10
2.2 History and Types of Malware and Cyber Attacks....12
2.3 Examples of Cyber Attacks....13
2.3.1 Attacks Against Estonia in 2007....13
2.3.2 Stuxnet....14
2.3.3 Red October....16
2.4 Technical Aspects of the Attacks....17
3 Regulation of the Use of Force....20
3.1 General Notions About War and Its Regulation....20
3.2 United Nations as the Keeper of International Peace....21
3.3 Interpretation of the Rules of International Law....23
4 Prohibition of the Use of Force in the Context of Cyber Operations....25
4.1 Article 2(4) of the United Nations Charter....25
4.2 Customary International Law....26
4.2.1 Prohibition on the Use of Force in Customary International Law....26
4.2.2 Prohibition of the Use of Force as a Peremptory Norm....28
4.3 Notion of 'Force'....30
4.4 Cyber Operations as Force....33
4.4.1 Overview of Cyber Operations....33
4.4.2 Some Unique Characteristics of Cyber Operations....34
4.4.3 Cyber Operations as Uses of Force....36
4.4.4 Attempts and Unsuccessful Attacks....40
4.4.5 Cyber Assistance as Force....41
4.5 Economic or Political Force....42

4.6 Chapter VII of the UN Charter....44
5 Cyber Operations as Armed Attacks and the Right to Self-Defence....47
5.1 Overview of the Right to Self-Defence....47
5.2 Notion of an 'Armed Attack'....50
5.2.1 Accumulation of Events....52
5.2.2 Notions of Armed Attacks and Force....53
5.2.3 Assistance as an Armed Attack?....56
5.3 Acts of Non-State Actors as Armed Attacks?....57
5.3.1 Acts by Irregular Forces....57
5.3.2 Level of Control for State Responsibility....60
5.4 Cyber Operations as Armed Attacks?....62
5.5 Anticipatory Self-Defence....65
5.5.1 Possibility of Anticipatory Self-Defence....65
5.5.2 Anticipatory Self-Defence and Cyber Attacks....68
5.6 Conclusions About Self-Defence....71
6 Principle of Non-Intervention and Countermeasures....73
6.1 Principle of Non-Intervention....73
6.2 Countermeasures....74
6.2.1 Right to Countermeasures....74
6.2.2 Restrictions on Countermeasures....77
6.2.3 Proportionality and Necessity of Countermeasures....78
6.2.4 Plea of Necessity....79
6.3 Acts of Retorsion....80
6.4 Criminal Jurisdiction....81
7 Conclusions....83

Bibliography

Treaties

Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 29 July 1899, in force 4 September 1900.

Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 18 October 1907, in force 26 January 1910.

The General Treaty for the Renunciation of War, 27 August 1928. LNTS vol. XCIV, No. 2137, 33.

Charter of the United Nations, San Francisco, 26 June 1945, in force 24 October 1945. 1 UNTS XVI.

Vienna Convention on the Law of Treaties, 23 May 1969, in force 27 January 1980. 1155 UNTS 331.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, in force 7 December 1979, 1125 UNTS 3.

Rome Statute of the International Criminal Court, 17 July 1998, in force 1 July 2002, 2187 UNTS 90.

Council of Europe Convention on Cybercrime, 23 November 2001, in force 1 July 2004, CETS No. 185.

United Nations Resolutions

General Assembly

Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, GA Res. 2131 (XX), 21 December 1965.

Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, GA Res. 2625 (XXV), 24 October 1970.

Definition of Aggression, GA Res. 3314 (XXIX), 14 December 1974.

Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, UN Doc. A/RES/42/22, 18 November 1987.

Responsibility of States for Internationally Wrongful Acts, UN Doc. A/RES/56/83, 28 January 2002.

Security Council

Resolution 678 (1990) of the Security Council, UN Doc. S/RES/678, 29 November 1990.

Resolution 836 (1993) of the Security Council, UN Doc. S/RES/836, 4 June 1993.

Resolution 1368 (2001) of the Security Council, UN Doc. S/RES/1368, 12 September 2001.

Resolution 1373 (2001) of the Security Council, UN Doc. S/RES/1373, 28 September 2001.

Resolution 1438 (2002) of the Security Council, UN Doc. S/RES/1438, 14 October 2002.

Resolution 1530 (2004) of the Security Council, UN Doc. S/RES/1530, 11 March 2004.

Resolution 1695 (2006) of the Security Council, UN Doc. S/RES/1695, 15 July 2006.

Resolution 1696 (2006) of the Security Council, UN Doc. S/RES/1696, 31 July 2006.

Resolution 1718 (2006) of the Security Council, UN Doc. S/RES/1718, 14 October 2006.

Resolution 1973 (2011) of the Security Council, UN Doc. S/RES/1973, 17 March 2011.

Other Documents

United Nations

Report of the International Law Commission on the Work of Its Eighteenth Session, UN Doc. A/6309/Rev.1 (1966).

Letter Dated 19 October 1987 from the Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council, UN Doc. S/19219.

Letter Dated 18 April 1988 from the Acting Permanent Representative of the United States to the United Nations Addressed to the President of the Security Council, UN Doc. S/19719.

Letter Dated 25 May 1993 from the Permanent Representative of the Islamic Republic of Iran to the United Nations Addressed to the Secretary-General. UN Doc. S/25843.

Letter Dated 24 July 1995 from the Charge d'Affaires A.I. of the Permanent Mission of Turkey to the United Nations Addressed to the President of the Security Council. UN Doc. S/1995/605.

Identical Letters Dated 27 June 1996 from the Charge d'Affaires A.I. of the Permanent Mission of Turkey to the United Nations Addressed to the Secretary-General and to the President of the Security Council. UN Doc. S/1996/479.

Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council. UN Doc. S/2001/946.

Report of the International Law Commission on the Work of Its Fifty-third Session, UN Doc. A/56/10 (2001).

Report of the High-Level Panel on Threats, Challenges and Change. UN Doc. A/59/565, 2 December 2004.

In Larger Freedom: Towards Development, Security and Human Rights for All, Report of the Secretary-General. UN Doc. A/59/2005.

European Union

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN[2013] 1 final), 7 February 2013, <ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667>.

National Security Strategies

Finnish Security and Defence Policy 2004, <www.defmin.fi/files/311/2574_2160_English_White_paper_2004_1_.pdf>.

Finland's Cyber Security Strategy 2013, <yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy>).

The United States International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World, May 2011, <whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

Case Law

International Court of Justice

Corfu Channel Case (UK v. Albania), Judgment, I. C. J. Reports 1949, p. 4.

North Sea Continental Shelf Cases (*Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands*), Judgment, I. C. J. Reports 1969, p. 3.

Military and Paramilitary Activities in and Against Nicaragua (*Nicaragua v. United States of America*), Judgment, I. C. J. Reports 1986, p. 14.

Territorial Dispute (Libyan Arab Jamahiriya/Chad), Judgment, I. C. J. Reports 1994, p. 6.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I. C. J. Reports 1996, p. 226.

Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea Intervening), Judgment, I. C. J. Reports 2002, p. 303.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I. C. J. Reports 2004, p. 136.

Armed Activities on the Territory of the Congo (*Democratic Republic of the Congo v. Uganda*), Judgment, I. C. J. Reports 2005, p. 168.

Armed Activities on the Territory of the Congo (New Application: 2002) (*Democratic Republic of the Congo v. Rwanda*), Jurisdiction and Admissibility, Judgment, I. C. J. Reports 2006, p. 6.

International Criminal Tribunal for the Former Yugoslavia

Prosecutor v. Furundzija, Case no. IT-95-17/1-T, ICTY Trial Chamber, Judgment (10 December 1998).

Prosecutor v. Tadić, Case no. IT-94-1-A, ICTY Appeals Chamber, Judgment (15 July 1999).

Books

Stanimir A. Alexandrov, *Self-Defense Against the Use of Force in International Law* (Kluwer Law International: The Hague, 1996).

Thomas Aquinas, *Summa Theologica, Secunda Secundae* (Benziger Brothers: New York, 1947).

Anthony Clark Arend and Robert J. Beck, *International Law and the Use of Force – Beyond the UN Charter Paradigm* (Routledge: London 1993).

Miia Aro and Jarna Petman, *Voimankäytön oikeuttaminen ja sotilaallisten järjestelmien muutokset Euroopassa ja Suomessa* (The Erik Castrén Institute of International Law, University of Helsinki, 1999).

Belatchew Asrat, *Prohibition of Force Under the UN Charter – A Study of Art. 2(4)* (Iustus Förlag: Uppsala, 1991).

Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press: Oxford, 1963).

Richard A. Clarke and Robert K. Knake, *Cyber War – The Next Threat to National Security and What to Do About It* (HarperCollins: New York, 2010).

Carl von Clausewitz, *Vom Kriege* (Rowohlt: Hamburg, 1963).

Noel Cox, *Technology and Legal Systems* (Ashgate: Farnham, 2006).

Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012).

Yoram Dinstein, *War, Aggression and Self-Defence* (5th Edition, Cambridge University Press, 2012).

Thomas M. Franck, *Recourse to Force – State Action Against Threats and Armed Attacks* (Cambridge University Press, 2002).

Tarcisio Gazzini, *The Changing Rules on the Use of Force in International Law* (Manchester University Press, 2005).

Christine Gray, *International Law and the Use of Force* (3rd Edition, Oxford University Press, 2008).

Lawrence T. Greenberg, Seymour E. Hoffman and Kevin J. Soo Hoo, *Information Warfare and International Law* (National Defense University: Washington, D.C. 1998).

Kari Hakapää, *Uusi kansainvälinen oikeus* (Talentum: Helsinki, 2005).

Lauri Hannikainen, *Peremptory Norms (Jus Cogens) in International Law – Historical Development, Criteria, Present Status* (Finnish Lawyers' Publishing Company: Helsinki, 1988).

Jason Healey and Karl Grindal (eds), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association: Arlington, 2013).

Hans Kelsen, *Collective Security Under International Law* (U.S. Naval War College: Newport, 1954).

David Kennedy, *Of War and Law* (Princeton University Press, 2006).

Peter Malanczuk and Michael Akehurst, *Akehurst's Modern Introduction to International Law* (7th Revised Edition, Routledge: London, 1997).

Hilaire McCoubrey and Nigel D. White, *International Law and Armed Conflict* (Dartmouth Publishing Company: Aldershot, 1992).

Myres S. McDougal and Florentino P. Feliciano, *Law and Minimum World Public Order* (Yale University Press: New Haven, 1961).

Lassa Oppenheim, *International Law – A Treatise. Volume I: Peace* (Longmans, Green and Co.: London, 1905).

Lassa Oppenheim, *International Law – A Treatise. Volume II: War and Neutrality* (Longmans, Green and Co.: London, 1906).

Pia Palojärvi, *A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict* (The Erik Castrén Institute of International Law, University of Helsinki, 2009).

Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013).

Malcolm Shaw, *International Law* (3rd Edition, Cambridge University Press, 1995).

Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).

Walter Gary Sharp, Sr., *Cyberspace and the Use of Force* (Aegis Research Corporation: Falls Church, 1999).

J. N. Singh, *Use of Force under International Law* (Harnam Publications: New Delhi, 1984).

Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents – Legal Considerations* (Cooperative Cyber Defence Centre of Excellence: Tallinn, 2010).

Grigorij Ivanovič Tunkin, *Recht und Gewalt im internationalen System* (Duncker & Humblot: Berlin 1986).

Alfred Verdross and Bruno Simma, *Universelles Völkerrecht – Theorie und Praxis* (Third Edition, Duncker & Humblot: Berlin, 1984).

Daniel Webster and Edward Everett, *The Works of Daniel Webster – Volume VI* (10th Edition, Little, Brown and Company: Boston, 1857).

Book Chapters

John Arquilla and David Ronfeldt, 'Cyberwar is Coming!', in John Arquilla and David Ronfeldt (eds), *In Athena's Camp – Preparing for Conflict in the Information Age* (Rand Corporation: Santa Monica, 1997), 23–60.

Alan Boyle, 'Soft Law in International Law-Making', in Malcolm D. Evans (ed.), *International Law* (3rd Edition, Oxford University Press, 2010), 122–140.

Jeffery L. Caton, 'Exploring the Prudent Limits of Automated Cyber Attack', in K. Podins, J. Stinissen, M. Maybaum (eds), *2013 5th International Conference on Cyber Conflict Proceedings* (NATO CCD COE Publications: Tallinn, 2013), 145–160.

Martti Koskenniemi, 'Colonization of the “Indies”: The Origin of International Law?', in Yalanda Gamarra (ed.), *La idea de la América en el pensamiento ius internacionalista del siglo XXI* (Institución Fernando el Católico: Zaragoza, 2010), 43–63.

Jochen Frowein and Nico Krisch, 'Article 41', in Bruno Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2nd Edition, Oxford University Press, 2002), 735–749.

Jochen Frowein and Nico Krisch, 'Article 43', in Bruno Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2nd Edition, Oxford University Press, 2002), 760–763.

Robin Geiß and Henning Lahmann, 'Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention', in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy* (NATO CCD COE Publications: Tallinn, 2013), 621–657.

Keir Giles and William Hagestad II, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English', in K. Podins, J. Stinissen, M. Maybaum (eds), *2013 5th International Conference on Cyber Conflict Proceedings* (NATO CCD COE Publications: Tallinn, 2013), 413–429.

Terry D. Gill, 'Non-Intervention in the Cyber Context', in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy* (NATO CCD COE Publications: Tallinn, 2013), 217–238.

Elzbieta Mikos-Skuza, 'International Law's Changing Terms: "War" Becomes "Armed Conflict"', in Mary Ellen O'Connell (ed.), *What Is War? An Investigation in the Wake of 9/11* (Martinus Nijhoff Publishers: Leiden, 2012) 19–29.

Albrecht Randelzhofer, 'Article 2(4)', in Bruno Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2nd Edition, Oxford University Press, 2002), 112–136.

Albrecht Randelzhofer, 'Article 51', in Bruno Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2nd Edition, Oxford University Press, 2002), 788–806.

Jari Rantapelkonen, 'Informaatiosodan monet kasvot', in Jyri Raitasalo and Joonas Sipilä (eds), *Sota – teoria ja todellisuus. Näkökulmia sodan muutokseen* (National Defence University: Helsinki, 2008), 63–89.

Georg Ress, 'Interpretation', in Bruno Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2nd Edition, Oxford University Press, 2002), 13–32.

Michael N. Schmitt, 'Responding to Transnational Terrorism under the Jus ad Bellum', in Michael N. Schmitt and Jelena Pejic (eds), *International Law and Armed Conflict: Exploring the Faultlines – Essays in Honour of Yoram Dinstein* (Martinus Nijhoff Publishers: Leiden, 2007), 157–195.

Michael N. Schmitt, 'Cyber Activities and the Law of Countermeasures', in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy* (NATO CCD COE Publications: Tallinn, 2013), 659–690.

Michael N. Schmitt, 'The "Use of Force" in Cyberspace: A Reply to Dr. Ziolkowski', in C. Czossek, R. Ottis and K. Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict Proceedings* (NATO CCD COE Publications: Tallinn, 2012), 311–317.

Joonas Sipilä, 'Puuneista Bastioneihin – Sota ja historialliset esimerkit', in Jyri Raitasalo and Joonas Sipilä (eds), *Muuttuva sota* (National Defence University: Helsinki, 2005), 25–54.

Kari Takamaa, 'Verkkosodankäyntiin liittyviä kansainvälisoikeudellisia ongelmia – oikeudellisen sääntelyn perusteiden kartoitusta', in Timo Koivurova (ed.), *Kansainvälistyvä oikeus – Juhlakirja, professori Kari Hakapää* (University of Lapland: Rovaniemi, 2005), 517–549.

Kari T. Takamaa, 'Sodankäyntiä järjestävän kansainvälisen oikeuden muutos – onko mikään muuttunut?', in Jyri Raitasalo and Joonas Sipilä (eds), *Muuttuva sota* (National Defence University: Helsinki, 2005), 55–100.

Hugh Thirlway, 'The Sources of International Law', in Malcolm D. Evans (ed.), *International Law* (3rd Edition, Oxford University Press, 2010), 95–121.

Nigel White and Ademola Abass, 'Countermeasures and Sanctions', in Malcolm D. Evans (ed.), *International Law* (3rd Edition, Oxford University Press, 2010), 531–558.

Katharina Ziolkowski, 'Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force', in C. Czossek, R. Ottis and K. Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict Proceedings* (NATO CCD COE Publications: Tallinn, 2012), 295–309.

Articles

Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification?', 1 *Goettingen Journal of International Law* (2009) 375–396.

Derek W. Bowett, 'Economic Coercion and Reprisals by States', 13 *The Virginia Journal of International Law* (1972) 1–12.

Derek W. Bowett, 'Reprisals Involving Recourse to Armed Force', 66 *The American Journal of International Law* (1972) 1–36.

Davis Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict', 47 *Harvard International Law Journal* (2006) 179–221.

Antonio Cassese, 'Ex iniuria ius oritur: Are We Moving Towards International Legitimation of Forcible Humanitarian Countermeasures in the World Community?', 10 *European Journal of International Law* (1999) 23–30.

Yoram Dinstein, 'Computer Network Attacks and Self-Defense', 76 *U.S. Naval War College International Law Studies* (2002) 99–119.

T. D. Gill, 'The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy', 11 *Journal of Conflict & Security Law* (2006) 361–369.

Emanuela-Chiara Gillard, 'Business Goes to War: Private Military/Security Companies and International Humanitarian Law', 88 *International Review of the Red Cross* (2006) 525–572.

Michael Gervais, 'Cyber Attacks and the Laws of War', 30 *Berkley Journal of International Law* (2012) 525–579.

James A. Green, 'Questioning the Peremptory Status of the Prohibition of the Use of Force', 32 *Michigan Journal of International Law* (2011) 215–257.

Oona Hathaway, Rebecca Crootof, William Perdue and Philip Levitz, 'The Law of Cyber-Attack', 100 *California Law Review* (2012) 817–885.

Michael V. Hayden, 'The Future of Things "Cyber"', 5 *Strategic Studies Quarterly* (1/2011) 3–7.

Louis Henkin, 'The Reports of the Death of Article 2(4) Are Greatly Exaggerated', 65 *The American Journal of International Law* (1971) 544–548.

Duncan B. Hollis, 'Why States Need an International Law for Information Operations', 11 *Lewis & Clark Law Review* (2007) 1023–1061.

Maziar Jamnejad and Michael Wood, 'The Principle of Non-intervention', 22 *Leiden Journal of International Law* (2009) 345–381.

Eric Talbot Jensen, 'Computer Network Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense', 38 *Stanford Journal of International Law* (2002) 207–240.

Carin Kahgan, 'Jus Cogens and the Inherent Right to Self-Defense', 3 *ILSA Journal of International & Comparative Law* (1997) 767–827.

Sean P. Kanuck, 'Information Warfare: New Challenges for Public International Law', 37 *Harvard International Law Journal* (1996) 272–292.

Michael J. Kelly, 'Time Warp to 1945 – Resurrection of the Reprisal and Anticipatory Self-Defense Doctrines in International Law', 13 *Journal of Transnational Law and Policy* (2003) 1–39.

Harold Hongju Koh, 'International Law in Cyberspace', 54 *Harvard International Law Journal Online* (2012).

Martti Koskenniemi, 'Oikeus ja asevoiman käyttö uudessa maailmassa', *Lakimies* 1/2003 90–95.

Martti Koskenniemi, 'The Lady Doth Protest too Much' – Kosovo, and the Turn to Ethics in International Law', 65 *The Modern Law Review* (2002) 159–175.

Sheng Li, 'When Does Internet Denial Trigger the Right of Armed Self-Defense', 38 *Yale Journal of International Law* (2013) 179–216.

Ulf Linderfalk, 'The Effect of Jus Cogens Norms: Whoever Opened Pandora's Box, Did You Ever Think About the Consequences?', 18 *The European Journal of International Law* (2008) 853–871.

Janne Malkki, 'Kuinka sota muuttuu?', *Kosmopolis*, Vol. 37:3/2007 42–58.

Sean D. Murphy, 'Protean Jus Ad Bellum', 27 *Berkeley Journal of International Law* (2009) 22–52.

Reese Nguyen, 'Navigating *Jus Ad Bellum* in the Age of Cyber Warfare', 101 *California Law Review* (2013) 1079–1131.

Bradley Raboin, 'Corresponding Evolution: International Law and the Emergence of Cyber Warfare', 31 *Journal of National Association of Administrative Law Judiciary* (2011) 602–668.

Horace B. Robertson, Jr., 'Self-Defense Against Computer Network Attack Under International Law', 76 *U.S. Naval War College International Law Studies* (2002) 121–145.

Marco Roscini, 'World Wide Warfare – Jus ad bellum and the Use of Cyber Force', 14 *Max Planck Yearbook of United Nations Law* (2010) 85–130.

Arie J. Schaap, 'Cyber Warfare Operations: Development and Use Under International Law', 64 *Air Force Law Review* (2009) 123–173.

Oscar Schachter, 'In Defense of International Rules on the Use of Force', 53 *University of Chicago Law Review* (1986) 113–146.

Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', 37 *Columbia Journal of Transnational Law* (1999) 885–937.

Michael N. Schmitt, 'Cyber Operations and the Jus Ad Bellum Revisited', 56 *Villanova Law Review* (2011) 569–605.

Michael N. Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed', 54 *Harvard International Law Journal Online* (2012).

Scott Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', 27 *Berkeley Journal of International Law* (2009) 192–251.

Daniel B. Silver, 'Computer Network Attack as a Use of Force Under Article 2(4)', 76 *U.S. Naval War College International Law Studies* (2002) 73–97.

Abraham D. Sofaer, 'On the Necessity of Pre-emption', 14 *European Journal of International Law* (2003) 209–226.

William H. Taft, 'Self-Defense and the Oil Platforms Decision'. 29 *Yale Journal of International Law* (2004) 295–306.

Li Zhang, 'A Chinese Perspective on Cyber War', 94 *International Review of the Red Cross* (2012) 801–807.

News Articles and Reports

Felix Reichmann, 'The Pennsylvania Rifle: A Social Interpretation of Changing Military Techniques', *The Pennsylvania Magazine of History and Biography*, January 1945.

Brian Krebs, 'A Short History of Computer Viruses and Attacks', *The Washington Post*, 14 February 2003, <www.washingtonpost.com/wp-dyn/articles/A50636-2002Jun26.html>.

Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', *The Guardian*, 17 May 2007 <www.theguardian.com/world/2007/may/17/topstories3.russia>.

John Markoff and Thom Shanker, 'Halted '03 Iraq Plan Illustrates U.S. Fear of Cybewar Risk', *The New York Times*, 1 August 2009, <www.nytimes.com/2009/08/02/us/politics/02cyber.html>.

'War in the Fifth Domain', *The Economist*, 1 July 2010, <economist.com/node/16478792>.

Kim Zetter, 'Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target', *Wired*, 23 September 2010, <www.wired.com/threatlevel/2010/09/stuxnet/>.

Liam O Murchu, 'Stuxnet Using Three Additional Zero-Day Vulnerabilities', *Symantec Official Blog*, 14 September 2010, <www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities>.

Josh Halliday, 'Stuxnet Worm is the "Work of a National Government Agency"', *The Guardian*, 24 September 2010, <www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency>.

Erik Chien, 'Stuxnet: A Breakthrough', *Symantec Blog,* 12 November 2010, <www.symantec.com/connect/blogs/stuxnet-breakthrough>.

Nicolas Falliere, Liam O Murchu and Eric Chien, 'W32.Stuxnet Dossier', *Symantec Security Response Whitepaper*, Version 1.4, 11 February 2011, <www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

Charles Arthur and Keith Stuart, 'PlayStation Network Uses Fear Identity Theft After Major Data Leak', *The Guardian*, 27 April 2011, <theguardian.com/technology/2011/apr/27/playstation-users-identity-theft-data-leak>.

Noah Shachtman and Peter W. Singer, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive', *Brookings Institution*, 15 August 2011, <www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman>.

Kim Zetter, 'How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History', *Wired*, 7 November 2011, <www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/>.

Andy Greenberg, 'Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits', *Forbes*, 23 March 2012, <www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>.

'"Red October" Diplomatic Cyber Attacks Investigation', *Kaspersky Lab SecureList*, 14 January 2013, <securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation>.

Jarno Limnéll, 'Defining the Qualities of Cyber Warfare', *SC Magazine*, 11 March 2013, <www.scmagazine.com/defining-the-qualities-of-cyber-warfare/article/283902/>.

Heidi Moore and Dan Roberts, 'AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging', *The Guardian*, 23 April 2013, <www.guardian.co.uk/business/2013/apr/23/ap-tweet-hack-wall-street-freefall>.

Sean Gallagher, 'Smart Toilet Vulnerable to Bluetooth Flushing Hack', *Wired*, 5 August 2013, <www.wired.co.uk/news/archive/2013-08/05/toilet-hack-attack>.

Ralph Langner, *To Kill a Centrifuge – A Technical Analysis of What Stuxnet's Creators Tried to Achieve*, November 2013, <www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>.

1 Introduction

1.1 Introduction to the Issue

Wars frequently make use of new technological advancements. They might be smaller, incremental developments such as more accurate traditional kinetic weapons like rifles or missiles, or they might be new types or improved vehicles like drones or stealth bombers. However new and improved, these kinds of weapons basically are means for achieving the same goals as before – in many ways it is trivial whether a missile is launched from a traditional fighter jet, a ship or an unmanned drone piloted from afar. These developments rarely are uncontroversial, either in a legal or a moral sense. The introduction of firearms was met by calls of cowardice: instead of bravely meeting and fighting within arm's and sword's length, the musket allowed for inflicting death and damage from afar.[1] Ballistic missiles made it possible to strike targets beyond the horizon, and now much debate revolves around unmanned aerial vehicles also known as drones. The laws of war adjust to the new technical developments. In 1868 the Saint Petersburg Declaration[2] banned the use of explosive projectiles weighing under 400 grammes and since then numerous different treaties have been concluded to regulate or completely ban the use of different kinds of weapons.

Especially the modern western societies are highly networked and reliant on computers in nearly everything ranging from hospitals to factories and from banks to nuclear reactors. Lest there be any doubt about the pervasiveness of connected devices, in August 2013 the security company Trustwave issued a security advisory after it found a vulnerability in a toilet seat. Because of lax security, a malicious user could use a smartphone to open or close the lid, flush the toilet or activate air-drying.[3] The connectivity of devices provides an attack surface unimaginable just a couple of decades ago. States have increasingly paid attention to securing the critical infrastructure from cyber attacks but also considered the

1 Felix Reichmann, 'The Pennsylvania Rifle: A Social Interpretation of Changing Military Techniques', *The Pennsylvania Magazine of History and Biography*, January 1945 at 6.

2 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, 11 December 1868.

3 Sean Gallagher, 'Smart Toilet Vulnerable to Bluetooth Flushing Hack', *Wired*, 5 August 2013 <www.wired.co.uk/news/archive/2013-08/05/toilet-hack-attack>. References to online sources are accurate as of 6 January 2014.

need for offensive capabilities. A state-run cyber army running attacks with direct consequences in the physical world has come far from the stereotype of the 1990s, an individual malicious computer enthusiast or a group writing viruses to claim fame among their peers.

Even though cyber operations have not so far played a major part in any larger conflict, it has been widely claimed that several countries are faced with vulnerable systems and that it might only be a matter of time until an enemy – be it a state or a non-state actor such as a terrorist group – uses its cyber capabilities either as the primary way of attacking or as a supplementary way to wreak havoc. The consequences of such attacks are by no means limited to the virtual world and may very well be significant for both civilians and soldiers.

Cyber attacks have several characteristics that separate them from traditional uses of force, which has implications for applying the existing legal framework on the use of force to them. A cyber attack might for example last only portions of a second and the source of the attack might be masked. The legal framework has its roots in the more traditional ways of waging war between nation-states and some of the problems emanating from cyber attacks follow the same lines of thought as the issues which have been discussed after the terrorist attacks of 11 September 2001 (hereafter referred to as the 9/11 attacks) regarding, among other things, non-state actors and the possibility of pre-emptive self-defence.

Cyber warfare has been a hot issue especially after the events in Estonia in 2007 and the discovery of Stuxnet, both of which will be introduced in the following pages. The dangers of cyber attacks have even been compared to the consequences of nuclear war with hyperbolic tones.[4] While it is true that the ultimate worst case cyber scenarios may include consequences comparable even to nuclear war, focusing on them has the tendency of misguiding the discussion from the arguably more common and more probable consequences of cyber operations. To quote former U.S. intelligence chief Michael Hayden, rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon.[5] While the discussion about cyber

4 For an overview of the problems with Cold War metaphors regarding cyber war, see Noah Shachtman and Peter W. Singer, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive', *Brookings Institution*, 15 August 2011, <www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman>.

5 Michael V. Hayden, 'The Future of Things "Cyber"', 5 *Strategic Studies Quarterly* (1/2011) 3–7 at 3.

attacks has been especially lively recently, the attacks and threats themselves are not a completely new phenomenon.[6] Already in 1993 John Arquilla and David Ronfeldt envisioned that information technology would be the technological breakthrough to bring about the 'next major shift in the nature of conflict and warfare'.[7]

The laws of war are not the only aspect of law being challenged by technological changes.[8] The possibility to make exact copies of digital media and easily disseminate them has challenged the conventional conceptions of copyright and the possibility to gather data in a scale unimaginable before poses a new kind of test for the protection of privacy, just to name two obvious examples. On a wider scale, the diminution of the significance of national borders brought on by the internet makes it more difficult to apply the traditional concept of territorial jurisdiction.[9] Whatever the challenges may be, they neither mean that the technology is immune to the legal system nor that the legal system is immune to the technology.[10] The same applies to *jus ad bellum* – the law concerning the resort to force by states – and cyber operations: the existing rules apply, but they may need to be interpreted in new ways and supplementary new rules may need to be agreed upon.

In this thesis I will examine the relationship of cyber operations and current international law in terms of *jus ad bellum*. First I shall discuss the terminology regarding the subject and present example cases which I will later refer to. I will then briefly present the history and evolution of the regulation of war leading from the *bellum justum* doctrine to the current system built around the Charter of the United Nations[11]. Then the much debated notions of force an armed attack will be examined, both of which are essential to the question of legality of military action. There is no agreed upon definition for either of the terms, and both will be discussed in the context of cyber operations. The aim is to determine if and when cyber operations may constitute a use of force or an armed attack.

---

6 In fact, September 2013 marked the release of the first history of cyber conflict: Jason Healey and Karl Grindal (eds), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association: Arlington, 2013).

7 John Arquilla and David Ronfeldt, 'Cyberwar is Coming!', in John Arquilla and David Ronfeldt (eds), *In Athena's Camp – Preparing for Conflict in the Information Age* (Rand Corporation: Santa Monica, 1997), 23–60 at 24–25, reprinted from 12 *Comparative Strategy* (1993) 141–165.

8 For an overview of the implications of the development of technology to legal systems see Noel Cox, *Technology and Legal Systems* (Ashgate: Farnham, 2006).

9 Cox, *Technology and Legal Systems*, *supra* note 8 at 172–173.

10 Cox, *Technology and Legal Systems*, *supra* note 8 at 217.

11 Charter of the United Nations, 26 June 1945, in force 24 October 1945, 1 UNTS XVI.

After this, I will shortly address the principle of non-intervention and discuss if and how it complements the *jus ad bellum* regarding operations falling short of the threshold of force. Finally, concluding remarks and some views towards the future of the issue will be presented.

1.2 Terminology

'Cyber warfare' has become an ominous catchphrase used especially in the media but also in the context of international law in a variety of contexts not all of which are appropriate or fitting.[12] It is very often referred to in situations more aptly described as espionage, be that commercial or targeted at military intelligence. Just as often it is used in describing activities of smaller scale with such consequences that they have little if anything to do with warfare, as in the case of the attacks against Estonia in 2007.[13] I will go through some of the terminology and definitions used in discussing the subject matter as well as argue what I consider to be their strengths and weaknesses.

'Information warfare' has been used to describe attacks and operations carried out via computer networks, although it seems that lately the term has been more or less replaced by first the notion of 'computer network attacks' and now, by 'cyber attacks'. Information warfare more aptly describes the battle of words and images.[14] Hence, the term has more to do with propaganda than with what now is referred to as cyber operations. This is also how information warfare has previously and widely been understood.[15] Fitting some of the newer attacks and developments into the concept of information warfare is problematic. It is theoretically possible to stretch the definition of information so that the target of a cyber attack is indeed the information resident in the memory of a computer, but it is forced and far-fetched. Also, it does not seem practical to group together traditional information warfare (such as propaganda) with newer forms of attacks, such as those targeting

12 Katharina Ziolkowski, 'Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force' in C. Czosseck, R. Ottis and K. Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict Proceedings* (NATO CCD COE Publications: Tallinn, 2012), 295–309 at 296.

13 For a description of the events see *infra* at 13.

14 Jari Rantapelkonen, 'Informaatiosodan monet kasvot' in Jyri Raitasalo & Joonas Sipilä (eds), *Sota – teoria ja todellisuus: Näkökulmia sodan muutokseen* (National Defence University: Helsinki, 2008) at 65.

15 As an example, The Finnish Security and Defence Policy 2004 defines information warfare as the use of information environment to influence decision-making, operability and public opinion. Finnish Security and Defence Policy 2004, <www.defmin.fi/files/311/2574_2160_English_White_paper_2004_1_.pdf> at 162.

industrial control systems and for which the objectives and outcomes are much different. Attacks against the network infrastructure would fit under the concept of information warfare more easily, especially if their ultimate aim is to disrupt the flow of information. Indeed, the communications networks were seen early on as a probable targets of cyber attacks.[16] It has also been argued that cyber operations and computer network attacks should be understood as one of the main capabilities of information warfare.[17] This is a reasonable claim from the perspective of information warfare, yet it should be clarified that this should only refer to those cyber operations whose goals pertain to information warfare. Not all cyber operations have such goals, and those that do not (such as an attack on the air traffic control system intended to crash aircraft or an attack on industrial control systems intended to cause an explosion) should not be forced into the category of information warfare.

Also frequently used is the term 'computer network attack' (or CNA). This is often an appropriate and aptly descriptive term, but it also seems in some cases too strict regarding the *network* part. Some of the critical infrastructure might be disconnected from the internet or any other network as part of security measures, yet these systems can very well be – and have been – targeted by a cyber attack. For example one of the main propagation methods of the Stuxnet malware which hit an Iranian nuclear facility was spreading via removable USB drives.[18] The use of the term 'computer network attack' also seems to be declining in favour of the term 'cyber attacks'.[19]

Richard A. Clarke and Robert K. Knake define cyber warfare as 'actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or

16 Sean P. Kanuck, 'Information Warfare: New Challenges for Public International Law', 37 *Harvard International Law Journal* (1996) 272–292 at 284.

17 See e.g. (in the context of law of armed conflict) Pia Palojärvi, *A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict* (The Erik Castrén Institute of International Law, University of Helsinki, 2009) at 3, Kari Takamaa, 'Verkkosodankäyntiin liittyviä kansainvälisoikeudellisia ongelmia – oikeudellisen sääntelyn perusteiden kartoitusta' in Timo Koivurova (ed.), *Kansainvälistyvä oikeus – Juhlakirja, professori Kari Hakapää* (University of Lapland: Rovaniemi 2005) 517–549 at 522–523 and Marco Roscini, 'World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force', 14 *Max Planck Yearbook of United Nations Law* (2010) 85–130 at 91.

18 Nicolas Falliere, Liam O Murchu and Eric Chien, 'W32.Stuxnet Dossier', *Symantec Security Response Whitepaper*, Version 1.4, 11 February 2011, <www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf> at 29. For a more detailed description of Stuxnet see *infra* at 14.

19 An obvious example is the use of the term by Michael Schmitt, who used the term 'computer network attacks' in a 1999 article (*infra* note Error: Reference source not found) but has since used the terms 'cyber operations', 'cyber attacks' and 'cyber war(fare)' (see e.g. *infra* note 190).

disruption'.[20] It bears resemblance with the definition of a cyber attack set forth in the Tallinn Manual, a study of international law applicable to cyber attacks published by the NATO Cooperative Cyber Defence Centre of Excellence: 'a cyber attack is an operation – – that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[21] It is, in other words, a cyber operation whose consequences are expected to exceed a certain threshold. A cyber operation is defined in the Tallinn Manual as the 'employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace'.[22] Clarke and Knake refer to 'warfare' whereas the Tallinn Manual defines 'attacks'. The difference is explained by context: Clarke and Knake talk about war in a broader, more traditional sense and in its definition the Tallinn Manual discusses individual attacks or operations. For the purposes of this thesis, I will subscribe to the definition of cyber operation set forth in the Tallinn Manual and use the term cyber operation to describe a variety of actions targeting computers and networks without prejudice to their legality or illegality.

Another kinds of suggestions have been made as well, such as defining 'cyber warfare operations' as 'the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state'[23]. This, however, seems on the one hand too broad: 'denying' information may be seen as referring to for example denial-of-service attacks, which generally should not, as will be discussed later in further detail, be seen neither as uses of force nor armed attacks.[24] On the other hand, it seems too strict. Limiting the acts to those done to computers *of* another state seems counterproductive as much of the infrastructure is privately owned and such civilian networks or computers can in certain cases be legitimate military targets.[25]

---

20 Richard A. Clarke – Robert K. Knake, *Cyber War – The Next Threat to National Security and What to Do About It* (HarperCollins: New York, 2010) at 6.

21 Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013) at 106. The term is defined in the context of international humanitarian law and in reference to the term 'attack' used in the Geneva Conventions.

22 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 258.

23 Arie J. Schaap, 'Cyber Warfare Operations: Development and Use Under International Law', 64 *Air Force Law Review* (2009) 123–173 at 127. The definition is based on an older version of a U.S. Department of Defense Dictionary of Military & Associated Terms.

24 *Infra* at 63.

25 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 128–129, applying Article 27 of the Hague Regulations (Convention [IV] Respecting the Laws and Customs of War on Land and its annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 18 October 1907, in force

The translation of the relevant terms presents another terminological challenge and the lack of agreed upon terms and concepts complicates international co-operation. Such key terms and concepts as 'cyber warfare' or 'information warfare' have different meanings in English, Russian and Chinese, and there are terms for which no clear equivalent exists in other languages. For example the Russian terminology includes the broad notion of an 'information weapon', which refers to, among other things, mass media propaganda. This relates to the notion of 'information warfare', whose meaning in Russian and Chinese differs from the one in English and is more broad and holistic.[26] Such issues have made it difficult to agree on common definitions,[27] and would arguably make it even more difficult to for example bring about a treaty on the issue of cyber attacks.

1.3 Applicability of the Existing Rules

There seems to be an emerging consensus that even though cyber attacks have certain special characteristics that set them in some ways apart from kinetic uses of force, the principles of international law apply to them as well.[28] The International Court of Justice (ICJ) stated in the *Nuclear Weapons* Advisory Opinion that the United Nations Charter provisions on the use of force apply to any use of force regardless of the weapons employed.[29] In the realm of *jus in bello* – the law concerning the conduct of hostilities – a similar concept is expressed in the so-called Martens Clause, which was first formulated in the preamble of the 1899 Hague Convention II[30] and restated in 1977 in its modern form in Article 1(2) of the Additional Protocol I to the Geneva Conventions:[31] 'in cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived

---

26 January 1910) to a cyber context.

26 Keir Giles and William Hagestad II, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' in K. Podins, J. Stinissen, M. Maybaum (eds), *2013 5th International Conference on Cyber Conflict Proceedings* (NATO CCD COE Publications: Tallinn, 2013), 413–429 at 420–422.

27 Giles and Hagestad, *Divided by a Common Language*, *supra* note 26 at 416–417.

28 See e.g. Harold Koh, 'International Law in Cyberspace', 54 *Harvard International Law Journal Online* (2012) at 3 and Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 75–76.

29 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, p. 22 at para. 39.

30 Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 29 July 1899, in force 4 September 1900.

31 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, in force 7 December 1979, 1125 UNTS 3.

from established custom, from the principles of humanity and from the dictates of public conscience'. The International Court of Justice referred to the clause in the *Nuclear Weapons* Advisory Opinion and stated that it has proved to be an effective means of addressing the rapid evolution of military technology.[32]

States have taken a similar position as well: for example the United States Cyber Strategy notes that existing international law does apply in cyberspace in times of peace and of conflict but recognizes the need for additional clarification regarding some of the unique aspects of cyber operations.[33] The strategy also states that the United States will respond to hostile acts in cyberspace as to any other threat.[34] China has taken a similar position, perhaps more underlining the need for revision and clarification.[35]

There have been calls for a specific convention on cyber warfare (or information warfare in general),[36] and such calls are not entirely without merit. There is for example an especially grey area under the threshold of force or an armed attack and regulating the acts falling to that category would certainly benefit from a new convention. Another area that would probably benefit from a treaty is the use of civilian contractors to carry out cyber attacks. This, however, is not a question specifically and exclusively related to cyber operations: the use of contractors has been the subject of a debate especially after the use of private military companies in Afghanistan and Iraq during the post-9/11 war on terrorism.[37]

One argument for the insufficiency of current international law and the need for a completely new treaty system is based on the non-physical nature of the cyber domain.[38]

---

32 *Nuclear Weapons, supra* note 29 at para. 78.

33 The United States International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World, May 2011, <www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> at 9.

34 The United States International Strategy for Cyberspace, supra note 33 at 14.

35 Li Zhang, 'A Chinese Perspective on Cyber War', 94 *International Review of the Red Cross* (2012) 801–807 at 804.

36 See e.g. Daniel B. Silver, 'Computer Network Attack as a Use of Force Under Article 2(4)', 76 *U.S. Naval War College International Law Studies* (2002) 73–97 at 94 and Oona Hathaway, Rebecca Crootof, William Perdue and Philip Levitz, 'The Law of Cyber-Attack' in 100 *California Law Review* (2012) 817–885 at 877 and more in the context of law of armed conflict, Davis Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict', 47 *Harvard International Law Journal* (2006) 179–221.

37 See e.g. Emanuela-Chiara Gillard, 'Business Goes to War: Private Military/Security Companies and International Humanitarian Law', 88 *International Review of the Red Cross* (2006), 525–572.

38 Duncan B. Hollis, 'Why States Need an International Law for Information Operations', 11 *Lewis & Clark Law Review* (2007) 1023–1061 at 1039–1040 and Bradley Raboin, 'Corresponding Evolution: International Law and the Emergence of Cyber Warfare', 31 *Journal of the National Association of*

Such a view overemphazises the disconnect between the cyber domain and the four other domains of warfare – land, sea, air and space. While some operations indeed can be carried out so that they have implications exclusively in the cyber domain, it is particularly the physical consequences of the attacks that have been at the centre of the discussion and can cause significant devastation. Another call of insufficiency rests upon the claim that the United Nations Charter system places too much reliance on the concepts of sovereign control and the established state responsibility, which are somewhat problematic in the context of cyber operations.[39] Such a claim is indeed not unfounded, yet it too much disregards the possibility of overcoming the challenges within the current system. It also places much faith on a political level in the possibility of reaching a new treaty and on a legal level in the possibility of finding a solution that would not lead out of the frying pan into the fire.

Administrative Law Judiciary (2011) 602–668 at 625.

39 Scott Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', 27 *Berkeley Journal of International Law* (2009) 192–251 at 197–198.

2 Evolvement of War and Cyber Attacks

2.1 Evolvement of the Notion of War

The emergence of cyber attacks and the problem of categorizing them as warfare relates to the more broad discussion about the definition of war and its evolvement. Lassa Oppenheim's definition of war from the beginning of the 20th century is an example of a traditional one. He defines war as 'the contention between two or more states through their armed forces for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases'.[40] The nature of warfare has changed considerably since the days of Oppenheim, and there have been several efforts to modernize the definition of war. Yoram Dinstein provides one version, and defines war as 'a hostile interaction between two or more States, either in a technical or in a material sense'. He considers war in a technical sense to be a formal status following a declaration of war. War in the material sense is about the actual use of armed force, 'which must be comprehensive on the part of at least one party to the conflict'.[41] The requirement of comprehensive force seems to be meant to distinguish incidents of smaller scale from war. Even though the definition of Dinstein is a more modern one, it still is firmly based in the traditional concept of nation-states waging war against each other.

The time period from the end of the Second World War has been marked by several changes in the context of war, among which is a shift in the terminology: large scale hostilities have increasingly been referred to as armed conflicts instead of wars.[42] The end of the Cold War opened up the paradigm of war for change and much of the changes indeed have happened since the end of the Cold War.[43] These include a reduction in the number of wars, especially the inter-state wars, and the geographical focusing of war to

40 Lassa Oppenheim, *International Law – A Treatise. Volume II: War and Neutrality* (Longmans, Green and Co.: London, 1906) at 56.

41 Yoram Dinstein, *War, Aggression and Self-Defence* (5th Edition, Cambridge University Press, 2012) at 15.

42 Elzbieta Mikos-Skuza, 'International Law's Changing Terms: “War” Becomes “Armed Conflict”' in Mary Ellen O'Connell (ed.), *What Is War? An Investigation in the Wake of 9/11* (Martinus Nijhoff Publishers: Leiden, 2012) 19–29 at 23.

43 Jyri Raitasalo, 'Läntinen sodan kuva kylmän sodan jälkeen' in Jyri Raitasalo and Joonas Sipilä (eds), *Muuttuva sota* (National Defence University: Helsinki, 2005) 101–125 at 101.

certain regions. Intra-state conflicts have been relatively prevalent, and increasingly professionalized armies have taken advantage of new military technology.[44]

In a sense, the post-Cold War era ended after the 9/11 terrorist attacks.[45] After the attacks, transnational terrorism has risen to the forefront of the threat debate and the notion of war has become even more diffuse and ambiguous.[46] The attacks were labelled as an 'act of war' by U.S. president George W. Bush on the day following the attacks,[47] and the response was labelled a 'war on terror'.[48] The attacks were also referred to as 'acts of war against the United States of America and its allies' in the U.S. National Strategy for Combating Terrorism of February 2003.[49]

War has not only been used to describe combat but also struggles of different kinds, such as the war on drugs. David Kennedy distinguishes wars of combat from wars of metaphor and notes that their distinction has blurred. An example of this blurring is the aforementioned war on terror: the opponent is more indeterminate yet the war is fought with military force. The debate about whether the terrorist detainees should be treated as prisoners of war, unlawful enemy combatants or criminals is also indicative of this.[50] All this points to the fact that the traditional concept of war has fragmented since the end of the Cold War and no clear and uniform concept has emerged in its place.[51]

The cyber world has often been described as the fifth domain of warfare, the newest addition to those of land, sea, air and space.[52] Such a characterization is, however, somewhat misleading.[53] In reality, the cyber domain is is not disconnected from the other four but quite the opposite, as it is closely related to them and forms an integral part of

---

44 Janne Malkki, 'Kuinka sota muuttuu?', *Kosmopolis Vol. 37:3/2007,* 42–58 at 49.
45 Raitasalo, *Läntinen sodan kuva kylmän sodan jälkeen*, *supra* note 43 at 107.
46 Raitasalo, *Läntinen sodan kuva kylmän sodan jälkeen*, *supra* note 43 at 114.
47 BBC News, *Text of Bush's Act of War Statement*, 12 September 2001, <news.bbc.co.uk/2/hi/americas/1540544.stm>.
48 Address by President Bush to the Joint Session of the 107th Congress, 20 September 2001, in Selected Speeches of President George W. Bush 2001–2008, <georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Selected_Speeches_George_W_Bush.pdf> at 68.
49 U.S. National Strategy for Combating Terrorism, February 2003, <www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf> at 1.
50 David Kennedy, *Of War and Law* (Princeton University Press, 2006) at 3–4.
51 Raitasalo, *Läntinen sodan kuva kylmän sodan jälkeen*, *supra* note 43 at 122.
52 See e.g. 'War in the Fifth Domain', *The Economist*, 1 July 2010, <www.economist.com/node/16478792>.
53 For a more detailed critique of such a view, see Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013) at 165–166.

them: for example many kinetic weapons and communications systems utilize computer networks.[54] Further discussion of the development of the concept and definition of war is outside the scope of this thesis, but suffice it to say that the emergence of cyber attacks is a part of the evolution and continuum of armed conflict and warfare. Like other similar developments, it too has implications for the regulation of war.

2.2 History and Types of Malware and Cyber Attacks

Malicious software, malware in short, has existed since the 1970s and spread on floppy disks and through bulletin board systems well before the internet was widely used. The early 2000s saw several widespread computer virus epidemics such as Love Letter, Code Red, Nimda and MyDoom.[55] These viruses were of varying levels of sophistication and generally their goal was to spread as wide as possible without a specific target. Some deleted or stole data from infected machines, some made their existence known in other ways and some were relatively unobtrusive. Another form of computer attacks are the more targeted strikes, such as the 2011 attack on Sony's PlayStation Network which resulted in the theft of credit card and other information of over 77 million users and an outage of almost a month.[56] Popular attacks have consisted of defacing the public websites of news organizations or governments or faking login sites in order to get login credentials from users. Some attackers might have been after sensitive or confidential information ranging from credit card information to nude photos of celebrities, some were after fame.

These kinds of viruses and attacks have generally been the product of individuals or groups and have not required very much resources, apart from time and skill. In the past few years however, much more carefully crafted attacks have been discovered. Some have even been so sophisticated and required so much resources to develop that computer security analysts all but agree that they must be a product of a state or at least the development must have been sponsored by a state.

---

54 Jarno Limnéll, 'Defining the Qualities of Cyber Warfare', *SC Magazine*, 11 March 2013, <www.scmagazine.com/defining-the-qualities-of-cyber-warfare/article/283902/>.

55 For an overview of the different epidemics see e.g. Brian Krebs, 'A Short History of Computer Viruses and Attacks', *The Washington Post*, 14 February 2003, <www.washingtonpost.com/wp-dyn/articles/A50636-2002Jun26.html>.

56 Charles Arthur and Keith Stuart, 'PlayStation Network Uses Fear Identity Theft After Major Data Leak', *The Guardian*, 27 April 2011, <www.theguardian.com/technology/2011/apr/27/playstation-users-identity-theft-data-leak>.

Yoram Dinstein lists four different types of cross-border cyber operations depending on who carries them out: 1) attacks conducted by individual persons, 2) attacks conducted by terrorists unsupported by a state, 3) attacks conducted by terrorists overtly or covertly supported by a state and 4) attacks conducted by official organs of a state.[57] The first two categories are generally issues for the national law enforcement authorities, unless the state where the attacks originated from knowingly allowed its territory to be used for such acts. This would be contrary to the obligation not to allow such activity articulated by the International Court of Justice in the *Corfu Channel* case.[58] International law comes in regarding the latter two cases. Dinstein further divides the cyber acts of states to three categories: espionage, computer network attacks without human casualties or significant property damage and computer network attacks with human casualties or significant property damage.[59]

2.3 Examples of Cyber Attacks

2.3.1 Attacks Against Estonia in 2007

In 2007 the Estonian government decided to relocate a Soviet World War II memorial – the bronze soldier statue, considered by many to be a symbol of the Soviet occupation of Estonia – from the centre of Tallinn to a nearby military cemetery. The move sparked mass protests mostly among ethnic Russians in the country and was the backdrop for a widespread cyber attack on Estonian websites, including those of the Estonian government, the parliament, banks and newspapers.[60] Technically the attacks were fairly straightforward distributed denial-of-service[61] (DDoS) attacks but they were carried out in a coordinated and organized fashion simultaneously on several targets, on a previously unseen scale, and for an unusually long period of time. There has been speculation of the involvement of the Russian authorities but the Kremlin has consistently denied any participation and the

57 Yoram Dinstein, 'Computer Network Attacks and Self-Defense', 76 *U.S. Naval War College International Law Studies* (2002) 99–119 at 103–104.
58 *The Corfu Channel Case (UK v. Albania)*, Judgment, I. C. J. Reports 1949, p. 4 at 22.
59 Dinstein, *Computer Network Attacks and Self-Defense*, *supra* note 57 at 105.
60 Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents – Legal Considerations* (NATO Cooperative Cyber Defence Centre of Excellence: Tallinn, 2010) at 15.
61 A distributed denial-of-service attack consists of multiple computers flooding the target with malicious traffic in order to prevent it from serving legitimate clients. For a closer explanation, see *infra* at 17.

Estonian authorities stated after the incident that they had no evidence that the Russian government was behind the attacks.[62]

The attacks have been widely used in the media as an example of cyber warfare,[63] but calling them an instance of war is an exaggeration. The first wave of the attacks targeted a group of public websites which were inaccessible because of the traffic flood.[64] Being unable to access a newspaper website is more aptly described as a nuisance than an act of war. The attacks have also been described as cyber riots,[65] which seems more appropriate. The attacks did also target the servers running the domain name system[66] of internet service providers. This caused some disruption to the Internet traffic in parts of Estonia, but the attacks did not target critical infrastructure systems.[67] The attacks also targeted the e-banking services of the two largest banks in Estonia causing outages of 1,5–2 hours. The question of how the attacks appear in light of the Charter of the United Nations and the relevant rules of customary international law will be discussed in the following chapters.

2.3.2 Stuxnet

In June 2010 a Belarusian computer security company VirusBlokAda discovered a piece of malicious software later named Stuxnet. In the following months it became clear that Stuxnet was a highly sophisticated program which targeted only specific types of computers and seems to have spread mainly to certain countries, with an unusually high prevalence in Iran.[68] The consensus among security researchers is that the targets of the malware were Iranian nuclear facilities, first and foremost an uranium enrichment facility near the city of Natanz. The malware tampered with the enrichment process by causing the centrifuge rotors to speed up and slow down abnormally with the probable intention of

62 'Estonia Has No Evidence of Kremlin Involvement in Cyber Attacks', *Ria Novosti*, 6 September 2007, <en.ria.ru/world/20070906/76959190.html>.
63 See e.g. Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', *The Guardian*, 17 May 2007 <www.theguardian.com/world/2007/may/17/topstories3.russia>.
64 Clarke and Knake, *Cyber War*, *supra* note 20 at 13–15.
65 Tikk *et al.*, *International Cyber Incidents, supra* note 60 at 18.
66 The DNS (domain name system) servers are often described as a sort of a phonebook of the internet: they match the domain (e.g. google.com) with the numerical IP address of the server so that the client computer knows where to connect.
67 Tikk *et al.*, *International Cyber Incidents*, *supra* note 60 at 21.
68 According to the internet security company Symantec, almost 59% of the Stuxnet infections were found in Iran <www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>.

causing vibrations that would either destroy or severely damage the centrifuges. Stuxnet apparently succeeded in causing some delays and disruptions in the uranium enrichment process but failed to cause any catastrophic damage.[69] Then again, subsequent analysis has shown that this might have been the intention of the creators of Stuxnet, for the malware had certain built-in limitations and safeguards and could apparently have caused more damage without them.[70]

In November 2013 security researcher Ralph Langner published a report on Stuxnet and described how the attack described above was only the second phase of the operation and was in fact preceded by a stealthier version which aimed to cause damage to the centrifuges by increasing their pressure. Langner argues that instead of causing a simultaneous destruction of hundreds of centrifuges – which would apparently have been possible – the attacker opted for a more surreptitious approach and seems to have strived to increase stress on the centrifuge rotors in order to shorten their lifespan without causing suspicion of any foul play. In 2009, after such an approach, the previously described more well known and less stealthy attack was launched. Nevertheless, this time too the attacker seems to have preferred an approach of somewhat less damage over a longer period of time compared to a simultaneous destruction of more centrifuges. Without the less stealthy version, Langner argues that the malware might never have been discovered.[71]

In a technical sense Stuxnet was in many ways exceptional. It used four different so-called zero-day vulnerabilities[72] to gain access to the computers it infected. To put this into perspective, a threat using even one zero-day vulnerability is described by the computer security company Symantec as 'quite an event'. Using four of them is highly extraordinary and unique to Stuxnet.[73] The attack was a wake-up call in the sense that it underscored and

---

69 Kim Zetter, 'How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History', *Wired*, 7 November 2011, <www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/>. The article refers to the International Atomic Energy Agency and its estimates that between 1 000 and 2 000 centrifuges were replaced during few months at Natanz. The normal decommission rate would have been around 800 centrifuges per year.

70 Ralph Langner, *To Kill a Centrifuge – A Technical Analysis of What Stuxnet's Creators Tried to Achieve*, November 2013, <www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf> at 15.

71 Langner, *To Kill a Centrifuge*, *supra* note 70 at 10.

72 Zero-day vulnerabilities refer to previously unknown vulnerabilities, meaning the developers have had zero days to patch them.

73 Liam O Murchu, 'Stuxnet Using Three Additional Zero-Day Vulnerabilities', *Symantec Official Blog*, 14 September 2010, <www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities>.

brought to the limelight the fact that it was indeed quite possible for a cyber attack to cause physical damage. Whether or not this damage was sufficient to classify the attack as a use of force or an armed attack will be examined in the corresponding chapters below.

The origin of the malware has not been officially confirmed, although several reports claim that the United States and Israel were behind it. *The New York Times* reported in June 2012 that Stuxnet was a part of an operation codenamed Olympic Games which began during the George W. Bush administration and has since been continued by president Obama. Security analysts pointed fairly quickly after the attack that the malware was so sophisticated that its crafting had required considerable resources, basically only available to a nation-state.[74]

2.3.3 Red October

In October 2012 the Russian computer security company Kaspersky Lab discovered a piece of malware later dubbed Red October (or Rocra). While the aforementioned attacks had the goal of disrupting or destroying either communications, data or ultimately even physical objects, Red October was an intelligence gathering tool. The malware spread via targeted spearphishing attacks[75] and it was exceptional in the sense that it had been active for an unusually long period of time, at least five years. The main targets of the attack included governments, embassies and research institutions and victims of the malware are spread around the world.[76]

As the main function of Red October seems to have been intelligence gathering, a closer inspection of it is outside the scope of this study. It is mentioned as an example of the variety of the possible cyber attacks and also to present the issue of possible difficulty in determining the aim of the attack after a breach has been discovered. Red October was in a

74 Langner, *To Kill a Centrifuge*, *supra* note 70 at 20. See also news articles Josh Halliday, 'Stuxnet worm is the "work of a national government agency"', *The Guardian*, 24 September 2010, <www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency> and Kim Zetter, 'Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target', *Wired*, 23 September 2010, <www.wired.com/threatlevel/2010/09/stuxnet/>.

75 Spearphishing attacks are specifically targeted: an attack might for example be carried out by sending an e-mail to someone in the target organization with an infected attachment file. The e-mail may be masked as coming from someone familiar to the receiver and the content of the message may be customized to coax the receiver into opening the malicious attachment.

76 '"Red October" Diplomatic Cyber Attacks Investigation', *Kaspersky Lab SecureList*, 14 January 2013. <www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation>.

sense a passive tool, lurking in the background and gathering information and passing it on. Theoretically, the same vulnerabilities that it used to intrude the systems could have been used to launch a more active piece of malware with more destructive consequences, and depending on the targeted computers, perhaps even physical damages. This, combined with the fact that examining and reverse engineering the discovered breaches may be time-consuming, may pose challenges for pondering the appropriate and legal response to the attacks.

2.4 Technical Aspects of the Attacks

While many of the technical details of cyber operations are not relevant to the application of international law, it is necessary to outline some general aspects regarding the techniques of different attacks. The aforementioned cases of Estonia and Stuxnet highlight two vastly different technical concepts behind computer attacks. In terms of their technical sophistication, the former may perhaps be compared to storming a town with thousands of soldiers, or perhaps to firing thousands of artillery rounds in the general direction of the target. In other words, the attack is in a technical sense rather simple. The latter, on the other hand, compares to a special operations mission carried out by a team of highly trained individuals with detailed intelligence on the target. Thomas Rid sees cyber weapons as spanning a spectrum reaching from generic but low-potential tools – such as the ones used in the case of Estonia – to specific but high-potential ones – such as Stuxnet – and uses paintball guns as an example of the generic, low-potential kind: they are easily available, getting hit is highly visible but the effects are not especially permanent.[77]

The Estonian websites were hit with a distributed denial-of-service attack. The aim of a denial-of-service attack is to saturate the bandwidth and/or the computing capacity of the target so that legitimate traffic cannot get through. A single user with a handful of computers cannot do much damage by such attacks, which is why the more common variant is a *distributed* denial-of-service attack carried out through a so-called botnet. The botnet consists of hundreds or thousands of malware-infected computers whose resources and bandwidth the attacker controls remotely to attack the target, perhaps unbeknownst to the owner or user of the computer. The attacks may also be coordinated so that individual

77 Rid, *Cyber War Will Not Take Place*, *supra* note 53 at 36.

users knowingly take part in a denial-of-service attack. This requires very little technical skill or resources, and in fact ready made software is available which makes taking part in an attack as simple as entering a URL address (such as google.com) or an IP address of the target.[78] These kinds of attacks do not require nor do they crucially benefit from resources of a state. The attacks cause problems mainly during the active attack phase when the target site is inaccessible due to the malicious traffic. When the traffic wounds down the site normally starts responding again.

Malicious pieces of software or malware, such as Stuxnet, are programs that take advantage of a vulnerability – basically an error in the code – of another piece of software (such as Microsoft Word or Java) or an operating system (such as Windows). The vulnerability allows for an attacker to insert the malware into the targeted computer or a network. From here, the malware may propagate autonomously to another computers with the same vulnerability. The malware may find its way onto the computer for example via a malicious e-mail attachment or a website or an infected USB drive. The malware might allow for the attacker to use the computer as a part of a botnet, it might allow for access to the webcam of the computer, it might delete all the files on the computer or it might allow for the attacker to send customized commands to a uranium centrifuge at a nuclear facility, the possibilities are practically limitless. It should also be mentioned that once the vulnerability is made public, it loses its value as the software may be patched and the vulnerability fixed.[79] This means that the malware used in an attack is essentially a one-off weapon if it is detected. The more significant the intended and inflicted consequences are, the more visible the attack is and the more likely it is that the used vulnerabilities will become public.[80]

As discussed, Stuxnet was a highly customized and very sophisticated piece of software intended to infect only certain machines. In fact, if the malware found its way to

78 An example of such software is the Low Orbit Ion Cannon application which was used by the hacktivist network Anonymous in for example targeting organisations that cut off services from Wikileaks in 2010.

79 As vulnerabilities are practically essential for getting the malware onto a system, a lucrative market has developed for them. According to a *Forbes* article in March 2012, the price for a zero-day exploit for the Windows operating system varied between 60 000 and 120 000 U.S. dollars. Andy Greenberg, 'Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits', *Forbes*, 23 March 2012, <www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>.

80 Rid, *Cyber War Will Not Take Place*, *supra* note 53 at 168.

a computer that did not match certain properties, it shut itself down.[81] Attacks like it are able to cause significant direct physical damage: speeding up and slowing down centrifuges might severe them, opening up the floodgates of a dam might damage the dam or cause flooding. A more indirect form of physical damage is possible as well: tinkering with traffic lights or the air traffic control system might cause accidents.

Another technical issue worth noting especially related to figuring out the origin of the attack, or requiring states to block malicious traffic from their network infrastructure, is the structure of the internet and they way traffic is routed. If a user located in Finland wants to access a web page stored on a server in Great Britain, he or she normally has no way of controlling what route the packets delivering the data back and forth will take. The request for the page might first head on a submarine cable from Helsinki to Sweden, but depending on the network conditions, it might just as well head south to Estonia, or it might be routed through land-based cables via St. Petersburg. The data may easily pass through a dozen of servers along the way, and if one of the servers along the way would get disconnected, the data would automatically be rerouted through another connection. It is also possible for the user to deliberately reroute the traffic through different servers and encrypt it on the way in order to try to hide the origin of the traffic. This makes it difficult if not impossible to trace the traffic back to its true origin.[82]

Fully securing computers against cyber attacks is practically impossible. The sheer complexity of the software guarantees that the total prevention of exploitable vulnerabilities is not feasible in practice. And as the saying in the industry goes, the attacks never get worse, they only get better. This combination assures that the race between the development of the attacks and the protection from them will continue as heated as ever. Because of this, the notion of cyber resilience has found its way into the discussion: that is, in addition to securing the systems from attacks, states and private actors aim to prepare themselves to mitigate the consequences of possible attacks as far as possible.[83]

---

81 Zetter, *How Digital Detectives Deciphered Stuxnet*, *supra* note 69.

82 For examples of the difficulties in practice see e.g. Rid, *Cyber War Will Not Take Place*, *supra* note 53 at 144–145.

83 See e.g. Finland's Cyber Security Strategy, <www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy> at 4, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN[2013] 1 final), 7 February 2013, <ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667> at 5–7 and The United States International Strategy for Cyberspace, *supra* note 33 at 18–19.

3 Regulation of the Use of Force

3.1 General Notions About War and Its Regulation

War, according to the famous Clausewitzian expression, is the continuation of politics by other means.[84] And that is what war was for a lengthy period of human history: a regular form of state behaviour.[85] The rules concerning war were few and far between and – in the Western culture – discussed by Christian theologians such as St. Augustine in the turn of the 5th century and Thomas Aquinas in the 13th century. They were influential thinkers contributing to the *bellum justum* doctrine which set out the conditions for a just war.[86] The original traces of the distinction between *bellum justum* and *bellum injustum* lead further back to the Roman Kingdom.[87] According to Aquinas, for a war to be just, it had to fulfil three criteria: it had to be conducted under the authority of a sovereign (that is, not privately), there had to be a just cause for the war, and those waging war had to have the right intention to advance good and to avoid evil.[88]

In the 16th century the Spanish colonization of the Indies and a debate about the justification of the actions of the conquistadors provided a spark for the emergence of modern international law at the University of Salamanca.[89] In the following decades *De Jure Belli* (1598) by Alberico Gentili and *De Jure Belli ac Pacis* (1623) by Hugo Grotius were published, both of which discussed the laws of war extensively and drew a distinction between theology and international law.[90] The Peace of Westphalia in 1648 marked the beginning of the era of the modern, independent nation-states and the end of the religious wars between Catholic and Protestant countries.[91] The 15th and 16th centuries were also a

84 Carl von Clausewitz, *Vom Kriege* (Rowohlt, Hamburg, 1963) at 22.
85 Kari Hakapää, *Uusi kansainvälinen oikeus* (Talentum, Helsinki, 2003) at 411.
86 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 66.
87 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 65.
88 Thomas Aquinas, *Summa Theologica, Secunda Secundae*, Q 40 (Benziger Brothers: New York, 1947).
89 Malcolm Shaw, *International Law* (5th Edition, Cambridge University Press, 2003) at 22–23 and Martti Koskenniemi, 'Colonization of the "Indies": The Origin of International Law?' in Yalanda Gamarra (ed.), *La idea de la América en el pensamiento ius internacionalista del siglo XXI* (Institución Fernando el Católico: Zaragoza, 2010), 43–63 at 43–44
90 Shaw, *International Law*, *supra* note 89 at 23.
91 Peter Malanczuk – Michael Akehurst, *Akehurst's Modern Introduction to International Law* (7th Revised Edition, Routledge, London, 1997) at 11.

period of military revolution and of a comprehensive change of the whole paradigm of war brought on by the proliferation of firearms and ever growing armies.[92]

The just war reasoning became quite extended and both sides of conflicts were able to resort to it in justifying their actions. From the 18th century onwards the distinction between legal and illegal wars faded and the justification of war revolved around the interests of the state, which were defined by each state themselves.[93] During the 19th century it was the sovereign that rose to the centre and claimed a monopoly on exercising military power. The legal analysis shifted as well, and it was the sovereign act that became the starting point of the assessment.[94]

After the suffering of the First World War, the Covenant of the League of Nations[95] (signed in 1919) set certain limitations on war, although did not ban it altogether. In 1928 the Kellogg–Briand Pact[96] (officially The General Treaty for the Renunciation of War) was concluded to provide for a more comprehensive prohibition of war. As widely as it was ratified, it failed to prevent for example the Italian invasion of Ethiopia in 1935 and the Japanese invasion of Manchuria in 1931 and, of course, ultimately, the Second World War. It was not a meaningless treaty, however, and as Ian Brownlie writes, its obligations were disregarded by some but repudiated by none. And indeed, the Pact also had a role in the post-war military tribunals.[97]

3.2 United Nations as the Keeper of International Peace

After the Second World War and the failures of the Kellogg–Briand Pact and the League of Nations, 51 states in 1945 formed the United Nations (UN), an organization whose purposes according to Article 1 of the UN Charter include the maintenance of international peace and security and the development of friendly relations among nations. As the threats to international peace and security have turned more to intra-state conflicts which the Charter does not explicitly deal with, the Charter system has evolved through interpretation

92 Joonas Sipilä, 'Puuneista Bastioneihin – Sota ja historialliset esimerkit' in Jyri Raitasalo and Joonas Sipilä (eds), *Muuttuva sota* (National Defence University: Helsinki, 2005), 25–55 at 40–41.
93 Malanczuk – Akehurst, *Akehurst's Modern Introduction to International* Law, *supra* note 91 at 306–307.
94 Kennedy, *Of War and Law*, *supra* note 51 at 61–62.
95 The Covenant of the League of Nations, 28 June 1919, in force 10 January 1920.
96 The General Treaty for the Renunciation of War, 27 August 1928. LNTS vol. XCIV, No. 2137, 33.
97 Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press: Oxford, 1963) at 80.

and the development of new rules and concepts such as peacekeeping, which has become an important part of the operation of the United Nations. This process has by no means been easy nor has there always been a clear consensus on how to apply the existing rules in new situations.

The maintenance of international peace and security builds around Article 2(4) of the Charter. It is arguably the most important paragraph of the Charter,[98] and it bans member states from using or threatening to use force against any another state. There are two exceptions to the prohibition: the use of force authorized by the Security Council and self-defence under Article 51 of the Charter. In addition to the United Nations Charter, an important source of rules regarding the use of force is customary international law. Some of the customary international law rules correspond to those of the UN Charter, but the relationship between the two is not always clear. Articles 2(4) and 51 and the corresponding rules of customary international law will be more closely examined later on. Article 33 along with the rest of Chapter VI of the Charter aims to ensure that states will settle their disputes peacefully. The Article obliges parties of any dispute whose continuance is likely to endanger the maintenance of international peace and security to first of all seek a solution by negotiation, mediation or other peaceful means.

The rules of customary international law and the UN Charter apply to states and may only apply to non-state actors if their actions are attributable to states. The International Law Commission (ILC) prepared the Draft Articles on Responsibility of States for Internationally Wrongful Acts[99] (hereafter referred to as Draft Articles on State Responsibility) whose Chapter II includes rules on the attribution of conduct to a state. In a subsequent resolution, the General Assembly commended the Draft Articles to the 'attention of governments without prejudice to the question of their future adoption or other appropriate action'.[100] The question of attribution will be touched upon later, and while a detailed examination of the issue is outside the scope of this study, suffice it to note at

98 It has for example been called 'the heart of the UN Charter', see Louis Henkin, 'The Reports of the Death of Article 2(4) Are Greatly Exaggerated', 65 *The American Journal of International Law* (1971) 544–548 at 544.

99 Report of the International Law Commission on the Work of Its Fifty-third Session, UN Doc. A/56/10 (2001).

100 Responsibility of States for Internationally Wrongful Acts, UN Doc. A/RES/56/83, 12 December 2001.

this point that if certain conditions are met, it is entirely possible for the acts of non-state actors to be attributed to a state in the context of cyber operations as well.

3.3 Interpretation of the Rules of International Law

The United Nations Charter is a central document regarding the rules of *jus ad bellum*. The articles of the Charter are, as we shall see on the following pages, not unambiguous and can, as nearly every treaty text, be interpreted in different ways. The Vienna Convention on the Law of Treaties[101] (VCLT), signed in 1969, offers rules and guidance as to the interpretation of treaties. Article 4 of the VCLT states that the Convention only applies to treaties concluded after the entry into force of the Convention, which happened in January 1980. However, this does not prevent applying the rules of the VCLT to the UN Charter, as the rules of the Convention also correspond to customary international law.[102]

There are three basic approaches to the interpretation of international treaties: one focuses on the text of the treaty, second on the intention of the adopting parties and the third more widely on the object and purpose of the treaty.[103] The International Court of Justice has emphasized that the interpretation must primarily be based upon the text of the treaty.[104] Articles 31–33 of the Vienna Convention include features of the three approaches. According to Article 31 and its general rule of treaty interpretation, the treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms in their context and in light of the object and purpose of the treaty. In addition, according to paragraph 3 of the Article, any subsequent agreement between the parties regarding the interpretation of the treaty and any subsequent practice in the application of the treaty establishing the agreement of the parties regarding the interpretation shall be taken into account. In addition to guiding the interpretation, the subsequent practice may also signify a change in the legal relationship between the parties to the treaty.[105]

101 Vienna Convention on the Law of Treaties, 23 May 1969, in force 27 January 1980. 1155 UNTS 331.
102 *Territorial Dispute (Libyan Arab Jamahiriya/Chad),* Judgment, I. C. J. Reports 1994, p. 6 at para 41. Also, Georg Ress, 'Interpretation' in Bruno Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2nd Edition, Oxford University Press, 2002), 13–32 at 18.
103 Shaw, *International Law*, *supra* note 89 at 839.
104 *Territorial Dispute (Libyan Arab Jamahiriya/Chad), supra* note 102 at para. 41.
105 Shaw, *International Law*, *supra* note 89 at 841.

Article 32 of the VCLT deals with the supplementary means of interpretation. According to it, supplementary means such as the preparatory work of the treaty – *travaux préparatoires* – can be referred to confirm an ambiguous meaning. Subparagraph b also states that the supplementary means may be used in interpretation if the result otherwise comes up manifestly absurd or unreasonable. While useful in some cases, there are also, to quote Stefan Kadelbach, good reasons to handle the drafting materials with reluctance.[106] In other words, the *travaux préparatoires* may indeed be useful in guiding the interpretation in some cases, but due consideration must also be given to the development that has taken place since the San Francisco Conference.

According to a strict view of the Vienna Convention, the reference to the subsequent practice in Article 31(3)(b) applies to the conduct of states and not to organs of an organization. Nevertheless, the International Court of Justice has used the practice of organs as guidance for interpretation. And indeed, the practice of for example the UN Security Council may, especially in cases of unanimity, be tied back to the member states. It is true that blindly accepting the practice of organs without due regard for the procedure behind them may in worst cases lead to the so-called tyranny of the majority, but this may be avoided by a case-by-case analysis and the acceptance of consistent and widely accepted practice.[107] And in practice soft law instruments are being used for authoritative interpretation of treaties, also in the context of the use of force.[108] Another question is whether for example the practice of the Security Council is of such uniformity that it would in this sense count or be useful.

106 Stefan Kadelbach, 'Interpretation of the Charter' in Bruno Simma, Daniel-Erasmus Khan, Georg Nolte and Andreas Paulus (eds), *The Charter of the United Nations – A Commentary, Volume I* (3rd Edition, Oxford University Press, 2012), 71–100 at 88–89.

107 Kadelbach, *Interpretation of the Charter*, *supra* note 106 at 86–87.

108 Alan Boyle, 'Soft Law in International Law-Making' in Malcolm D. Evans (ed.), *International Law* (3rd Edition, Oxford University Press, 2010), 122–140 at 127–128.

4 Prohibition of the Use of Force in the Context of Cyber Operations

4.1 Article 2(4) of the United Nations Charter

Article 2(4) of the United Nations Charter states that

> *All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*

The article does not merely set a prohibition on war, but forbids the 'use of force' and thus covers a wider set of situations.[109] The Article also refers to the use of force against the territorial integrity or political independence of a state, but these should not, according to the more common view, be read as a restriction on the scope of the ban.[110] In fact, the smaller states who were behind the insertion meant for it to strengthen, not weaken the prohibition.[111] And indeed, the last part of the sentence includes a catch-all prohibition on the use or threat of force in any other manner inconsistent with the purposes of the United Nations.

The notion of 'force' is not defined in the Charter, yet it is crucial to the content of the Article. It is no surprise, then, that there are some varying views on which kind of acts Article 2(4) covers. The Charter includes a range of terms whose usage is not entirely unambiguous. As mentioned, Article 2(4) bans the use of 'force' whereas the Preamble of the Charter speaks about 'armed force' and Article 51 guarantees the right to self-defence in cases of an 'armed attack'. The definition and content of the terms force and armed attack shall be examined more closely below. It should also be noted that while Article 2(4) is a central rule also in the context of cyber operations, it is not the only one. Actions that do not constitute force may still for example violate the principle of non-intervention or other

109 Shaw, *International Law*, *supra* note 89 at 686.
110 Albrecht Randelzhofer, 'Article 2(4)' in Bruno Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2nd Edition, Oxford University Press, 2002), 112–136 at 123–124.
111 Hilaire McCoubrey and Nigel D. White, *International Law and Armed Conflict* (Dartmouth Publishing Company: Aldershot, 1992) at 25.

facets of international law. These too will be more closely examined on the following pages.

4.2 Customary International Law

4.2.1 Prohibition on the Use of Force in Customary International Law

Article 38(1) of the Statute of the International Court of Justice is generally recognized as an enumeration of the sources of international law.[112] In addition to international treaties, it also recognizes international custom as a source, and indeed it is an elementary part of international law. For a norm to be part of customary international law there are two conditions that have to be met: there has to be settled state practice and a belief of the existence of an obligation (*opinio juris*).[113] That is, states acting in a certain way in and of itself is not enough, but the states must believe that there exists a rule that behoves them to do so.

The prohibition on the use of force is considered to be part of customary international law, as evidenced by the statements of the International Court of Justice in the *Nicaragua* case and the International Law Commission.[114] The Court noted that sufficient *opinio juris* can be found for example from the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations[115] (hereafter referred to as the Friendly Relations Declaration), which includes the principle of non-use of force. The Court argued that consenting to the text does not merely reiterate the treaty commitment in the Charter but marks the acceptance of the validity of the set of rules declared in the resolution. Thus, as the resolution was adopted without a vote, the member states can be seen as expressing *opinio juris*.[116]

---

112 Hugh Thirlway, 'The Sources of International Law' in Malcolm D. Evans (ed.), *International Law* (3rd Edition, Oxford University Press, 2010), 95–121 at 98.

113 *North Sea Continental Shelf Cases (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands)*, Judgment, I. C. J. Reports 1969 at para. 77.

114 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment, I. C. J. Reports 1986 at paras 188–190 and Report of the International Law Commission on the Work of Its Eighteenth Session, UN Doc. A/6309/Rev.1 (1966) at 247.

115 Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, GA Res. 2625 (XXV), 24 October 1970.

116 *Nicaragua*, *supra* note 114 at para 188.

While the Court considered the existence of *opinio juris* in *Nicaragua*, it did not discuss the prevalence of force in state behaviour. War has not been eradicated from the world, nor will it be in the foreseeable future. Does this then mean that the first prerequisite – settled state practice – of a customary law norm is missing? It bears worth noting that states have generally attempted to justify their actions in terms of self-defence instead of claiming that Article 2(4) or a customary law norm with the same content would be invalid.[117] Indeed, these claims and justifications could also be seen as evidence of the expression of *opinio juris* by states and thus reinforcing the status of the customary law norm of non-use of force. And as the ICJ stated in *Nicaragua*, for a rule to be established as customary, the practice must not be absolutely conforming but generally consistent with the rule. The Court also noted that if a state that acts contrary to the rule indeed does appeal to the exceptions to the rule, the significance of the attitude confirms rather than weakens the rule, even if the conduct of the state is not in reality justifiable on such basis.[118]

Another question is the content of the customary international law rule versus the content of Article 2(4). In *Nicaragua*, the United States argued that the rule of customary international rule and Article 2(4) were uniform, but the Court dismissed this proposition.[119] The Court stated that even if customary international law and the Charter did overlap, they still would maintain their separate identities.[120] Yoram Dinstein argues that the present form of the rule of customary international law is 'essentially a replica' of Article 2(4), but reminds that it is improbable that the correlation will not develop over the years.[121]

The customary law prohibition is, to simplify the issue, potentially more broad in its scope but evolves more rigidly through state practice and *opinio juris*. And the prohibition of Article 2(4) can perhaps be more nimbly interpreted, yet the text of the treaty and the rules of its interpretation set certain limits. It is thus possible for a rule of customary international law to emerge regarding specifically cyber operations and the use of force, but at this point there is not sufficient evidence of such a norm.[122] The same can be said

117 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 97.
118 *Nicaragua*, *supra* note 114 at para. 186.
119 *Nicaragua*, *supra* note 114 at para. 175.
120 *Nicaragua*, *supra* note 114 at para. 177.
121 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 100.
122 Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', 37 *Columbia Journal of Transnational Law* (1999) 885–937 at 921–922.

with regard to other issues as well, as the question of the evolvement of *jus ad bellum* is of course not limited to cyber operations. It has been also claimed that the whole framework is and has been challenged by developments such as the rise of global terrorism and the diminishing effect of globalization on the sovereignty of states.[123]

4.2.2 Prohibition of the Use of Force as a Peremptory Norm

It is clear that the ban on the use of force is part and parcel of customary international law, but is it also part of *jus cogens*, a set of unconditional peremptory norms from which no exceptions are allowed? This is the view of most scholars, and the International Law Commission has referred to the prohibition of the use of force as a 'conspicuous example' of a rule that has 'the character of *jus cogens*'.[124] The International Court of Justice referred to the view of the ILC in *Nicaragua*[125] without explicitly taking the same position, except for the Separate Opinions of Judges Singh[126] and Sette-Camara[127]. Article 53 of the Vienna Convention on the Law of Treaties defines a peremptory norm as 'a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character'. This has been generally accepted as the definition for a peremptory norm.[128] Common examples of peremptory norms include the prohibition of genocide[129] and the prohibition of torture,[130] but the prohibition of the use of force has also been widely used as an obvious example of such a norm.[131] While a closer examination of the question is outside the scope of this study, it is worth acknowledging some of the critique and possible problems regarding outright classifying the wider ban on the use of force as *jus cogens*.

---

123 Sean D. Murphy, 'Protean *Jus Ad Bellum*', 27 *Berkeley Journal of International Law* (2009) 22–52 at 23.
124 Report of the ILC, Eighteenth Session, *supra* note 422 at 247. ILC also referred to such a view in the Report of the ILC, Fifty-third Session, *supra* note 99 at 283.
125 *Nicaragua*, *supra* note 114 at para. 190.
126 *Nicaragua*, *supra* note 114, Separate Opinion of Judge Singh at 153.
127 *Nicaragua*, *supra* note 114, Separate Opinion of Judge Sette-Camara at 199. He argues that in addition to the prohibition of force also the prohibition of intervention qualifies as a norm of *jus cogens*.
128 Lauri Hannikainen, *Peremptory Norms (Jus Cogens) in International Law – Historical Development, Criteria, Present Status* (Finnish Lawyers' Publishing Company: Helsinki, 1988) at 3.
129 *Armed Activities on the Territory of the Congo (New Application: 2002) (Democratic Republic of the Congo v. Rwanda)*, Jurisdiction and Admissibility, Judgment, I. C. J. Reports 2006, p. 6 at para. 64.
130 *Prosecutor v. Furundzija*, Case no. IT-95-17/1-T, Trial Chamber, Judgment (10 December 1998) at para. 153.
131 For an overview of such views, see e.g. Carin Kahgan, 'Jus Cogens and the Inherent Right to Self-Defense', 3 *ILSA Journal of International & Comparative Law* (1997), 767–827 at 777–781.

By definition, peremptory norms allow for no derogation, yet the prohibition of the use of force as laid out in the Charter of the United Nations includes two uncontested exceptions: the use of force in self-defence, which is also acknowledged to be part of customary international law, and the use of force with the authorization of the Security Council. One common approach is to view the *jus cogens* prohibition as a wider norm encompassing the right to self-defence.[132] This, however, leads to other problems, such as ambiguity as to the content of the right to self-defence.[133] One of the virtues of the other *jus cogens* norms is their clarity: torture is prohibited without exceptions, as is genocide (their definitions can of course be debated). This is not the case with the ban on the use of force, which includes somewhat ambiguous exceptions which are in constant evolution, as demonstrated by for example the emergence of the concept of responsibility to protect (R2P) and the discussion of pre-emptive self-defence. As James A. Green notes, the reality of the development of *jus ad bellum* does not fit well into the static and stable nature presumed from a *jus cogens* norm.[134]

A better alternative is to define the *jus cogens* norm more precisely as a ban of aggression or aggressive force. This is the approach referred to by the International Law Commission in the commentary on the Draft Articles on State Responsibility.[135] Such an approach has also been adopted by several scholars, including Lauri Hannikainen in his study on peremptory norms.[136] The Definition of Aggression resolution adopted by the United Nations General Assembly in 1974 defines aggression as 'the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations'.[137]

---

132 For an example of such a formulation, see Ulf Linderfalk, 'The Effect of *Jus Cogens* Norms: Whoever Opened Pandora's Box, Did You Ever Think About the Consequences?', 18 *The European Journal of International Law* (2008), 853–871 at 860.

133 James A. Green, 'Questioning the Peremptory Status of the Prohibition of the Use of Force', 32 *Michigan Journal of International Law* (2011) 215–257 at 232–236.

134 Green, 'Questioning the Peremptory Status of the Prohibition of the Use of Force', *supra* note 133 at 241.

135 Report of the ILC, Fifty-third Session, *supra* note 99 at 283.

136 Hannikainen, *Peremptory Norms (Jus Cogens) in International Law*, supra note 128 at 356.

137 *Definition of Aggression*, GA Res. 3314 (XXIX), 14 December 1974.

4.3 Notion of 'Force'

Article 2(4) of the UN Charter bans the threat or the use of 'force', but there is no explicit definition of what constitutes force. The International Court of Justice has examined the notion in the *Nicaragua* case, and based on the case the possible illegal acts can be divided into three categories, of which Article 2(4) covers the first two: armed attacks, uses of force and interventions.[138] While the Court did not explicitly define these, the judgment offers some indication as to what each category comprises. Firstly, the Court drew a distinction between the 'most grave forms of the use of force', that is armed attacks referred to in Article 51 of the Charter, and 'other less grave forms'.[139] This distinction represents the prevailing view, but it has been disputed as well.[140] The relationship between Article 2(4) and Article 51 will be further discussed below in chapter 5.2.2 in junction with the notion of an 'armed attack'. Secondly, the Court drew a distinction between acts breaching the principle of non-intervention and those constituting a use of force: 'acts constituting a breach of the customary principle of non-intervention will also, if they directly or indirectly involve the use of force, constitute a breach of the principle of non-use of force in international relations'.[141] The Court also referred to an operation 'classified as an armed attack rather than as a mere frontier incident'[142] and to the Friendly Relations Declaration, which posits 'a duty to refrain from acts of reprisal involving the use of force'. The principle of non-intervention will be summarily discussed in chapter 6.1 below.

While the term 'force' is not preceded by 'armed', it is widely acknowledged that 'force' refers particularly to armed force and thus excludes for example economic force.[143] Some authors have taken a contrary position and argued that the prohibition is wider and does indeed include other forms of force as well: for example Hans Kelsen argues that the notion of force is meant to include any illegal action of a state that violates the interests of another, not just armed force.[144] Even though especially from the viewpoint of poor states

138 McCoubrey and White, *International Law and Armed Conflict*, *supra* note 111 at 62.
139 *Nicaragua*, *supra* note 114 at para. 191.
140 Albrecht Randelzhofer, 'Article 51' in Bruno Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2nd Edition, Oxford University Press, 2002), 788–806 at 790–791.
141 *Nicaragua*, *supra* note 114 at para. 209.
142 *Nicaragua*, *supra* note 114 at para. 195.
143 Randelzhofer, *Article 2(4)*, *supra* note 110 at 117–118; also Alfred Verdross and Bruno Simma, *Universelles Völkerrecht – Theorie und Praxis* (3rd Edition, Duncker & Humblot: Berlin, 1984) at 293.
144 Hans Kelsen, *Collective Security Under International Law* (U.S. Naval War College: Newport, 1954) at 55, 57. For an overview of such commentary, see Belatchew Asrat, *Prohibition of Force Under the UN*

there might be compelling reasons to treat harsh economic pressure as force, there seems to be little support available for such an interpretation but instead much stronger arguments supporting the opposite view.[145] Among these is the rejection of a proposal introduced by Brazil at the San Francisco Conference in 1945 to broaden the ban to include economic coercion. The issue was also raised during the committee work leading to the Friendly Relations Declaration, but the view of limiting the notion of force to military force prevailed and the Declaration refers to measures of economic coercion in the context of the principle of non-intervention instead of the principle of non-use of force.[146] The same kind of a conclusion was reached with the Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations,[147] also known as the Declaration on the Non-Use of Force: it differentiates between armed interventions (paragraph I, subparagraph 7) and economic or other coercion (paragraph I, subparagraph 8). It thus seems clear that economic coercion is not covered by Article 2(4), yet it may still be contrary to international law based on the principle of non-intervention.[148] The question of economic force will be addressed in more detail and in the context of cyber attacks in chapter 4.5.

Article 2(4) bans the use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations. The prevailing view is that the language is not intended to restrict the scope of the prohibition and that it basically covers all uses of force – especially with the catch-all provision in the end[149] – except the ones authorized by the Charter.[150] The United Kingdom argued during the oral proceedings of the *Corfu Channel* case that the minesweeping carried out by the Royal Navy in the territorial waters of Albania did not breach Article 2(4) because it was not directed at the territorial integrity or political independence of

Charter – A Study of Art. 2(4) (Iustus Förlag: Uppsala, 1991) at 115–117.

145 For an overview of the argument see e.g. Randelzhofer, *Article 2(4)*, *supra* note 110 at 118.

146 Asrat, *Prohibition of Force Under the UN Charter*, *supra* note 144 at 113–114.

147 Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, GA Res. 42/22, 18 November 1987.

148 Derek W. Bowett, 'Economic Coercion and Reprisals by States', 13 *The Virginia Journal of International Law* (1972) 1–12 at 1–2.

149 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 82.

150 Schmitt, *Computer Network Attack and the Use of Force in International Law*, *supra* note 122 at 901.

Albania.[151] The ICJ did not accept this line of reasoning and regarded the claimed right to intervene as a 'policy of force'.[152]

Also according to the prevailing view not every act of physical force will be in breach of the Article as it seeks specifically to ban military force. A popular example of a forceful non-military act is the opening of the floodgates of a dam, causing severe flooding downstream. A curious exception to the prevailing view is, however, the use of non-military force whose effects rise to the level of an armed attack. In such a case a victim state would be able to act in self-defence based on Article 51. This, however, according to Albrecht Randelzhofer, would be acceptable only in extreme cases.[153] And as with economic force, even though the acts would not be illegal under Article 2(4), they very well might be unlawful based on another norm of international law.[154]

For an act to be considered a use of force, it does not necessarily have to be direct, such as an attack carried out by the military forces of a state. The International Court of Justice examined the question in *Nicaragua*: in the case, the United States argued that it was acting in collective self-defence following acts of aggression by Nicaragua towards Costa Rica, El Salvador and Honduras.[155] The United States claimed that the Nicaraguan government had supported armed groups that took military and paramilitary actions against primarily El Salvador, but on a smaller scale against Costa Rica, Honduras and Guatemala as well, and that the Nicaraguan military had engaged in attacks on Honduran and Costa Rican territory.[156] The ICJ declared that the arming and training of the Nicaraguan contras by the United States did involve the threat or use of force. For this kind of assistance to constitute a use of force, it has to cross a certain threshold. As the ICJ noted, while the arming and training of the contras did include use of force, mere supply of funds did not.[157]

The issue of new types of weapons, namely those that do not involve any explosive effect, such as bacteriological, biological and chemical weapons, was addressed by Ian Brownlie

151 *The Corfu Channel Case (UK v. Albania),* I. C. J. Pleadings (1950), Volume III. Oral Proceedings, Statement by Sir Eric Beckett (U.K.), Sitting of 12 November 1948 at 296.
152 *Corfu Channel, supra* note 58 at 35.
153 Randelzhofer, *Article 2(4)*, *supra* note 110 at 118–119.
154 J. N. Singh, *Use of Force Under International Law* (Harnam Publications: New Delhi, 1984) at 213.
155 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* I. C. J. Pleadings, Volume II, Counter-Memorial of the United States of America at para. 202.
156 *Nicaragua*, *supra* note 114 at para. 128.
157 *Nicaragua*, *supra* note 114 at para. 228.

in 1963. He argued that the use of such non-conventional weapons constitutes use of force as well, on the basis of two arguments. First, the agents in question were commonly referred to as weapons and secondly – and more importantly – they are used for the destruction of life and property.[158] The approach follows from a teleological reading of the UN Charter and the corresponding customary international law rule. According to the Preamble of the Charter, the aim of the United Nations is to save succeeding generations from the scourge of war. It is thus reasonable to come to the conclusion that the myriad ways of inflicting death and damage not imaginable during the drafting of the Charter should be included in the notion of force of Article 2(4), the very article that in effect carries out the promise of the Preamble.

4.4 Cyber Operations as Force

4.4.1 Overview of Cyber Operations

The International Court of Justice affirmed in the *Nuclear Weapons* Advisory Opinion that Articles 2(4), 42 and 51 of the UN Charter apply to any use of force, regardless of the weapons employed.[159] It is thus clear that it is entirely possible for a cyber operation to qualify as a use of force. Such a view is also supported by the Vienna Convention on the Law of Treaties, whose Article 31(3)(b) states that any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation shall be taken into account. In their statements several countries have considered certain cyber attacks to be a type of force.[160] This approach has been widely acknowledged and the contrary claims have mostly been limited to operations with non-physical consequences which indeed do not qualify as force.[161] Because cyber operations are a group of very divergent actions, sweeping claims that would bring all such acts under the notion of force are excessive and not justifiable and thus rare. Determining exact and absolute rules for which kinds of cyber operations do constitute force is impossible. The following pages aim to draw some conclusions as to what kind of actions might cross the threshold.

158 Brownlie, *International Law and the Use of Force by States*, *supra* note 97 at 362.
159 *Nuclear Weapons*, *supra* note 29 at para 39. For an example of such a view in earlier literature see e.g. Singh, *Use of Force Under International Law*, *supra* note 154 at 213.
160 For an overview of such statements, see Roscini, *World Wide Warfare*, *supra* note 17 at 108–109.
161 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 46–47.

It has also been argued that the interpretative methods of the VCLT do not allow for the inclusion of cyber force to the ambit of Article 2(4).[162] Such claims are not convincing, for they view cyber force as not a type of armed force but a new type of force of its own. As mentioned, sweeping claims of either inclusion or exclusion regarding the notion of force are too broad. While it is true that for example the aforementioned possible severe economic consequences of a cyber operation may pose challenges for the exclusion of economic force from the prohibition of Article 2(4), certain types of cyber operations do without a doubt fit into the notion of armed force.

It is worth emphasizing the distinction of *lex lata*, the law as it currently exists and *lex ferenda*, the possible law in the future. It is entirely reasonable to claim *de lege ferenda* that for example an attack with only economic consequences could in the future be viewed by states as a use of force and thus the interpretation of Article 2(4) or the customary international law rule prohibiting the use of force could be expanded to include such attacks. It is a completely different statement to claim such an interpretation to be representative of *lex lata*. It has also been suggested that the distinction might not always be appropriate when discussing cyber operations on the basis that a *de lege ferenda* argument can only be presented if it differs from the existing law. The discussions regarding cyber operations mostly are, however, about applying the current law in cyberspace.[163]

4.4.2 Some Unique Characteristics of Cyber Operations

The International Court of Justice noted in the *Nuclear Weapons* Advisory Opinion that taking into account the unique characteristics of nuclear weapons was imperative in applying the Charter law to the case at hand.[164] Accordingly, the unique characteristics of cyber operations must be taken into account when applying the *jus ad bellum* to them. There are several ways of describing and categorizing these characteristics, and Heather Harrison Dinniss provides one example. She identifies four characteristics of cyber operations that distinguish them from conventional attacks in terms of the framework of

162 Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification?' in 1 *Goettingen Journal of International Law* (2009) 375–396 at 392.

163 Ziolkowski, *Ius ad bellum in Cyberspace – Some Thoughts on the 'Schmitt-Criteria' for Use of Force*, *supra* note 12 at 309.

164 *Nuclear Weapons*, *supra* note 29 at para. 36.

the use of force: indirectness, intangibility, locus and result.[165] Some of the issues have already been touched upon and some will be discussed in further detail later. What follows is a summary of the issues based on the four distinguishing characteristics before turning to the question of when cyber operations qualify as uses of force.

Indirectness is indeed one potentially distinguishing factor: several types of cyber operations require further action by a second actor after the initial act. Examples of such include an attack on the targeting system of a missile, or disabling air traffic control systems.[166] Direct cyber attacks are possible as well. One example is the breach of a control system of a dam and the opening of floodgates. The ICJ stated in *Nicaragua* that also indirect acts, such as support of a certain type for terrorist activities, may constitute uses of force.[167] Thus, the possible indirectness of a cyber attack seems not to be a prohibitive factor in applying the current law if there is a sufficient causal nexus between the attack and the destructive effect.

The intangibility factor refers to the fact that neither the target of the attack nor the weapon used might not exist in a physical level. The damage might be intangible as well, as in the case of an attack on a stock exchange.[168] Even attacks that ultimately result in physical consequences target the information resident in computers. For example the Stuxnet attack modified the spinning frequencies of the centrifuges, which directly resulted in physical damage to them.[169] More difficult are the cases where the target is the destruction or altering of the information itself. Such attacks, too, might lead to physical consequences, but with a less direct nexus.[170]

The locus factor takes into consideration the fact that in some cases it may be difficult to ascertain the origin of the attack.[171] The attack may be routed through several points in different countries in order to hide the true source, or the malicious traffic may come from

---

165 Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012) at 65.
166 Dinniss, *Cyber Warfare and the Laws of War*, *supra* note 165 at 65–66.
167 *Nicaragua*, *supra* note 114 at paras 195, 205, 228.
168 Dinniss, *Cyber Warfare and the Laws of War, supra* note 165 at 67.
169 Erik Chien, 'Stuxnet: A Breakthrough', *Symantec Blog*, 12 November 2010, <www.symantec.com/connect/blogs/stuxnet-breakthrough>.
170 Dinniss, *Cyber Warfare and the Laws of War, supra* note 165 at 67–68.
171 Michael N. Schmitt, 'Cyber Operations and the *Jus Ad Bellum* Revisited', 56 *Villanova Law Review* (2011) 569–605 at 594.

several countries. During the attacks on Estonia in 2007 the traffic originated from 178 countries.[172] It should be noted, though, that the attacks were distributed denial-of-service attacks which by definition originate from countless sources. Nevertheless, the incident provides an example of how difficult it may be to trace the attack back to the real origin, at least in a timely manner.

As has already been discussed, the results of cyber operations cover a wide range of consequences spanning from mere inconvenience to physical destruction. The indeterminacy and variety of the results spanning from inconvenience to physical destruction is arguably the most challenging factor in categorizing in applying the rules on the use of force to cyber attacks.[173] The results might in some cases also be more unpredictable than in the case of kinetic force. A common example of such a case is a cyber attack on a stock exchange or a bank.[174]

4.4.3 Cyber Operations as Uses of Force

The proposals for solving the question of cyber operations and the threshold of force may be divided to three main approaches: effects-based, target-based, and instrument-based. The instrument-based approach uses the weapon used as the determining factor: a cyber operation may qualify as force if the weapon used sufficiently resembles the conventionally used ones. The target-based approach treats any operation targeting critical infrastructure as an armed attack (and thus, also, as force). The effects-based approach uses the overall effects of the operation as the determining factor.[175] None of these approaches is without issues,[176] but the most prevalent of the approaches seems to be the effects-based one, also adopted by the Tallinn Manual.[177] The Manual refers to the 'scale and effects' assessment used by the International Court of Justice in *Nicaragua*. The ICJ stated that the

172 Tikk *et al.*, *International Cyber Incidents*, *supra* note 60 at 23.
173 Schmitt, *Computer Network Attack and the Use of Force in International Law*, *supra* note 122 at 912. Heather Harrison Dinniss takes a similar view. Dinniss, *Cyber Warfare and the Laws of War, supra* note 165 at 72–73.
174 See *infra* at 43.
175 Hollis, *Why States Need an International Law for Information Operations*, *supra* note 38 at 1041.
176 Reese Nguyen, 'Navigating Jus Ad Bellum in the Age of Cyber Warfare', 101 *California Law Review* (2013) 1079–1131 at 1117–1124.
177 See e.g. Silver, *Computer Network Attack as a Use of Force under Article 2(4)*, *supra* note 36 at 84–85, Hathaway *et al.*, *The Law of Cyber-Attack*, *supra* note 36 at 847, Dinniss, *Cyber Warfare and the Laws of War*, *supra* note 165 at 74 and Dinstein, *Computer Network Attacks and Self-Defense*, *supra* note 57 at 105.

sending of armed bands by a state to another state may classify as an armed attack if the scale and effects of the attack are such that it would have constituted an armed attack if it were carried out by regular armed forces.[178] The ICJ mentioned the scale and effects of the attack with regard to the threshold of an armed attack, but the Tallinn Manual finds it to be equally useful in determining whether an operation constitutes force.[179]

Effects-based Approach

The group behind the Tallinn Manual agreed that 'acts that injure or kill persons or damage or destroy objects are unambiguously uses of force'. Towards the other end of the spectrum, the Manual states that non-destructive, psychological cyber operations intended solely to undermine confidence in a government or economy do not qualify as uses of force.[180] As regards other, more ambiguous cases, the Manual non-exhaustively lists eight factors which are considered to be influential when states assess whether a cyber operation constitutes a use of force.[181] These criteria are severity, immediacy, directness, invasiveness measurability of effects, military character, state involvement and presumptive legality. They are based on the ones suggested by Michael Schmitt first in 1999 and are not, according to the Manual, meant as legal criteria.[182] Neither are the criteria meant to give a binary answer to whether or not a certain act qualifies as force, and such a claim would of course be overreaching. The criteria do, however, make it possible to examine an operation on a sliding scale. Such an approach is justified. Exact rules and their automatic application is, as noted by Martti Koskenniemi, problematic because of their over- and under-inclusiveness.[183] The extreme variety of possible cyber operations and the uncertainty regarding the whole field emphasizes this point even further.

The Tallinn Manual expressly states that the presented criteria are meant to be factors influencing the use of force assessments by states and not legal criteria.[184] This is a bit more hesitant view than the one presented by Schmitt in his earlier article in 1999 and it

178 *Nicaragua*, *supra* note 114 at para. 195.
179 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 45–46.
180 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 46–48.
181 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 47–51.
182 Schmitt, *Computer Network Attack and the Use of Force in International Law*, *supra* note 122 at 914–915.
183 Martti Koskenniemi, 'The Lady Doth Protest too Much' – Kosovo, and the Turn to Ethics in International Law', 65 *The Modern Law Review* (2002) 159–175 at 167.
184 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 48.

has been the target of some critique.[185] Schmitt himself noted that his approach is influenced by the New Haven School and its policy-oriented view.[186] While the criteria of the Tallinn Manual – sometimes also referred to as the Schmitt criteria – do offer a basis for the evaluation of an operation, the determination seems to in many cases boil down to the severity criterion and a seemingly simple result: if a cyber operation produces physical damage to persons or property comparable to that produced by a kinetic attack, the operation counts as force.[187] Katharina Ziolkowski approaches the issue from a similar viewpoint and argues that there is no need for special criteria beyond focusing on the effects.[188] What kind of physical damage suffices, is, of course, another question. The Tallinn Manual notes that the severity criterion is subject to a *de minimis* rule.[189] Such a rule should indeed be applied in the determination as cyber attacks are also capable of causing negligible physical damage, such as damage to a hard drive of a single computer which should not by itself count as a use of force.

One problem with the Tallinn Manual criteria is related to their ambiguity and malleability, which has also been acknowledged by Michael Schmitt.[190] They have been used to argue that the 2007 attacks on Estonia reached the threshold of force.[191] The argument is, however, not convincing without subscribing to the view that the notion of force includes economic force – and even then it could be asked whether or not the attacks caused so much economic damage as to constitute force. The same criteria can, more convincingly, also be used to argue that the attacks did in fact not constitute a use of force.[192] The wide-ranging criteria allow for broad interpretation to whichever direction wanted.[193] Then

185 See e.g. Ziolkowski, *Ius ad bellum in Cyberspace – Some Thoughts on the 'Schmitt-Criteria' for Use of Force*, *supra* note 12 at 308–309 and Lianne J. M. Boer, '"Restating the Law 'As It Is'": On the Tallinn Manual and the Use of Force in Cyberspace', 5 *Amsterdam Law Forum* (2013) 4–18 at 13–17. Boer's critique is not without issues, as it seems to be heavily based on the premise of the Manual and especially the rule at issue being a restatement of the law. However, the Manual itself states that 'any claim that every assertion in the Manual represents an incontrovertible restatement of international law would be an exaggeration'. Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 3.

186 Michael N. Schmitt, 'The "Use of Force" in Cyberspace: A Reply to Dr. Ziolkowski' in C. Czossek, R. Ottis and K. Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict Proceedings* (NATO CCD COE Publications: Tallinn, 2012), 311–317 at 315.

187 Silver, *Computer Network Attack as a Use of Force under Article 2(4)*, *supra* note 36 at 91.

188 Ziolkowski, *Ius ad bellum in Cyberspace – Some Thoughts on the 'Schmitt-Criteria' for Use of Force*, *supra* note 12 at 308.

189 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 48.

190 Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, *supra* note 171 at 578.

191 Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, *supra* note 171 at 577.

192 Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, *supra* note 176 at 1123-1124.

193 Silver, *Computer Network Attack as a Use of Force under Article 2(4)*, *supra* note 36 at 89 as well as Hathaway *et al.*, *The Law of Cyber-Attack*, *supra* note 36 at 847–848.

again, the criteria are, as stated in the Tallinn Manual, meant as factors that influence the assessments of states instead of purely legal criteria.[194]

Article 41 of the Charter states that the Security Council may decide what measures *not* involving the use of force may be employed, and that these may include interruption of economic relations and of postal, telegraphic, radio and other means of communication. Thus, on the basis of such formulation it can be surmised that the mere interruption of communication would not constitute a use of force. This supports the determination following from the effects-based view that for example denial-of-service attacks do not constitute uses of force.

Target-based Approach

The target-based approach expands the notion of force to be needlessly extensive. It would considerably lower the threshold of the use of force and risk escalating responses. Walter Gary Sharp, Sr. argues that the mere penetration by a state to critical computer systems which are important to the ability of a state to defend itself would demonstrate such hostile intent that it would justify the use of force in self-defence.[195] Such a view, however, is not reasonable. Gaining unauthorized access to a computer system may well be a criminal offence for an individual, but it does not by itself constitute a use of force even in the case of a critical system. Eric Talbot Jensen argues that the traditional framework on the use of force and self-defence does not offer sufficient protection from potential threats.[196] He claims that international law should evolve to recognize an inherent right of a state to self-defence against a computer network attack on critical national infrastructure, even if the attack does not amount to an armed attack in light of Article 51 of the UN Charter.[197] Jensen also argues that 'the requirement to attribute an attack before responding presents a significant gap in a nation's ability to defend itself'. According to him, the target of the attack should be a determining factor in justifying an active response 'regardless of the attacker's identity'.[198] This, then would mean that states would be able to respond by

194 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 48.
195 Walter Gary Sharp, Sr., *Cyberspace and the Use of Force* (Aegis Research Corporation: Falls Church, 1999) at 129–130.
196 Eric Talbot Jensen, 'Computer Network Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense', 38 *Stanford Journal of International Law* (2002) 207–240 at 221.
197 Jensen, *Computer Network Attacks on Critical National Infrastructure*, *supra* note 196 at 229.
198 Jensen, *Computer Network Attacks on Critical National Infrastructure*, *supra* note 196 at 232–234.

military force to attacks on certain targets without even determining the true source of the attack. Such a claim is insupportable and would even in practice bring about insurmountable difficulties: the attack may be routed through a neutral and an innocent country, or even through a computer in the same country as the target. His approach certainly takes into account the unique characteristics and challenges of cyber operations, but does not sufficiently consider the possibilities and dangers of escalation, even taking into account his view of the response being proportionate. Neither does it consider the possible problem of taking action against a state whose network was merely used as a vehicle for the delivery of the attack. Attribution must not be seen as an obstacle[199] but an unconditional requirement of a lawful response.

Instrument-based Approach

Applying the instrument-based model to cyber operations is problematic as well. Cyber attacks might well have severe consequences without using traditional military weapons which has been seen as the defining factor in the approach.[200] It would thus be difficult to fit cyber attacks into the framework. The possible consequences of cyber attacks vary a great deal, from inconvenience to physical destruction.[201] Grouping cyber attacks together and analogizing them to military weapons would be, because of the varying consequences, difficult if not impossible. Dividing the possible attacks into smaller, more detailed groups such as cyber attacks with physical consequences would effectively mean applying the effects-based model first.

4.4.4 Attempts and Unsuccessful Attacks

Another question is that of unsuccessful attacks and how they fit into the framework so focused on the effects of the attacks. The issue is somewhat different with cyber operations compared to conventional kinetic attacks: a missile or a bomb might miss its target, but it will nevertheless cause physical consequences. A failed cyber operation, however, might not cause any kind of physical consequences – in fact, it might very well go unnoticed altogether. While it is true that a purely effects-based rule would be under-inclusive in this sense and would not necessarily do much to deter attack attempts, there seems to currently

199 Jensen, *Computer Network Attacks on Critical National Infrastructure*, *supra* note 196 at 239–240.
200 Hathaway *et al.*, *The Law of Cyber-Attack*, *supra* note 36 at 846.
201 Schmitt, *Computer Network Attack and the Use of Force in International Law*, *supra* note 122 at 912.

be little support for counting unsuccessful attacks without any kind of physical consequences as uses of force.

A similar question can be raised regarding attacks that have been spotted and successfully foiled by the target of the attempted attack. A hypothetical situation can be drawn up to illustrate the issue: an attacker has successfully taken advantage of a vulnerability and placed a piece of malicious software on the computer network of a nuclear power plant. The attacker has not yet activated the malware and everything at the power plant is running normally. Then, the breach is discovered, the malware found, disabled and removed from the system. Subsequent analysis shows that the malware was capable of tampering with the cooling processes of the power plant in such a way that would have purportedly resulted in a meltdown and a major accident and significant loss of life. Furthermore, by reverse engineering the malware the breach and the placement of the malware can with reasonable confidence be attributed to a hostile state. Again, there has been no physical consequences but an act without a clear equivalent in the world of conventional kinetic attacks. It could reasonably be argued that the mere placement of the malware does not constitute a use of force and an attack had not yet taken place. In this sense, the breach might be likened to an airspace violation or, depending on the gravity of the possible consequences, perhaps to locking a missile on an enemy aircraft. The situation can be complicated more by hypothesizing that the malware was written in a way that it would have activated without an external command from the attacker, for example on a certain time and date. In such a case it could well be argued that an attack has already taken place, although it is less clear whether or not there would be support for such argumentation. Both instances could also be described as breaches of the principle of non-intervention, more closely examined later on. It is easy to imagine, though, that the victim state, especially in the latter case, would react in a more fierce way than the strict limitations of countermeasures would allow.

4.4.5 Cyber Assistance as Force

The question of the possibility of assistance counting as a use of force is especially relevant to cyber operations. There are several ways how a state may offer assistance to another state or a non-state actor in preparing a cyber attack. It might provide them knowledge about a zero-day vulnerability (or several of them), it might provide them more specific information about how to take advantage of said vulnerabilities or it might provide

them with a ready-made piece of software. Or, it might provide them information about the targeted system and how to achieve the intended consequences once they have gained access. The Tallinn Manual states, following the position of the International Court of Justice, that mere funding of for example a hacktivist group who conducts cyber operations does not constitute a use of force. Providing an organized group with malware and the training necessary to use it to carry out attacks would, however, qualify as a use of force.[202] This leads to the question of what kind of malware suffices? The malware might, for example allow for the attacker to gain access to a system. Such access could, theoretically and depending on the target, be used for either espionage or conducting an attack. Merely providing access to a system would not, in my view, constitute a use of force, even though access to the system is of course a central element of the attack. On the other hand, providing a malware that would not merely be an enabling factor but would in essence form the crux of the attack would more probably constitute a use of force, depending on the circumstances.

Whereas the provision of traditional weapons and training undoubtedly benefits the recipient and may even be the *sine qua non* of an operation, there still remains much to be done to carry out the proper operation. Cyber operations may, however, be considerably different in this sense. That is, the actual execution of the attack is a much smaller part of the whole operation when compared for example the paramilitary operations discussed in the *Nicaragua* case. In an extreme example, the assisting state may provide a complete attack package which merely needs to be executed.

4.5 Economic or Political Force

The prevailing view is that the ban of force in Article 2(4) does not cover economic or political force. One of the new threats brought along by cyber attacks is the possibility to cause potentially catastrophic economic consequences without any physical damage. An example of such would be a widespread attack on the banking system or a stock exchange that could topple the economy of a country, as well as cause cross-border ripple effects. Granted, the example is a rather extreme one, yet it helps to underline how cyber

202 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 46.

operations might affect and cause problems for the previously more clear distinction between physical and economic force.

Some of the views and argumentation advocating the inclusion of economic force into the ambit of Article 2(4) seem to often place unduly emphasis on the part of Article 2(4) that considers the use of force *against the territorial integrity or political independence* of any state. An example of such a view is the one of Walter Gary Sharp, Sr., who sees Article 2(4) as covering acts starting from coercive political and economic sanctions that threaten the territorial integrity or political independence of a state.[203] While the text of Article 2(4) surely enables such a reading, it is not supported by the *travaux préparatoires*, the Preamble of the UN Charter, the Friendly Relations Declaration or the Definition of Aggression Resolution, all of which point to interpreting Article 2(4) as banning the use of *armed* force.[204]

While they indisputably do not qualify as a use of force, the events of 23 April 2013 do provide an example of how susceptible to a variety of attacks the economy is. A group calling themselves the Syrian Electronic Army (aligned with the al-Assad regime) hacked the Twitter account of the news agency AP and posted a tweet claiming there had been an explosion at the White House and that president Obama had been injured.[205] In the minutes that followed the tweet, the Dow Jones index plummeted over 140 points equalling almost 140 billion dollars. As it became clear that no explosion had happened, the Dow bounced back in a matter of minutes. Another example of the fickleness of the global financial system is the reportedly planned cyber operation by the United States against Iraqi banks in preparation of the 2003 Operation Iraqi Freedom.[206] According to news reports, the U.S. had a plan to effectively freeze Saddam Hussein's funds by launching a cyber attack on Iraqi banks, but the plan was scrapped because it was feared that unpredictable consequences would spread around the globe in the highly networked banking system.

---

203 Sharp, *Cyberspace and the Use of Force*, *supra* note 195 at 91.
204 Randelzhofer, *Article 2(4)*, *supra* note 110 at 118.
205 Heidi Moore and Dan Roberts, 'AP Twitter hack causes panic on Wall Street and sends Dow plunging', *The Guardian*, 23 April 2013, <www.guardian.co.uk/business/2013/apr/23/ap-tweet-hack-wall-street-freefall>.
206 John Markoff and Thom Shanker, 'Halted '03 Iraq Plan Illustrates U.S. Fear of Cybewar Risk', *The New York Times*, 1 August 2009, <www.nytimes.com/2009/08/02/us/politics/02cyber.html>.

It remains to be seen whether or not the emergence of cyber operations with possible severe economic consequences affects the debate about economic force. As Grigorij Tunkin writes, the use of economic force may represent a considerable threat to the political independence of states and to the stability of international relations.[207] Cyber operations pose new opportunities for the realization of such a threat. This may very well call for a reappraisal of the scope of the notion of force, or alternatively of the possibilities of states to react to breaches of the principle of non-intervention. Many commentators focus on the textual reading of the Charter when arguing that Article 2(4) covers only armed force and note that the Preamble of the Charter speaks of 'armed force' and that Article 44 supports such a view as well.[208] While it is true that such evidence is hard to pass, somewhat less notice has been paid to the customary international law rule banning the use of force. As mentioned, the prohibition is also part of customary international law,[209] and as such subject to modification. As the ICJ noted in *Nicaragua*, the reliance by a state on a novel right may tend towards a modification of customary international law if shared by other states.[210] There is no evidence of such state practice at the moment, but just as the events after the 9/11 terrorist attacks arguably lowered the standard for attribution to state from the levels set forth by the ICJ in *Nicaragua* or by the ICTY in *Tadić* rather swiftly,[211] a cyber attack with extreme economic consequences might very well have a similar effect to state practice. Such a hypothesis is, of course, at this point pure speculation. It is clear, however, that cyber operations are capable of pure economic consequences unachievable by other types of attacks.[212] Thus, analogizing cyber operations with traditional economic pressure is not necessarily a satisfactory approach.

4.6 Chapter VII of the UN Charter

Chapter VII of the United Nations Charter sets a framework for the legitimate use of force under the authorization of the Security Council. Article 39 gives the Security Council the power to 'determine the existence of any threat to the peace, breach of the peace or act of aggression' and the power to decide what responsive measures are in order to maintain

207 Grigorij Ivanovič Tunkin, *Recht und Gewalt im internationalen System* (Duncker & Humblot: Berlin 1986) at 62.
208 Randelzhofer, *Article 2(4)*, *supra* note 110 at 118.
209 *Nicaragua*, *supra* note 114 at paras 188–190.
210 *Nicaragua*, *supra* note 114 at para. 207.
211 Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, *supra* note 171 at 599.
212 Benatar, *The Use of Cyber Force*, *supra* note 162 at 391.

international peace and security. The variety of measures range in practice from economic sanctions and no-fly zones to authorizing the use of force against a UN member state.

When using Chapter VII as a legal basis for actions, the Security Council has previously shown a clear preference to referring generally to Chapter VII rather than to specific articles.[213] More recently, however, the Security Council has also referred to specific articles after the controversy regarding the concept of revived or implied authorization used by the USA and the UK in Iraq (both after the first Gulf War and in 2003) and Kosovo.[214] To avoid any possibility for using the potentially ambiguous references in the resolutions to constitute a justification for the use of force, specific references were made in resolutions 1695 (2006) and 1718 (2006) regarding North Korea and resolution 1696 (2006) regarding Iran. The Security Council has also preferred to use a 'threat to peace' as the basis of its actions instead of a 'breach of peace' or an 'act of aggression'[215] and avoided pointing out the offenders.[216]

The Charter gives the Security Council the power to determine which actions it deems fit for a particular situation, so it is possible for it to authorize cyber operations as well. This might be done either specifically or, as seems more likely, as part of 'all necessary measures' to implement a resolution.[217] Article 41 empowers the Security Council to take non-forceful measures such as interruption of economic relations or means of communication and if such measures are inadequate, the Security Council may authorize forceful measures pursuant to Article 42. Thus far the Security Council has shied away from restricting communications because of the possibly ensuing human rights issues,[218] but cyber operations might theoretically offer a way to target military communications more specifically. Originally it was envisaged in Article 43 of the Charter that member countries would make armed forces available to the Security Council based on separate agreements. Article 43 has never completely been implemented and in the cases where the Security Council has authorized the use of force the operations have been carried out by

213 Tarcisio Gazzini, *The Changing Rules on the Use of Force in International Law* (Manchester University Press, 2005) at 7.
214 Christine Gray, *International Law and the Use of Force* (Oxford University Press, 2008) at 366.
215 Gazzini, *The Changing Rules on the Rules of Force in International Law, supra* note 213 at 10.
216 Gray, *International Law and the Use of Force*, *supra* note 214 at 22.
217 Such formulation has been used by the Security Council in resolutions 1973 (2011) and 678 (1990), and in 836 (1993) limited to the use of air power.
218 Jochen Frowein and Nico Krisch, 'Article 41' in Bruno Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2nd Edition, Oxford University Press, 2002), 735–749 at 741.

coalitions of the willing.[219] Were the Security Council to authorize cyber operations, it is imaginable that they would be carried out in a similar fashion.

Article 39 gives the Security Council the power to determine the existence of a threat to or a breach of the peace or an act of aggression. It thus may determine that a cyber operation would qualify for such an act, even if it would not be sufficiently grave as to justify self-defence based on Article 51 or breach Article 2(4). The Tallinn Manual suggests that in addition to in specific cases identifying cyber operations belonging to the purview of Article 39 it could declare certain cyber operations (for example those targeting critical national infrastructure) as threats to or breaches of the peace or acts of aggression *in abstracto* similarly to international terrorism and weapons of mass destruction.[220] This, of course, is entirely possible, especially should a disrupting attack take place or an inability to conclude a multilateral treaty transpire. However, it does not seem likely: defining which kinds of operations and targets would suffice would present considerable difficulties.

219 Jochen Frowein and Nico Krisch, 'Article 43' in Bruno Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2nd Edition, Oxford University Press, 2002), 760–763 at 762–763.

220 Schmitt, *Tallinn Manual*, *supra* note 21 at 69.

5 Cyber Operations as Armed Attacks and the Right to Self-Defence

5.1 Overview of the Right to Self-Defence

After the freedom to wage war became more limited in the beginning of the 20th century the legal justifications for going to war became more significant. The idea of self-defence as a justification for the use of force was by no means a new development: it had indeed been used previously as a justification as well, but for political purposes.[221] The right to self-defence is considered to be a part of customary international law,[222] and it is included in the UN Charter, whose Article 51 states that

> *Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security.*

The Article can be interpreted in various ways which will more closely be examined in the following pages. The most pressing question is what is considered to be an armed attack that triggers the right to self-defence. As with the previously discussed notion of force, there is no explicit and agreed upon definition but some positions by the International Court of Justice and a plethora of scholarly opinions. The Court stated in *Nicaragua* that just as Articles 2(4) and 42 of the UN Charter, also Article 51 does not refer to specific weapons.[223] It thus follows that they also apply to cyber operations as well and that a state has the right to use force in self-defence if it is a victim of a cyber attack that rises to the level of an armed attack. And correspondingly, a state may use cyber operations when acting in self-defence in response to an armed attack regardless of the weapons used in the attack against it.

---

221 Randelzhofer, *Article 51*, *supra* note 140 at 789.

222 *Nicaragua*, *supra* note 114 at para. 176. For a similar view of self-preservation as grounds for the use of force predating both the United Nations and the League of Nations see Lassa Oppenheim, *International Law – A Treatise. Volume I: Peace* (Longmans, Green and Co.: London, 1905) at 178.

223 *Nuclear Weapons*, *supra* note 29 at para. 39.

As mentioned, the right to self-defence is also part of customary international law. The ICJ stated in *Nicaragua* that customary international law continues to co-exist with treaty law, and the rules do not have exactly the same content.[224] This, of course, begs the question of how does the right to self-defence based on customary international law differ from the right guaranteed in Article 51. This will be discussed especially in the context of anticipatory self-defence in chapter 5.5.

Another essential issue involves the content and limitations of the right to self-defence. These stem from the *Caroline* affair of 1837, which has since gained a somewhat mythical status in the field of international law. In the correspondence between United States Secretary of State Daniel Webster and the British authorities after the incident, Webster wrote that the British government must show 'a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation'.[225] There is some ambiguity as to whether the incident is a useful and generally applicable precedent, as it originally related to cases of anticipatory self-defence.[226] However, the requirements of necessity and proportionality have been affirmed by the International Court of Justice in several cases and there remains little controversy about the existence of such requirements in customary international law.[227] The more detailed content of the requirements and their application in specific cases is however far from uncontroversial. It is agreed, though, that the purpose of self-defence must be to stop and repel an attack and not retaliate.[228] The ICJ usually applies the requirements separately,[229] yet they are clearly linked. Providing a comprehensive definition for a proportionate attack is impossible: the facts and context of a particular case influence the answer.[230]

While states do have differing interpretations on which acts justify self-defence and the content of the right, they nevertheless usually rely on self-defence as the legal justification

224 *Nicaragua*, *supra* note 114 at paras 176, 178.
225 The correspondence is reprinted in *The Works of Daniel Webster – Volume VI, 10th Edition* (Little, Brown and Company: Boston, 1857) at 261.
226 *Nicaragua*, *supra* note 114, Dissenting Opinion of Judge Schwebel at para. 200.
227 *Nicaragua*, *supra* note 114 at para. 194, *Nuclear Weapons*, *supra* note 29 at para. 141, *Oil Platforms* (*Islamic Republic of Iran v. United States of America*), Judgment, I. C. J. Reports 2003, p. 161. at para. 43 and *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, I. C. J. Reports 2005, p. 168 at para. 147.
228 Gray, *International Law and the Use of Force*, *supra* note 216 at 150.
229 See e.g. *Oil Platforms*, *supra* note 227 at paras. 73, 77.
230 Gray, *International Law and the Use of Force, supra* note 214 at 151.

for their actions,[231] even though they might at the same time push the boundaries of the right to a breaking point. An example of the contrary are the military actions of Turkey against Iraq, especially after the first Gulf War in the 1990s when Turkish forces carried out operations against Kurds on Iraqi territory. Turkey never explicitly invoked the right to self-defence but instead justified its operations on the basis that Iraq could not prevent using its territory for 'staging terrorist acts against Turkey', and thus the 'legitimate' acts of Turkey did not violate the sovereignty of Iraq.[232] Later, Turkey referred to the Friendly Relations Declaration and to the principle of necessity.[233] Iran, while conducting similar operations in Iraqi territory, invoked Article 51 and notified the Security Council that it was acting in self-defence.[234] Turkey carried out military operations in 2006 and 2007 against the Kurdish group PKK, but did not offer any legal justification for its use of force in this case and did not report the operations to the Security Council.[235]

Article 51 preserves the right to individual or collective self-defence. The consensus is that collective self-defence does not require any pre-existing arrangement, such as a regional treaty or a bilateral assistance treaty.[236] In other words, *ad hoc* assistance of another state is possible. That said, the victim state of the attack must still declare that it has been the target of an armed attack.[237] In other words, a third state may not unpromptedly, solely based on its own assessment, act in self-defence of the victim state. The ICJ discussed the issue in *Nicaragua* regarding the claim presented by the United States that it was acting in self-defence on behalf of El Salvador, Honduras and Costa Rica. The Court stated that Honduras and Costa Rica did not make any references to collective self-defence and that El Salvador asked for the United States to exercise the right to collective self-defence only on

231 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 97, see also McCoubrey and White, *International Law and Armed Conflict, supra* note 111 at 112 and *supra* at 27.

232 Letter Dated 24 July 1995 from the Charge d'Affaires A.I. of the Permanent Mission of Turkey to the United Nations Addressed to the President of the Security Council. UN Doc. S/1995/605. It should be noted that Turkey did not unpromptedly report the operations to the Security Council (as would be required by the Charter in cases of self-defence based on Article 51) but its letter was in response to a condemnation of the acts by the Libyan ambassador to the UN (UN Doc. S/1995/566).

233 Identical Letters Dated 27 June 1996 from the Charge d'Affaires A.I. of the Permanent Mission of Turkey to the United Nations Addressed to the Secretary-General and to the President of the Security Council. UN Doc. S/1996/479. These letters followed a letter from the Minister for Foreign Affairs of Iraq (UN Doc. S/1996/401).

234 Letter Dated 25 May 1993 from the Permanent Representative of the Islamic Republic of Iran to the United Nations Addressed to the Secretary-General. UN Doc. S/25843.

235 Gray, *International Law and the Use of Force*, *supra* note 216 at 143.

236 Stanimir A. Alexandrov, *Self-Defense Against the Use of Force in International Law* (Kluwer Law International: The Hague 1996) at 101.

237 *Nicaragua*, *supra* note 114 at para. 195 and *Oil Platforms*, *supra* note 227 at para. 51.

a much later date.[238] This led the Court to conclude that the condition *sine qua non* for the exercise of collective self-defence was not fulfilled.[239]

5.2 Notion of an 'Armed Attack'

As discussed in chapter 4.3, the illegal acts of states relating to the topic at hand may be divided to three categories: interventions, uses of force and armed attacks.[240] As is the case with Article 2(4) and the term 'force', the UN Charter does not explicitly define the term 'armed attack' either. The relation of the two terms has also been the subject of some debate and will be discussed in further detail in chapter 5.2.2.

A traditional case and a clear example of an armed attack is a sufficiently grave attack (with significant damage, including fatalities) carried out by the armed forces of a state. Such is indisputably an armed attack to which a state may respond forcibly with the justification of Article 51 of the UN Charter as well as the 'inherent right' to self-defence. But what about cases where the attack and its consequences are less grave? Or where the attack is carried out by non-state forces? These issues have been heatedly discussed, and after the 9/11 attacks the much of the debate has concerned the possibility of self-defence against terrorist attacks. The questions are also relevant to the discussion about cyber operations, since the consequences of such operations are varied and do not in most cases clearly cross the threshold of an armed attack. Cyber operations can also easily be carried out by non-state actors, either with or without the support of a state.

The International Court of Justice has contemplated the notion of an armed attack in several cases, and while the exact limits of the notion remain elusive, some guidance can be mustered by examining the relatively clear cases. The Court first examined the issue in the *Nicaragua* case, which was summarily described earlier with regard to the notion of force.[241] The majority of the ICJ found that even though the assistance to the contras could be regarded as a threat or use of force or an intervention, it did not constitute an armed attack that would have justified collective self-defence,[242] which was what the United

238 *Nicaragua*, *supra* note 114 at paras 233–234.
239 *Nicaragua*, *supra* note 114 at para. 237.
240 McCoubrey and White, *International Law and Armed Conflict*, *supra* note 111 at 62.
241 *Supra* at 32.
242 *Nicaragua*, *supra* note 114 at para. 195.

States claimed.[243] In discussing the matter, the Court also distinguished 'mere frontier incidents' from armed attacks.[244] It is also noteworthy that the ICJ stated that it did not have enough information available about the circumstances and the possible motivations of the incursions into the territory of Honduras and Costa Rica.[245] This has been taken to imply that the Court would find the circumstances and motivations relevant for the determination of whether the operation would be classified as a frontier incident or an armed attack.[246]

Another significant case is *Oil Platforms*, where the Court considered another claim of self-defence by the United States in response to alleged attacks by Iran on U.S.-flagged ships during the Iran–Iraq War in the 1980s. Two incidents were at the centre of the case brought by Iran. First, in October 1987 the *Sea Isle City*, a Kuwaiti tanker sailing under the U.S. flag at the time was hit by a missile near Kuwait.[247] The ship was damaged and six crew members were injured.[248] The United States responded by attacking Iranian offshore oil production facilities. Six months later, a U.S. navy frigate, the *Samuel B. Roberts*, struck a mine near Bahrain, and the United States again responded by attacking two oil production complexes.[249] Regarding the *Sea Isle City* attack, the Court found that the evidence indicating the responsibility of Iran was not sufficient.[250] The Court also noted that the missile could not have been specifically aimed at a certain ship. The United States also named other attacks in the preceding months and asserted that the attack on the *Sea Isle City* was only the latest in a series of attacks, but the Court dismissed these claims for various reasons and stated that even setting aside the question of Iranian responsibility, the incidents did not constitute an armed attack on the United States.[251] As regards the *Samuel B. Roberts* attack, the Court again dismissed the U.S. claim of self-defence due to the circumstances, including the inconclusive evidence of the responsibility of Iran. In discussing the attack, the Court stated that it did not exclude the possibility of an attack on a single military vessel constituting an armed attack.[252]

---

243 *Nicaragua*, Counter-Memorial of the United States of America, *supra* note 155 at para. 202.
244 *Nicaragua*, *supra* note 114 at para. 195.
245 *Nicaragua, supra* note 114 at para. 231.
246 Gray, *International Law and the Use of Force*, *supra* note 214 at 179.
247 *Oil Platforms, supra* note 227 at para. 25.
248 *Oil Platforms*, *supra* note 227 at para. 52.
249 *Oil Platforms, supra* note 227 at para. 25.
250 *Oil Platforms*, *supra* note 227 at para. 61.
251 *Oil Platforms*, *supra* note 227 at para. 64.
252 *Oil Platforms*, *supra* note 227 at para. 72.

Generally the International Court of Justice has taken a cautious view and steered clear of the most controversial issues where possible.[253] It did so for example in the *Armed Activities* case where it first found that there was not enough evidence to attribute the activities of the rebel group ADF to the Republic of Congo and then explicitly stated that because of this, there is no need for the Court to examine whether states may invoke the right to self-defence against large-scale attacks by irregular forces.[254]

The issue of what constitutes an armed attack was also touched upon by the Eritrea/Ethiopia Claims Commission. It briefly noted that 'localized border encounters', even those involving the loss of life, do not constitute armed attacks.[255] It thus followed the reasoning of the International Court of Justice and the distinction it made in *Nicaragua* separating armed attacks and 'mere frontier incidents'.[256]

5.2.1 Accumulation of Events

Small-scale attacks and incursions have been considered in light of a theory of accumulation of events, also sometimes called the pin prick theory. States have claimed to have responded to a series of attacks that collectively have amounted to an armed attack, even though each individual attack considered separately has not crossed the threshold.[257] The International Court of Justice has referred to the possibility of acts collectively amounting to an armed attack in its judgments without taking a definite position on the matter.

In *Nicaragua*, the ICJ stated that the lack of information made it difficult to decide whether or not the separate smaller incidents 'singly or collectively' amounted to an armed attack.[258] In other words, the Court implied that such a possibility indeed existed. In the *Oil Platforms* case the United States asserted both before the ICJ and in its letters to the Security Council that it was responding not merely to the attack on the *Sea Isle City* and the *Samuel B. Roberts* but to a series of such attacks.[259] While the Court did state that the

253 Gray, *International Law and the Use of Force*, *supra* note 214 at 129.
254 *Armed Activities*, *supra* note 227 at para. 147.
255 *Partial Award, Jus Ad Bellum, Ethiopia's Claims 1–8 Between the Federal Democractic Republic of Ethiopia and the State of Eritrea,* Eritrea-Ethiopia Claims Commission, 19 December 2005 at para. 11.
256 *Nicaragua*, *supra* note 114 at para. 195.
257 Gray, *International Law and the Use of Force*, *supra* note 173 at 155.
258 *Nicaragua*, *supra* note 114 at para. 231.
259 *Oil Platforms*, *supra* note 227 at paras 62, 67. See also Letter Dated 19 October 1987 from the

incidents in question did not amount to an armed attack because of other reasons (for example, the *Sea Isle City* could not have been specifically targeted, and another ship, the *Texaco Caribbean* was not sailing under a U.S. but a Panamanian flag), it implied that certain acts, taken cumulatively, could constitute an armed attack.[260] In the *Armed Activities* case the Court again could be seen as insinuating to the direction of such a possibility, although less explicitly than in *Nicaragua* and *Oil Platforms*.[261] The Court stated that even if the 'series of deplorable attacks could be regarded as cumulative in character', they were not attributable to the Republic of Congo. The question of cumulative attacks was at issue in the *Cameroon v. Nigeria* case as well, but the Court concluded that Cameroon had not sufficiently shown that the acts in question were imputable to Nigeria and thus avoided ruling on the issue of whether the separate acts taken as a whole constituted an armed attack.[262]

It is thus conceivable that a series of pin-prick attacks could be collectively seen as an armed attack if the attacks are sufficiently related and the consequences sufficiently grave. The same logic applies to cyber operations as well. In other words, a series of related cyber attacks by the same actor may be considered as a 'composite armed attack'.[263] An example might be a cyber attack on the electricity grid: attacking an individual transformer or even a power plant might cause physical damage that would constitute force but might not be sufficiently grave as to be an armed attack. However, a series of similar attacks carried out simultaneously on several transformers or power plants might very well collectively cross the threshold of an armed attack.

5.2.2 Notions of Armed Attacks and Force

According to Article 2(4) of the UN Charter, states shall refrain from the threat or use of force and Article 51 gives states the right to defend themselves if an 'armed attack' occurs. The International Court of Justice has described armed attacks as the most grave forms of

---

Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council, UN Doc. S/19219 and Letter Dated 18 April 1988 from the Acting Permanent Representative of the United States to the United Nations Addressed to the President of the Security Council, UN. Doc S/19719.

260 *Oil Platforms*, *supra* note 227 at para. 64.

261 *Armed Activities*, *supra* note 227 at para. 146.

262 *Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea Intervening)*, Judgment, I. C. J. Reports 2002, p. 303 at paras. 323–324.

263 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 56.

the use of force in *Nicaragua,*[264] and has since reaffirmed its position in *Oil Platforms.*[265] It thus seems clear that not all uses of force trigger the right to self-defence. This distinction has been challenged as well, and some commentators note it is not fully supported by state practice. They argue that states generally do not tolerate hostile military activity and reserve the right to counter such activities even if they do not amount to a grave use of force.[266] Among the critics is the former U.S. State Department Legal Advisor William H. Taft, who argues that the separation of the two notions would encourage states to engage in a series of smaller attacks to avoid responsibility.[267] Christine Gray, for example, considers this argument to be implausible and notes the lack of such practice since the case.[268] Tarcisio Gazzini argues that setting a higher threshold for the right to self-defence would expose states to 'unacceptable risks' and notes that the limits set by the requirements of immediacy, proportionality and necessity do provide an adequate safeguard against the abuse of the right to self-defence.[269] While the legal status of responding forcibly to all uses of force is not clear, it should also be noted that states most likely may rely on the response being accepted if it was proportional to the original attack.[270]

In a separate opinion to the *Oil Platforms* judgment, Judge Simma reaffirms a sort of an intermediate position taken earlier in a 1984 book. He submits that there are indeed two levels of acts: the level of armed attacks in the sense of Article 51 and a lower level of hostile military action (he avoids using using the term 'force'). According to his view, a state may defend itself against the lower level actions as well, but 'within a more limited range and quality of responses'. Such acts do not justify collective self-defence and are 'in a particularly strict way' subject to the requirements of necessity and proportionality.[271] Such a view indeed would resolve some of the practical problems ensuing from the separation of thresholds of an use of force and an armed attack and would be in line with state practice

264 *Nicaragua*, *supra* note 114 at para. 191.
265 *Oil Platforms*, *supra* note 227 at para. 51.
266 Gazzini, *The Changing Rules on the Use of Force in International Law*, *supra* note 213 at 133 and 139.
267 William H. Taft, 'Self-Defense and the Oil Platforms Decision', 29 *Yale Journal of International Law* (2004) 295–306 at 300–01. The current State Department Legal Advisor Harold Koh reaffirmed in 2012 that this is the position of the United States. See Koh, *International Law in Cyberspace*, *supra* note 28 at 7.
268 Gray, *International Law and the Use of Force*, *supra* note 214 at 148.
269 Gazzini, *The Changing Rules on the Use of Force in International Law*, *supra* note 213 at 138.
270 Miia Aro and Jarna Petman, *Voimankäytön oikeuttaminen ja sotilaallisten järjestelmien muutokset Euroopassa ja Suomessa* (The Erik Castrén Institute of International Law, University of Helsinki, 1999) at 37.
271 *Oil Platforms*, *supra* note 227, Separate Opinion of Judge Simma at paras 12–13.

of not tolerating even smaller scale operations. States regularly have invoked the right to self-defence when resorting to force,[272] however far-fetched it might be in some situations especially regarding attacks of a smaller scale.[273]

In discussing the separation of the notions and especially in arguing on the basis of the drafting process and the *travaux préparatoires* of the Charter, it should be kept in mind that the collective security system envisioned in the Charter differs from the one that it has developed to. The Cold War effectively paralyzed the Security Council for decades and no special agreements pursuant to Article 43 have been concluded to make armed forces available to the Security Council.[274] Justifying the separation of armed attacks and force on the basis of the text of the Charter and the *travaux préparatoires* thus warrants a critical look. If Article 51 was meant as a mechanism which could only be resorted to in the most grave forms of the use of force and in cases where the Security Council has not yet acted – as can be construed from the text of Article 51, seeing how it only gives the right to self-defence 'until the Security Council has taken measures' – Articles 43–49 gain much more significance which has never materialized. Thus, a central element of the original Charter system is missing. In other words, if the forces never made available to the Security Council were meant to address also those uses of force not constituting armed attacks, it begs the question whether or not the higher threshold for armed attacks is still justified. That said, good arguments remain for the separation, among which is the avoidance of a spiralling use of force. Also, Tarcisio Gazzini argues that even assuming the effective functioning of the collective security system, the disconnect between the notions of force and armed attack would still represent an 'unrealistic loophole'.[275]

To summarize, the prevailing view is that there is a difference between the notions of force and armed attack. There are arguments to challenge the view, and *de lege ferenda* claims that the gap is shrinking have some support in state practice. However, the text of the Charter and the repeated interpretations by the International Court of Justice cannot be easily bypassed.

---

272 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 97. Also McCoubrey and White, *International Law and Armed Conflict, supra* note 111 at 113.

273 Thomas M. Franck, *Recourse to Force – State Action Against Threats and Armed Attacks* (Cambridge University Press, 2002) at 112.

274 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 317–318, 329–330.

275 Gazzini, *The Changing Rules on the Use of Force in International Law*, *supra* note 213 at 138.

5.2.3 Assistance as an Armed Attack?

The Court concluded in *Nicaragua* that the supply of weapons or logistical or other support to the rebels did not amount to an armed attack. This could, however, according to the Court be regarded as a threat or use of force as well as an intervention in the affairs of other states.[276] The Court held the same view in 2005 in *Armed Activities on the Territory of the Congo*, where Uganda argued unsuccessfully that logistical support to armed bands with knowledge of their objectives might constitute an armed attack.[277] In a dissenting opinion to the *Nicaragua* judgment, Judge Jennings saw that the provision of arms coupled with 'other kinds of involvement' may be an important element of an armed attack.[278] Dissenting Judge Schwebel disagreed with the majority and took the position that the Nicaragua was indeed 'substantially involved' in supporting of the insurgents in a way referred to in the Definition of Aggression, and that the substantial involvement was enough to justify self-defence.[279] Christine Gray, for example, does not find the view of the dissenting Judges persuasive and finds no support for their argumentation. The Security Council has also discussed the supply of arms or other forms of support in several cases, but never has it considered them to amount to an armed attack.[280]

It also seems improbable that assistance in the context of cyber operations would constitute an armed attack. It might, of course, be possible for a state to supply a ready-made cyber attack for a non-state actor to be launched, or such guidance that it would, at least following the view of Judges Jennings and Schwebel, constitute an armed attack – provided, of course, that the resulting attack would be of sufficient gravity. However, such close connection with the attack would probably mean that the question would be approached from the side of state responsibility and whether or not the attack would be attributable to a state.

276 *Nicaragua, supra* note 114 at para. 195.
277 *Armed Activities on the Territory of the Congo,* Counter-Memorial by Uganda, Volume I, 21 April 2001, at para. 350.
278 *Nicaragua, supra* note 114, Dissenting Opinion of Judge Jennings at 543.
279 *Nicaragua, supra* note 114, Dissenting Opinion of Judge Schwebel at paras 166–167.
280 Gray, *International Law and the Use of Force*, *supra* note 214 at 132.

5.3 Acts of Non-State Actors as Armed Attacks?

5.3.1 Acts by Irregular Forces

Article 2(4) refers explicitly to member states and bans them from using force, whereas Article 51 does provide for member states the right to self-defence against an armed attack without reference to the perpetrator. There has been debate about the issue since the *Nicaragua* judgment by the International Court of Justice, and some, such as Yoram Dinstein, have argued that just as the target state is entitled to exercise self-defence against an attack by another state, it is empowered to defend itself against a group operating within that state.[281] Indeed, there is nothing in the text of the Charter to *prima facie* prevent such a reading. The prevailing view is that Article 51 covers the acts of states and acts committed by non-state actors that are attributable to the state.[282]

The question has been prominent after the 9/11 attacks, and the Security Council has several times referred to international terrorism as a threat to the peace since the 9/11 attacks and passed several resolutions imposing sanctions in response to terrorism.[283] It has not, however, responded to terrorism by explicitly mandating the use of force.[284] The United States stated it was exercising its right to individual and collective self-defence and cited the 9/11 attacks and an ongoing threat.[285] As much as the issue has been debated after the 9/11 attacks, using self-defence as the legal basis for responding to acts of terrorism is by no means an occurrence brought on by 9/11. Portugal claimed it was acting in self-defence in response to terrorist acts from Guinea, Senegal and Zambia in the 1960s and 1970s. Such claims were also made by the South African apartheid regime and Israel. These claims were by and large not accepted, but the circumstances were rather different: for example Portugal claimed to be defending its colonies in the midst of decolonization.[286]

281 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 269–270.

282 See e.g. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, I. C. J. Reports 2004, p. 136, Separate Opinion of Judge Kooijmans at para. 35, where he notes the view to have been the 'generally accepted interpretation for more than 50 years' and Randelzhofer, *Article 51*, *supra* note 140 at 802.

283 For example resolutions 1368 (2001, after the 9/11 attacks), 1438 (2002, after the Bali bombing), 1530 (2004, after the Madrid metro attacks).

284 Michael N. Schmitt, 'Responding to Transnational Terrorism under the Jus ad Bellum' in Michael N. Schmitt and Jelena Pejic (eds), *International Law and Armed Conflict: Exploring the Faultlines – Essays in Honour of Yoram Dinstein* (Martinus Nijhoff Publishers, Leiden, 2007), 157–195 at 161.

285 Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council. UN Doc. S/2001/946.

286 Gray, *International Law and the Use of Force*, *supra* note 214 at 136–140.

In *Nicaragua*, the ICJ took the position that actions by irregular forces ('armed bands, groups, irregulars or mercenaries') against another state may constitute an armed attack if the forces are sent by or on behalf of a state and if the actions are of certain gravity. That is, if the scale and effects of the actions are comparable to an attack by the regular forces. The Court refers to the description in Article 3(g) of the Definition of Aggression resolution, which, according to the Court, may be taken to reflect customary international law.[287] The Article defines the sending of irregular forces who carry out acts of armed force as an act of aggression if the acts carried out are of sufficient gravity against a state. Also a 'substantial involvement' in the sending of the armed bands suffices. The application of such a concept has been more controversial than its existence, and much of the debate and disagreement has primarily been about whether there has been an armed attack in the first place.[288]

The Court touched upon the issue of irregular forces again in its *Wall* Advisory Opinion of 2004, which concerned the building of a wall by Israel in the West Bank. Israel claimed it was acting in self-defence, but the Court found that Article 51 had no relevance in the case. The majority interpreted Article 51 as recognizing the right to self-defence in cases of armed attacks by states against another states but noted that Israel had not claimed that the attacks against it were in fact imputable to a state.[289] Judge Higgins in his dissenting opinion finds this to be a result of the determination the Court made in *Nicaragua* and notes that nothing in the text of Article 51 specifies that self-defence would only be available against armed attacks by states.[290] Also relevant was the fact that the threat Israel referred to originated from Israeli-controlled Occupied Palestinian Territory and the question was not thus of international terrorism.[291] Judge Kooijmans, in his separate opinion, regrets that the Court did not take notice of the 'new approach' to self-defence as manifested in the Security Council resolutions 1368 (2001) and 1373 (2001), where the Security Council recognized the right to self-defence in cases of international terrorism

287 *Nicaragua*, *supra* note 114 at para. 195. The Nicaraguan memorial on the merits of the case quotes extensively the writings of jurists, the actions of the United Nations and positions taken by the United States in demonstrating that the use of non-regular forces by a state is in breach of Article 2(4). I. C. J. Pleadings, Volume IV, Memorial of Nicaragua (Merits) at paras 227–247.
288 Gray, *International Law and the Use of Force*, *supra* note 214 at 173–175.
289 *Wall*, *supra* note 282 at para. 139.
290 *Wall*, *supra* note 282, Separate Opinion of Judge Higgins at para. 33.
291 *Wall*, *supra* note 282 at para. 139.

without referencing a state as the perpetrator.[292] Then again, as Christine Gray points out, the Court did not explicitly say that the right of self-defence exists *only* in cases of attacks by a state. The Court noted that Article 51 had no relevance in the case because of the non-international nature of the threat and the lack of claim by Israel imputing another state. The opinion could then also be interpreted as leaving open the possibility of armed attacks by non-state actors justifying self-defence in cases of international terrorism.[293] Indeed, the Court refers to the aforementioned Security Council resolutions and explicitly states that the situation was different from them.[294]

Another case where the Court was again faced with the issue of irregular forces and self-defence is the *Armed Activities on the Territory of the Congo*. The Court found there to be no proof that the attacks against Uganda were carried out by irregular forces sent by or on behalf of the Democratic Republic of Congo.[295] Because of the circumstances, the Court noted that it had no need to examine the question of irregular forces and self-defence more closely.[296] This was to the chagrin of Judges Simma and Kooijmans who both would have liked the Court to clarify its position regarding the actions a state could take in cases where the involvement of a state could not be proved.[297]

The Tallinn Manual notes that the ICJ 'does not seem to have been prepared' to adopt the approach taken by the United States after the 9/11 attacks, that is, invoking Article 51 and using self-defence as a justification for Operation Enduring Freedom in Afghanistan.[298] The Manual refers to the *Wall* Advisory Opinion and the *Armed Activities* judgment, both of which were discussed above. Such a view of the ICJ is not necessarily well reasoned. As mentioned, the circumstances taken as a whole in *Wall* led to the dismissal of the claim of self-defence: the attacks originated from Israeli-occupied territory and Israel did not impute them to another state. In *Armed Activities* the Court found there to be no evidence of a state being behind the attacks. It should also be noted that even though it was Al-Qaeda that carried out the 9/11 attacks, the United States in its letter to the Security

292 *Wall, supra* note 282, Separate Opinion of Judge Kooijmans at para. 35.
293 Gray, *International Law and the Use of Force*, *supra* note 214 at 135–136.
294 *Wall, supra* note 282 at para. 139.
295 *Armed Activities*, *supra* note 227 at para. 146.
296 *Armed Activities*, *supra* note 227 at para. 147.
297 *Armed Activities, supra* note 227, Separate Opinion of Judge Kooijmans at para. 25 and Separate Opinion of Judge Simma at para. 8.
298 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 58–59.

Council explicitly refers to the support given to Al-Qaeda by the Taliban regime of Afghanistan and notes that the regime is controlling parts of Afghanistan and allowing those parts to be used as bases of operation, as well as that the regime refused to change its policy.[299] In other words, the United States relied not only on the terrorist attacks perpetrated by Al-Qaeda as the basis for self-defence but also on the acts of the Taliban regime which at the time *de facto* governed parts of Afghanistan. That said, the majority of the group behind the Tallinn Manual agreed that state practice established a right of self-defence also in response to attacks by non-state actors and groups but recognized the 'significant uncertainty' as to for example the degree of organization such a group must have.[300]

5.3.2 Level of Control for State Responsibility

For a state to be responsible for the acts of non-state actors, it has to have a certain level of control over the acts. In *Nicaragua*, the ICJ formulated the so-called 'effective control' test: for a state to be responsible, it had to be proved that the state had effective control of the acts.[301] The Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia (ICTY) took a different view on the level of control required for acts to attributable to a state in the *Tadić* case. The Chamber did not 'hold the *Nicaragua* test to be persuasive' for two reasons: it was considered to be inconsistent with the logic of the law of state responsibility and to be inconsistent with judicial and state practice.[302] Instead, the ICTY applied an 'overall control' test, which is less strict than the one used by the ICJ. According to the Chamber, it is sufficient for the attribution of acts to the state that the group as a whole is under the overall control of the state.[303] This means that in the case of militias or paramilitary units the state did not have to issue specific orders or direct each individual operation for the acts to be attributable to the state. A role in organising, coordinating or planning the military actions sufficed, in addition to financing, training,

299 Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council. UN Doc. S/2001/946.
300 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 59.
301 *Nicaragua*, *supra* note 114 at para. 115.
302 *Prosecutor v. Tadić*, Case no. IT-94-1-A, ICTY Appeals Chamber, Judgment (15 July 1999) at paras 115–145.
303 *Tadić*, *supra* note 302 at paras. 120, 145.

equipping and providing operational support. With less organized groups or individuals the threshold is higher.[304]

The International Court of Justice considered the different standards in the *Genocide* case. The Court stated that in determining whether an armed conflict was international, the overall control test put forth by the ICTY might well be applicable and suitable. The ICJ however disagreed with the ICTY on whether or not it was applicable in determining whether a state was responsible for acts committed by non-state actors. The ICJ noted that different tests may be applied in resolving the issues without logical inconsistency. In the view of the ICJ, using the overall control test in issues of state responsibility broadens the scope too much and stretches the connection between the organs of the state and the responsibility of the state too far.[305] Nevertheless, while there is disagreement as to the level of control needed to incur the responsibility of the state, the Courts agreed that it is indeed possible for the acts of non-state actors to be attributed to a state.

Self-defence against non-state actors might also be available in situations where a state is unable to prevent its territory to be used in preparation or carrying out terrorist attacks.[306] This widens the possibilities of responding to terrorist attacks by self-defence considerably. It should be reminded that also these acts of self-defence are subject to the requirements of necessity and proportionality, so even a relatively wide interpretation of whose acts can be countered with self-defence does not provide a *carte blanche* for the use of force. The Tallinn Manual adopted a similar view regarding cyber operations and noted that if a state is unable or unwilling to take actions to repress the attack, self-defence is permissible. Interestingly, the Manual noted that the inability might stem from the lack of expertise or technology.[307] It should be reminded, though, that in all such questions the requirement of necessity would arguably not allow for self-defence if the attack could also be deterred by providing technical assistance to the state in question.

To summarize the issue of acts of irregular forces, it is possible for acts of non-state actors to qualify as armed attacks if they are attributable to a state or if the state knowingly allows

304 *Tadić*, *supra* note 302 at para. 137.
305 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I. C. J. Reports 2007, p. 43 at paras 404–406.
306 Randelzhofer, *Article 51*, *supra* note 140 at 802.
307 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 60–61.

for its territory to be used for terrorist activity or is unable to prevent such activity. The responsibility of a state lies, as Michael Schmitt writes, on a continuum.[308] And as the ICTY stated in *Tadić*, the extent of the control varies.[309] The problem of attribution regarding cyber operations is twofold: firstly, it is possible to cover the original source of the operation so that it is difficult if not impossible to quickly determine the origin at all. Secondly, it is possible to fake the source of the operation so that it appears at least *prima facie* to originate from a different source. And even in cases where the true origin can be determined, it might take a considerable amount of time to reverse-engineer or otherwise decipher the attack sufficiently to reveal the origin. It should also be kept in mind that in some cases it may well be in the interests of the attacker to make it known who was behind the attack. And in cases where cyber attacks are carried out in tandem with other actions it might even be obvious.

5.4 Cyber Operations as Armed Attacks?

The Tallinn Manual adopts the position that uses of force that injure or kill persons or damage or destroy property do satisfy the scale and effects requirement derived from the *Nicaragua* judgment and thus qualify as armed attacks.[310] Conversely, cyber espionage and operations that merely cause brief or periodic interruption of non-essential services do not count. Such a view is well justified, and indeed there seems to be a consensus that at least attacks that have resulted in lethal results or significant property damage may constitute an armed attack.[311] As with traditional armed attacks, the exact point of the threshold of an armed attack is however unclear.[312] In *Nicaragua*, the International Court of Justice distinguished between mere frontier incidents and armed attacks,[313] and in *Oil Platforms* did not exclude the possibility of the mining of a single military ship constituting an armed attack.[314] It would thus seem that the operation does not have to be widespread for it to cross the threshold of an armed attack. For example a cyber attack causing death, injury, damage or destruction on a single target could thus constitute an armed attack.

---

308 Schmitt, *Cyber Operations and the Jus ad Bellum Revisited*, *supra* note 171 at 577.
309 *Tadić*, *supra* note 302 at para. 137.
310 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 55.
311 Dinniss, *Cyber Warfare and the Laws of War*, *supra* note 165 at 81. Also, Dinstein, *Computer Network Attacks and Self-Defense*, *supra* note 57 at 100.
312 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 56.
313 *Nicaragua, supra* note 114 at para. 195.
314 *Oil Platforms*, *supra* note 227 at para. 72.

As is the case with the notion of force and cyber operations, some have argued for setting the threshold much lower, and have for example analogized denial-of-service attacks with naval blockades and claimed that as such they can qualify as armed attacks.[315] While such an analogy is an interesting one, it lacks support and compelling justification and is weakened by a number of issues. The reasoning goes that blocking access to communications networks can be likened to blocking access to sea or to airspace. One problem has to do with the technical nature of the denial-of-service attacks: they are usually directed at certain specific sites – in the case of Estonia, mostly governmental websites and banking websites.[316] These kinds of attacks only affect the sites in question, and perhaps sites hosted on the same servers.[317] If the viewpoint in the case of a naval blockade is that of those behind the blockade, that is, those unable to access the sea at all, the situation is not a comparable to someone being unable to access only a certain website but being able to access all others.

The analogy of a naval blockade would seem more reasonable in cases where the the users could not access any websites at all because of the attack. During the Estonian incident some attacks on the domain name servers (or DNS servers) succeeded in temporarily disrupting the DNS services around the country,[318] which could effectively block the users of the affected server from accessing any website.[319] Also Article 41 of the UN Charter may be recalled here. The Article states that the Security Council may decide what measures not involving the use of force are to be employed and notes that such measures may include complete or partial interruption of for example communications means. Taking account the consequences and the nature of denial-of-service attacks, it is more reasonable to analogize them with the disruption of communications not amounting to a use of force referred to in Article 41 of the Charter than the blockade mentioned in Article

315 See e.g. Sheng Li, 'When Does Internet Denial Trigger the Right of Armed Self-Defense', 38 *Yale Journal of International Law* (2013) 179–216 at 191, 200.

316 Tikk *et al.*, *International Cyber Incidents, supra* note 60 at 22.

317 A hypothetical example: if the website of the Faculty of Law of the University of Helsinki is a target of a denial-of-service attack, the users might (depending on the hosting arrangements) also be unable to access the website of the Faculty of Medicine. The attack would not, however, block the user from accessing any other websites.

318 Tikk *et al.*, *International Cyber Incidents, supra* note 60 at 21.

319 If the DNS servers are unable to respond, the attack would effectively prevent the client computer from knowing where it should connect to. It is also worth noting that changing to another DNS server would bypass the effect of such attacks. While such a change is not necessarily a feasible alternative for a common user, it is technically a trivial task that can be done in less than a minute.

42. It thus seems highly unlikely that a denial-of-service attack could ever constitute an armed attack, even in cases of extensive attack as in Estonia in 2007, without a significant change in the whole notion of an armed attack. It is doubtful that such attacks could constitute force either, unless the notion of force evolves so that the economic damage would be enough to cross the threshold.

Because a cyber attack might be effectively carried out in fractions of a second, some have mentioned the idea of automatic self-defence.[320] Such a concept has several problems, one of which is the identification of the attacker. As discussed earlier, the true origin of the attack may be masked and the *prima facie* source of the attack might turn out to be merely a conduit. Attacking such a target does nothing to cease the attack even if it were still on-going[321] and it would highly likely be unlawful as well.[322] Another, arguably the most important issue is that of correctly identifying attacks that warrant a response. Wrongly interpreted signals of attacks incur the risk of escalation,[323] and the risk is especially pertinent to cyber attacks because of the speed with which the attacks and responses may be carried out. It should be reminded, though, that active defence may also very well be cautiously used in a manner that neither risks escalation nor presents problems with the *jus ad bellum*.

Some members of the group behind the Tallinn Manual argued for a view that would put more weight on the severity of the consequences of a cyber attack and not only on the physical consequences. An example of an attack with severe but not physical consequences would be one against a stock exchange.[324] While the economic consequences of such an attack could indeed be catastrophic and thus might even warrant a reappraisal of the question of economic force, there seems to be no support for such view *de lege lata.* The

320 See e.g. Dinstein, *Computer Network Attacks and Self-Defense*, *supra* note 57 at 106. Dinstein also recognizes the difficulties with such an approach.
321 The attack traffic could merely end up taking another route. *Supra* at 19.
322 Dinstein, *Computer Network Attacks and Self-Defense*, *supra* note 57 at 107.
323 For examples of dangers caused by false alarms see Jeffery L. Caton, 'Exploring the Prudent Limits of Automated Cyber Attack' in K. Podins, J. Stinissen, M. Maybaum (eds), *2013 5th International Conference on Cyber Conflict Proceedings* (NATO CCD COE Publications: Tallinn, 2013), 145–160 at 149–152.
324 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 56–57 and Michael N. Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed', 54 *Harvard International Law Journal Online* (2012) at 22. The issue was also discussed in the context of the notion of force, *supra* at 42.

other members of the Tallinn Manual group took a similar position and accepted the possibility of the interpretation developing to such an approach in the future.[325]

As regards self-defence, the requirement of necessity may be a somewhat problematic one regarding computer network attacks. Data travels through the networks at ever increasing speeds, and the attack may be carried out in a very short period of time. A strict interpretation of the necessity requirement would thus make it in practice very difficult if not completely impossible to resort to self-defence in response to cyber attacks, as the attack could already be over when it is discovered. An example of a prolonged cyber attack would be a denial-of-service attack, but as it generally does not constitute a use of force, much less an armed attack, it is not significant in this context. Yoram Dinstein argues that the victim state must be given a 'reasonable window to respond'. He also argues that the recourse to self-defence may be lawful even when the interval between the initial attack and the response 'is longer than usual', if the delay is exculpated by circumstances.[326] Following such reasoning, the delay caused by determining the attacker could indeed count as an exculpatory circumstance. That said, unless there was a threat of further attacks, the response would arguably still be vulnerable to criticism of being retaliatory. The possibility of self-defence based on the threat of further attacks will be more closely examined in chapter 5.5.2.

5.5 Anticipatory Self-Defence

5.5.1 Possibility of Anticipatory Self-Defence

The text of Article 51 of the UN Charter articulates a right to self-defence 'if an armed attack occurs'. The Article has been interpreted in varying ways regarding whether or not the Article only applies in situations where an armed attack has already taken place or whether it allows for anticipatory self-defence as well. The scholarly interpretations of Article 51 can with some simplification be divided to four categories:[327] the first group rejects the legality of anticipatory self-defence.[328] The second allows for self-defence in cases of incipient attacks or already launched attacks which have not yet reached their

325 Schmitt, *International Law in Cyberspace*, *supra* note 324 at 22.
326 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 267.
327 T. D. Gill, 'The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy', 11 *Journal of Conflict & Security Law* (2006) 361–369 at 367.
328 See e.g. Brownlie, *International Law and the Use of Force by States*, *supra* note 97 at 278.

target (this has been referred to as interceptive self-defence by Yoram Dinstein).[329] The third group sees the Article as allowing for self-defence in the cases of an immediate threat of an attack which has not yet been launched. And the fourth one argues that anticipatory self-defence is allowed also in cases where there is a more indeterminate possibility of an attack in the future. No clear consensus on the issue exists, and another question is whether or not the right to self-defence based on customary international law is in this sense wider and allows for anticipatory action. Anthony Clark Arend and Robert J. Beck argue that there is a general agreement that the pre-Charter customary international law included a right to anticipatory self-defence subject to the requirements of necessity and proportionality derived from the *Caroline* incident.[330] Albrecht Randelzhofer considers the view that excludes the possibility of any self-defence other than that based on Article 51 in response to an armed attack to be the prevailing one, but it should be noted, that he sees the opposing view as a very wide one and as including not just anticipatory self-defence but for example the forceful protection of economic interests in a foreign country.[331]

While a strict textual reading of Article 51 certainly makes it possible to claim that it does not allow for any kind of anticipatory self-defence, it seems counterintuitive to claim the Charter requires states to patiently wait for an attack to occur before they can act, in worst cases effectively making it a suicide pact. Article 2(4) prohibits states from using force, but the ban is not without exceptions. The United Nations strives, according to the Preamble of the Charter to ensure 'that armed force shall not be used, save in the common interest'. In other words, it is certainly accepted that in certain cases the use of force is necessary, even though the ultimate goal is to achieve peace. Such a concept is inherently tensional, and as Martti Koskenniemi and others note, it is at the same time impossible and necessary to accept the doctrine of pre-emptive self-defence as a part of the international legal system.[332]

Using a strict textual interpretation of Article 51 as a basis for dismissing any possibility of anticipatory self-defence also seems to overlook the fact that the collective security system

329 See e.g. Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 203–205.
330 Anthony Clark Arend and Robert J. Beck, *International Law and the Use of Force – Beyond the UN Charter Paradigm* (Routledge: London 1993) at 72.
331 Randelzhofer, *Article 51*, *supra* note 140 at 792–793.
332 Martti Koskenniemi, 'Oikeus ja asevoiman käyttö uudessa maailmassa', *Lakimies* 1/2003 90–95 at 95. For a similar argument regarding humanitarian intervention and an overview of scholars sharing the same view see Koskenniemi, '*The Lady Doth Protest Too Much'*, *supra* note 183 at 162.

envisaged in the Charter never turned out the way it was intended. While the issue more closely relates to the debate about the existence of a gap between the thresholds of force and armed attack,[333] it is still noteworthy that the Security Council has in practice been less able to react to threats to peace than originally planned. The most obvious example of this is probably that of Kosovo.

The possibility of anticipatory self-defence has been criticized on the basis that because there is usually no objective criteria to assess the imminence of an attack, the decision would be left to the discretion of the state.[334] While the argument is not without merit, a restrictive view of Article 51 still would leave open the question of what constitutes an armed attack and similarly leave much to the discretion of the state. As the cases before the International Court of Justice, the scholarly debate and the differing interpretations by states has shown, no explicit objective criteria by which to assess the acts exists. And even if such criteria were to exist, it would inevitably face the problems of over- and under-inclusiveness already mentioned regarding the notion of force.[335]

The International Court of Justice noted the question of self-defence in response to an imminent threat of an armed attack in *Nicaragua*, but did not express a view on the issue since neither party invoked it.[336] The uncertain status of pre-emptive self-defence is also reflected in state practice: states generally prefer to interpret the notion of an armed attack expansively and justify self-defence on that basis rather than invoke the right to anticipatory self-defence.[337] The disagreement of states has also prevented the inclusion of any detailed provisions in the General Assembly resolutions touching upon the issue of self-defence, such as the Friendly Relations Declaration and the Definition of Aggression.[338]

While more than 170 years have passed since the *Caroline* plunged down the Niagara Falls in flames and Daniel Webster wrote the famous letter in which he formulated the prerequisites for lawful anticipatory self-defence, they still remain useful. As Oscar Schachter writes, the formulation of Webster meets the idea of opposing the pre-emptive

333 Discussed *supra* at 55.
334 Randelzhofer, *Article 51*, *supra* note 140 at 803.
335 *Supra* at 37.
336 *Nicaragua*, *supra* note 114 at para. 194.
337 Gray, *International Law and the Use of Force*, *supra* note 214 at 161.
338 Gray, *International Law and the Use of Force*, *supra* note 214 at 160.

resort to force but acknowledges its necessity in cases where the attack is of such nature that it would be absurd to demand for the targeted state to wait before defending itself.[339] There are contrary views as well, and for example Myres McDougal and Florentino Feliciano see the formulation to be 'so abstractly restrictive as almost, if read literally, to impose paralysis'.[340] Abraham Sofaer argues that the language should not be applied as a general rule for all pre-emptive actions and that the standard applicable to pre-emptive self-defence is the same that applies to all uses of force.[341]

A 2004 report by a UN High-Level Panel on Threats, Challenges and Change stated that according to 'long established international law', a state can take military action as long as the threatened attack is 'imminent, no other means would deflect it and the action is proportionate'.[342] The report does not refer to Article 51, whereas a 2005 report of the Secretary-General states that 'imminent threats are fully covered by Article 51'.[343]

5.5.2 Anticipatory Self-Defence and Cyber Attacks

Cyber operations pose some challenges for the doctrine of anticipatory self-defence. Some of these, such as the question of the level of certainty and proof needed, are shared with kinetic attacks, but in addition to these, there are issues specific to cyber operations. It can, for example, be difficult to determine whether an intrusion into a system or a network is merely espionage or the first stage of a destructive attack. In fact, during the early stages of their analysis, security researchers believed Stuxnet to be another tool for industrial espionage,[344] and in other cases software errors have caused consequences which could be interpreted as resulting from a cyber attack.[345] A strict interpretation of the temporal limits of self-defence would practically render it impossible to respond to cyber attacks in self-defence. The attack might be prepared in secrecy and there might not be any external

339 Oscar Schachter, 'In Defense of International Rules on the Use of Force', 53 *University of Chicago Law Review* (1986) 113–146 at 136.
340 Myres S. McDougal and Florentino P. Feliciano, *Law and Minimum World Public Order* (Yale University Press: New Haven, 1961) at 217.
341 Abraham D. Sofaer, 'On the Necessity of Pre-emption', 14 *European Journal of International Law* (2003) 209–226 at 220.
342 Report of the High-Level Panel on Threats, Challenges and Change. UN Doc. A/59/565 at para. 188.
343 In Larger Freedom: Towards Development, Security and Human Rights for All, Report of the Secretary-General. UN Doc. A/59/2005 at para. 124.
344 Zetter, *How Digital Detectives Deciphered Stuxnet*, *supra* note 69.
345 Lawrence T. Greenberg, Seymour E. Hoffman and Kevin J. Soo Hoo, *Information Warfare and International Law* (National Defense University: Washington, D.C. 1998) at 21–22.

pointers of an impending attack as in the case of a traditional kinetic attack, such as gathering of troops near a border or strengthening a fleet at sea.[346] And the attack itself might only take fractions of a second to carry out, and the physical consequences might or might or might not be instantaneous. Either the acts of self-defence would be anticipatory or carried out after the attack has already taken place. The majority of the group behind the Tallinn Manual took the view that even though Article 51 does not explicitly allow for anticipatory self-defence, a state need not wait in cases where a cyber attack rising to the level of an armed attack is 'imminent'.[347]

The Tallinn Manual correctly distinguishes between the insertion of a logic bomb and the placement of a remotely activated malware. A logic bomb refers to a piece of software that will execute the attack based on some predetermined factors without a further external command, as distinct from a malware that requires an external command for the attack to commence. The Manual analogizes the situation with the laying of naval mines in shipping lanes and takes the position that the insertion of a logic bomb qualifies as an armed attack if the conditions for activation 'are likely to occur'. A mere placement of the malware to the targeted computer or a network does not, however, meet the criterion of imminence. Such is the case also with the placement of a backdoor – that is, a piece of software allowing unauthorized access to a system. This does not yet imply an imminent attack and thus does not in and of itself justify self-defence.[348] Self-defence becomes justified when the attacker has decided to launch the attack and the target state faces a situation where postponing the defensive act would deprive it from effectively defending itself.[349] Such a view is justified and in line with position of the aforementioned UN High-Level Panel on Threats, Challenges and Change. The problem, of course, is recognizing and differentiating between the situations in practice.

As regards the requirement of immediacy and the question whether or not states can act in self-defence after the cyber attack has concluded, the Tallinn Manual takes the position that states may act in self-defence after the attack has ceased if it is reasonable to conclude that such attacks are likely to follow. In these cases, the Manual presents, the state may treat the

346 Dinniss, *Cyber Warfare and the Laws of War*, *supra* note 165 at 90.
347 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 63.
348 Dinniss, *Cyber Warfare and the Laws of War*, *supra* note 165 at 90.
349 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 65.

attacks as a 'cyber campaign'.[350] Without such a conclusion, the self-defence may be seen as retaliatory. The Manual speaks of a cyber campaign, but it should also be noted that the attacks likely to follow may also be other than cyber attacks. In fact, as cyber attacks can be used as a first phase of a wider attack to prepare the battlefield, the following attacks may very well be other than cyber operations. An attacking state might, for example, first aim to disable or disturb the military communications networks of the target state by a cyber attack and then launch a kinetic attack.[351] If such an attack were imminent, the victim state could legally act in self-defence.

It may also be the case that the fact that a cyber attack has occurred only becomes apparent after a longer period of time. The Tallinn Manual uses the Stuxnet incident as an example of such an attack and argues that the criterion of immediacy is not met in such cases, and that self-defence is only possible in cases where further attacks are imminent.[352] While it is true that the consequences of a cyber attack may well become known only after some time has passed or that it may only be discovered later on that some previously apparent consequences were indeed the result of a cyber attack, it is doubtful that such attacks would in most cases qualify as armed attacks anyway due to their consequences probably being less severe. There might of course also be attacks attacks whose consequences are instantaneously evident and sufficiently grave but whose perpetrator is only identified later on. While the 2007 attacks on Estonia do not qualify as armed attacks, they are a fitting example of the problems of ascertaining who is behind the attacks. The Tallinn Manual takes the position that self-defence in such cases too is only possible if further attacks are imminent.[353] As mentioned earlier, Yoram Dinstein argues that the circumstances of the attack may justify a longer period of time between the initial attack and the response,[354] and the investigation of a cyber attack could well count as such circumstances.

350 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 66.
351 Dinniss, *Cyber Warfare and the Laws of War*, *supra* note 165 at 82.
352 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 66.
353 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 66.
354 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 267.

5.6 Conclusions About Self-Defence

The notion of self-defence remains controversial. No clear rules exist as to when states may act in self-defence, and neither is there any clear rules on which kinds of acts are justified in terms of their proportionality. The International Court of Justice, scholars and states have varying interpretations of the UN Charter and the customary international law rules, and in fact, also of the very relationship between the Charter and customary international law. And no exact rules even could exist. Ultimately, the question is of a case-by-case analysis. The distinction between uses of force and armed attacks continues to divide opinions, but the prevailing view is that they indeed are different and, as the International Court of Justice stated in *Nicaragua*, only the most grave forms of the use of force constitute an armed attack.[355]

Just as a cyber operation may constitute a use of force, it may also rise to the level of an armed attack. Such attacks are exceptional, and as the Tallinn Manual notes, no attacks have as of 2012 been unambiguously characterized by the international community as armed attacks. Some members of the group behind the Manual did, however, argue that Stuxnet in fact reached the level of an armed attack.[356] Assuming that the public reports of the consequences caused by Stuxnet are true, classifying the operation as an armed attack would lower the threshold quite far. It seems indisputable that Stuxnet caused physical damage: subsequent analysis showed that the malware tampered with the frequencies of the rotors in a way that could cause damage and at the same time an unusual number of centrifuges had to be replaced at Natanz.[357] That said, the damage was somewhat limited, and it would seem that the operation did constitute a use of force but that the consequences remained below the threshold of an armed attack. More severe physical damage, injury or death would, on the other hand, been enough to qualify the operation as an armed attack.

Because of the nature of cyber attacks, especially the possibly very short duration of the active phase of an attack, responses are practically limited to those used after the initial attack. Such acts are prone to criticism of being retaliatory in nature if the requirement of necessity is interpreted strictly. Dinstein however argues that the lapse of time between the

355 *Nicaragua*, *supra* note 114 at para. 191.
356 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 57–58.
357 For a closer look at Stuxnet, see *supra* at 14.

initial attack and the response does not by itself give the response a punitive character.[358] He also suggests that circumstances may justify a longer period between the initial attack and the response.[359] And as discussed with regard to pre-emptive self-defence, a response is also justified if there is a threat of the attacks continuing. In any case, it should be kept in mind that the responses are also subject to the requirement of proportionality.

358 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 251–252.
359 Dinstein, *War, Aggression and Self-Defence*, *supra* note 41 at 267.

6 Principle of Non-Intervention and Countermeasures

6.1 Principle of Non-Intervention

As discussed in the previous chapters, for an operation to be qualified as a of use of force or as an armed attack, it has to reach a certain level of gravity. There is, however, a plethora of actions that may not cross the threshold of the use of force, let alone an armed attack, but are still questionable in terms of their legality in light of international law. Such acts may for example be used to erode trust in institutions such as governments and companies,[360] and they may be breaches of the principle of non-intervention and may justify countermeasures as a response. This chapter takes a brief look at the principle and countermeasures as well as acts of retorsion in the context of cyber operations. Also the issue of criminal jurisdiction will be briefly mentioned.

The International Court of Justice stated in *Nicaragua* that the principle of non-intervention, the right of every sovereign state to conduct its affairs without outside interference, is part and parcel of customary international law.[361] The principle has also been stated in UN General Assembly Resolutions, such as the Friendly Relations Declaration[362] and the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty.[363] The UN Charter does not explicitly refer to the principle of non-intervention, yet it may be seen as being included in several of the Charter provisions referencing the sovereignty of states.[364] The principle has also been included or referenced in several other treaties.[365]

As formulated in the Friendly Relations Declaration, the principle of non-intervention indicates that no state has the right to intervene in the internal or external affairs of another state. Consequently, the Declaration continues, armed intervention and all other forms of

360 Rid, *Cyber War Will Not Take Place*, *supra* note 53 at 26.
361 *Nicaragua*, *supra* note 114 at para. 202.
362 Friendly Relations Declaration, *supra* note 115.
363 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, GA Res. 2131 (XX), 21 December 1965.
364 Terry D. Gill, 'Non-Intervention in the Cyber Context' in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy* (NATO CCD COE Publications: Tallinn, 2013), 217–238 at 220.
365 For an overview, see Maziar Jamnejad and Michael Wood, 'The Principle of Non-intervention', 22 *Leiden Journal of International Law* (2009) 345–381 at 362–367.

interference or attempted threats against the personality of the state or political, economic and cultural elements of the state are in violation of international law. The Declaration also notes that no state may use or encourage the use of economic, political or any other type of measures to coerce another state, and that no state shall *inter alia* organize, assist, finance or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another state, or interfere in civil strife in another state. While the formulation is somewhat ambiguous, the core meaning of an intervention is fairly clear.[366] There is a close relationship between the notions of intervention and the use of force, and the two are partly overlapping.[367] A threat or use of force constitutes an intervention,[368] but the notion of intervention also includes lesser acts of coercive nature that fall under the threshold of the use of force, and those are of interest in the present chapter.

6.2 Countermeasures

6.2.1 Right to Countermeasures

States who have been subjected to an intervention by another state under the threshold of an armed attack may respond by countermeasures and acts of retorsion. In cases of attacks by individuals or groups whose conduct is not attributable to a state, the state may exercise national criminal jurisdiction. All of these may be useful depending on the situation, yet they share a variety of potential problems, not least of which being the effectiveness of each of them.[369] According to the commentary of the International Law Commission on the Draft Articles on State Responsibility, countermeasures are 'measures that would otherwise be contrary to the international obligations of an injured state *vis-à-vis* the responsible State' which are carried out as a response to an internationally wrongful conduct.[370] Article 2 of the Draft Articles states that an internationally wrongful act consists of two elements: the act is attributable to the state under international law and it constitutes a breach of an international obligation of the state. The breach may relate to treaty-based obligations of a state or those stemming from customary international law.[371] Also an omission may constitute an internationally wrongful act.

366 Gill, *Non-Intervention in the Cyber Context*, *supra* note 364 at 222.
367 Jamnejad and Wood, *The Principle of Non-intervention*, *supra* note 365 at 348.
368 Gill, *Non-Intervention in the Cyber Context*, *supra* note 364 at 221.
369 Gill, *Non-Intervention in the Cyber Context*, *supra* note 364 at 228, 231.
370 Report of the ILC, Fifty-third Session, *supra* note 99 at 324–325.
371 Report of the ILC, Fifty-third Session, *supra* note 99 at 71.

The ILC commentary to the Draft Articles on State Responsibility acknowledges the previous usage of the term reprisal, but notes that it is no longer widely used in the context of countermeasures due to the association with belligerent reprisals in the context of international humanitarian law.[372] The notion of reprisals also was wider than that of countermeasures as it included both forceful and non-forceful acts[373] as well as acts that were punitive in character.[374] Traditional examples of countermeasures include *inter alia* the freezing of assets of a state and the suspension of a trade agreement.[375] According to the prevailing view, countermeasures must be non-forceful, and the Friendly Relations Declaration clearly notes that states have a duty to refrain from acts of reprisal involving the use of force.[376] In the *Nuclear Weapons* Advisory Opinion the International Court of Justice took the same position and stated that armed reprisals in the time of peace are considered unlawful.[377] According to Article 50 of the Draft Articles on State Responsibility, countermeasures shall not affect the obligation to refrain from the threat or use of force as embodied in the UN Charter. As the Charter only allows the use of force in self-defence or with the authorization of the Security Council, it thus effectively outlawed armed reprisals.[378] The ILC commentary on the Draft Articles describes the limitation as a fundamental substantive obligation and notes that the prohibition is consistent with the prevailing doctrine and refers to the Friendly Relations Declaration as well as judgments of the International Court of Justice and UN Security Council Resolutions.[379]

As the other element of an internationally wrongful act is the attributability of the act to a state, the question of attribution is as relevant to countermeasures as it is to self-defence and it involves the same kind of problems.[380] The ILC commentary on the Draft Articles

372 Report of the ILC, Fifty-third Session, *supra* note 99 at 181.
373 Michael N. Schmitt, 'Cyber Activities and the Law of Countermeasures' in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy* (NATO CCD COE Publications: Tallinn, 2013), 659–690 at 662.
374 Derek W. Bowett, 'Reprisals Involving Recourse to Armed Force', 66 *The American Journal of International Law* (1972) 1–36 at 3.
375 Report of the ILC, Fifty-third Session, *supra* note 99 at 331.
376 Nigel White and Ademola Abass, 'Countermeasures and Sanctions' in Malcolm D. Evans (ed.), *International Law* (3rd Edition, Oxford University Press, 2010), 531–558 at 532.
377 *Nuclear Weapons*, supra note 29 at para. 46.
378 Brownlie, *International Law and the Use of Force by States*, *supra* note 97 at 281. Also McCoubrey and White, *International Law and Armed Conflict, supra* note 111 at 111–112.
379 Report of the ILC, Fifty-third Session, *supra* note 99 at 333–334.
380 Robin Geiß and Henning Lahmann, 'Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention' in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy* (NATO CCD COE Publications: Tallinn, 2013), 621–657 at 634.

recognizes the difficulty in determining when a wrongful act is sufficiently attributable to a state.[381] The ILC quotes the Iran-United States Claims Tribunal and states that it is necessary to identify *with reasonable certainty* the actors and their association with the state.[382] This, again, is especially relevant to cyber operations. As discussed, the true origin of cyber operations may well be masked so as to lead the victim state to believe that the attacker is someone else.[383] The true origin of the attack might be revealed by subsequent, more time-consuming analysis, but this might happen much later than the operation actually took place.[384] Reasonable certainty is, of course, a rather ambiguous level of certitude and no clear rules for what kind of evidence is enough to fulfil the requirement cannot be set forth. The question is one to be dealt with on a case-by-case basis.

As the previously discussed aspects of international law, also the law of state responsibility applies to cyber operations of states as well.[385] In other words, if the conditions are met, states may respond to cyber attacks conducted on them as well as use cyber operations as countermeasures themselves. This view was also adopted in the Tallinn Manual.[386] Countermeasures have been a relatively rare occurrence, especially since the end of the Cold War. The legal uncertainty and the strict limitations of countermeasures combined with the fact that states seem to steer clear of invoking the right to take countermeasures when reacting to less grave uses of force suggests that the role of countermeasures will remain less significant in the future as well. This is also the case with cyber countermeasures too.[387]

Sanctions imposed on states by the Security Council on the basis of Chapter VII of the Charter may be similar to countermeasures, but they should be distinguished from them due to the different legal basis. Sanctions imposed by the Security Council derive their lawfulness from the Charter and the decisions of the Security Council.[388]

---

381 Report of the ILC, Fifty-third Session, *supra* note 99 at 91.
382 Report of the ILC, Fifty-third Session, *supra* note 99 at 83–84.
383 *Supra* at 19.
384 The better known variant of Stuxnet, for example, was presumably launched in the summer of 2009 and first discovered in June 2010. It was not until the fall of 2010 that it became clear that the targets were Iranian centrifuges. Langner, *To Kill a Centrifuge*, *supra* note 70 at 10, Zetter, *How Digital Detectives Deciphered Stuxnet*, *supra* note 69 and *supra* at 14.
385 Schmitt, *Cyber Activities and the Law of Countermeasures*, *supra* note 373 at 661. Also, Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 29–31.
386 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 36–37.
387 Gill, *Non-Intervention in the Cyber Context*, *supra* note 364 at 233.
388 Schmitt, *Cyber Activities and the Law of Countermeasures*, *supra* note 373 at 663.

6.2.2 Restrictions on Countermeasures

Countermeasures are subject to strict limitations. According to Article 49 of the Draft Articles on State Responsibility an injured state may only take countermeasures against a state which is responsible for an internationally wrongful act in order to induce that state to comply with its obligations. It thus follows that no countermeasures can be taken if the original wrongful act has already ceased. This is also expressly stated in Article 52(3)(a). In other words, countermeasures may only be used in order to restore a state of lawfulness and not for retaliation or punishment,[389] nor in situations where the wrongful act has already been committed and there is no threat of it being repeated.[390] In the context of cyber operations, this poses similar challenges than the temporal limitation of self-defence:[391] the attack may be over in a matter of seconds, after which the countermeasures could easily be seen as retaliatory and thus contrary to Article 49 of the Draft Articles. As the Tallinn Manual notes, however, states have sometimes appeared to carry out countermeasures punitively, which according to the Manual makes it uncertain whether or not the ILC commentary reflects customary international law.[392]

Even though the prevailing view is that countermeasures must be non-forceful, the debate about the possibility of forceful countermeasures continues. It has for example been suggested that there may be an emerging customary international law doctrine allowing forceful countermeasures in the context of humanitarian intervention[393] and the fight against terrorism.[394] Derek Bowett claimed in 1972 – that is, after the Friendly Relations Declaration but before the Draft Articles on State Responsiblity – that due to the practice of states, there existed a credibility gap and because of the separation from actual practice the law on reprisals was degenerating. Bowett argues that the total outlawing of armed reprisals presupposed 'a capacity for collective action to suppress any resort to unlawful force' which had not been achieved, which in turn led states to resort to self-help.[395]

---

389 Report of the ILC, Fifty-third Session, *supra* note 99 at 331.
390 Schmitt, *Cyber Activities and the Law of Countermeasures*, *supra* note 373 at 674–675.
391 *Supra* at 68.
392 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 37.
393 Antonio Cassese, 'Ex iniuria ius oritur: Are We Mving Towards International Legitimation of Forceible Humanitarian Countermeasures in the World Community?', 10 *European Journal of International Law* (1999) 23–30 at 27.
394 Michael J. Kelly, 'Time Warp to 1945 – Resurrection of the Reprisal and Anticipatory Self-Defense Doctrines in International Law', 13 *Journal of Transnational Law and Policy* (2003) 1–39 at 19–22.
395 Bowett, *Reprisals Involving Recourse to Armed Force*, *supra* note 374 at 1–2.

Closely related to this issue is the debate about the separation of the notions of force and armed attack.[396] Some have argued that no gap exists between the two, which leads to the conclusion that states have the right to act in self-defence in all cases where force is used against them, not just in the most grave forms of the use of force.[397] The position taken by Judge Simma should also be recalled here: in a separate opinion to the *Oil Platforms* decision, Simma suggests that the permissibility of 'strictly defensive military action' taken against attacks that do not cross the threshold of an armed attack cannot be denied. He suggests a distinction between full-scale self-defence (based on Article 51 of the UN Charter) and lesser, proportionate defensive measures.[398] Simma refers to the *Nicaragua* judgment, where the Court noted that if the acts in question were imputable to Nicaragua, they could only have justified 'proportionate counter-measures' by the victim states and not by third states, 'and particularly could not justify intervention involving the use of force'.[399] According to Simma, considering the context the Court cannot have meant 'mere pacific reprisals'. The responses to less grave forms of attacks would be subject to requirements of necessity, proportionality and immediacy in a particularly strict way.[400] There is, however, a lack of state practice and *opinio juris* supporting the view as states generally have justified their actions as self-defence – even when it has meant, in the words of Thomas Franck, resorting to creative fictions[401] – and rejected the notion of armed reprisals.[402]

6.2.3 Proportionality and Necessity of Countermeasures

According to Article 51 of the Draft Articles, countermeasures must be commensurate with the injury suffered, taking into account the gravity of the wrongful act and the rights in question. Countermeasures are thus subject to a requirement of proportionality, but as Michael Schmitt points out, the proportionality of countermeasures is different from the notion of proportionality regarding self-defence.[403] The proportionality of self-defence is

396 Discussed in more detail *supra* at 54.
397 See e.g. Taft, *Self-Defense and the Oil Platforms Decision*, *supra* note 267 at 300–301 and Gazzini, *Changing Rules on the Use of Force in International Law*, *supra* note 213 at 138.
398 *Oil Platforms*, *supra* note 227, Separate Opinion of Judge Simma at para. 12
399 *Nicaragua*, *supra* note 114 at para. 249.
400 *Oil Platforms*, *supra* note 227, Separate Opinion of Judge Simma at paras 12–13
401 Franck, *Recourse to Force*, *supra* note 273 at 112.
402 Gazzini, *The Changing Rules on the Rules of Force in International Law, supra* note 213 at 169. For somewhat older examples of such claims see McCoubrey and White, *International Law and Armed Conflict, supra* note 111 at 114–115.
403 Schmitt, *Cyber Activities and the Law of Countermeasures*, *supra* note 373 at 682–683.

measured against the level needed to repel the attack and may thus be of different gravity than the original attack. The proportionality of countermeasures, however, stems from harm suffered by the victim state. The ILC commentary on the Draft Articles notes that reciprocal countermeasures – that is, countermeasures which involve the suspension of a similar obligation to the one violated by the responsible state – are more likely to be considered necessary and proportionate.[404]

Countermeasures are also subject to a requirement of necessity. Article 52(1) of the Draft Articles on State Responsibility states that before taking countermeasures, an injured state shall call upon the responsible state to fulfil its obligations – in other words, cease the wrongful act. The injured state must also notify the responsible state of any decision to take countermeasures and offer to negotiate. This, too, may in practice present difficulties for countermeasures in the cyber context.[405] However, paragraph 2 of the Article states that injured states may take such urgent countermeasures as are necessary to preserve its right without notifying the responsible state first. The ILC commentary explicitly refers to the possibility of the notification requirement frustrating its own purpose.[406]

The International Court of Justice has recognized countermeasures in several cases and also referred to the requirement of their proportionality. In *Nicaragua*, the Court stated that the acts that were of issue could only have justified proportionate countermeasures on the part of the victim state.[407] In the *Gabčíkovo-Nagymaros Project* case the Court *inter alia* reaffirmed the requirement of proportionality and stated that countermeasures must be reversible.[408] The ILC took a slightly less strict position and notes in the commentary to the Draft Articles that countermeasures must be as far as possible reversible.[409]

6.2.4 Plea of Necessity

In addition to countermeasures, the Draft Articles on State Responsibility includes the notion of the plea of necessity in Article 25. According to the Article, a state may invoke

404 Report of the ILC, Fifty-third Session, *supra* note 99 at 326–327.
405 Schmitt, *Cyber Activities and the Law of Countermeasures*, *supra* note 385 at 677.
406 Report of the ILC, Fifty-third Session, *supra* note 99 at 347.
407 *Nicaragua*, *supra* note 114 at para. 249.
408 *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)* (Judgment), I. C. J. Reports 1997, p. 7 at paras 83–87.
409 Report of the ILC, Fifty-third Session, *supra* note 99 at 327.

necessity as a ground for precluding wrongfulness if it is the only way for the state to safeguard an essential interest against a grave and imminent peril and the act does not seriously impair an essential interest of a state towards which the obligation exists or the international community as a whole. The commentary of the ILC notes that the plea of necessity will only rarely be available and it is subject to strict limitations to prevent possible abuse.[410] It is also noteworthy that no internationally wrongful act must exist for a state to be able to invoke the plea of necessity.[411]

As necessity may only be invoked in very exceptional circumstances, it should not be seen as substitute for self-defence or countermeasures, but rare as it may be, there is nothing to absolutely exclude the possibility of a cyber attack constituting such a grave and imminent peril that necessity does preclude the wrongfulness of the acts taken in response to the attack.[412] Even though the limitations are strict, the peril does not need to originate from a state actor and the origin need not necessarily even be identified. This is especially relevant to cyber operations, because of the possible difficulties in determining the origin of the attack.[413] Uncertainty of the origin does, of course, in practice set quite strict limits on the possible responses. The Tallinn Manual notes that it is 'highly uncertain' whether or not a state may use force in accordance with the plea of necessity.[414]

6.3 Acts of Retorsion

Acts of retorsion are, according to the view adopted by the International Law Commission, distinct from countermeasures: they may be defined as unfriendly acts which are not itself inconsistent with any international obligation of a state even though they may be a response to an internationally wrongful act.[415] Acts of retorsion may also be taken in response to acts that in some way fall below the threshold of an intervention, for example due to the lack of a coercive element.[416] States may, of course, use them in response to interventions as well, if they see them as adequate or otherwise the best alternative. Acts of retorsion might include for example limitations on the diplomatic relations, embargoes or

410 Report of the ILC, Fifty-third Session, *supra* note 99 at 195.
411 Schmitt, *Cyber Activities and the Law of Countermeasures*, *supra* note 385 at 663.
412 Geiß and Lahmann, *Freedom and Security in Cyberspace*, *supra* note 380 at 646, 648.
413 Schmitt, *Cyber Activities and the Law of Countermeasures*, *supra* note 385 at 663.
414 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 39.
415 Report of the ILC, Fifty-third Session, *supra* note 99 at 325.
416 Gill, *Non-Intervention in the Cyber Context*, *supra* note 364 at 230.

withdrawal of voluntary aid *et cetera*.[417] The general principles of international law apply to retorsions too, and also they are subject to the requirements of necessity and proportionality.[418]

As with countermeasures, the exact content and limitations of retorsions make them somewhat difficult tools for states to use in responding to cyber operations. Compared to them, the concept of self-defence offers a more established and wide legal basis for actions. Without any significant developments clarifying the situation, it is imaginable states will continue to prefer the framework of self-defence.

6.4 Criminal Jurisdiction

While the focus of this thesis is on acts of states and those attributable to them, it bears worth mentioning the Council of Europe Convention on Cybercrime[419] (also known as the Budapest Convention on Cybercrime) which deals with criminal offences by individuals. The Convention entered into force in 2004 and calls upon states to adopt legislation that makes it a criminal offence under domestic law to for example access a computer system without authorization (Article 2) and to damage, delete, deteriorate, alter or suppress computer data (Article 4). It also includes provisions on issues such as jurisdiction, cooperation between states and information exchange. The Convention has also been signed and ratified by states which are not members of the Council of Europe, such as Japan and the United States. While a closer look at the criminal justice paradigm regarding cyber operations is outside the scope of this thesis, suffice it to say that prosecuting individuals responsible for a cyber operations poses significant challenges as well.[420] Many of the most visible non-state cyber attacks such as the previously mentioned Sony PlayStation Network breach and the hacking of several news outlet websites have been carried out by individuals or groups such as Anonymous and LulzSec and have thus fit within the purview of the Convention.

417 Report of the ILC, Fifty-third Session, *supra* note 99 at 325.
418 White and Abass, *Countermeasures and Sanctions*, *supra* note 376 at 538.
419 Council of Europe Convention on Cybercrime, 23 November 2001, in force 1 July 2004, CETS No. 185.
420 Gill, *Non-Intervention in the Cyber Context*, *supra* note 364 at 228–229.

As regards the criminal liability for cyber operations, also the Kampala Amendments to the Rome Statute of the International Criminal Court[421] should be mentioned. Article 8 *bis* of the Rome Statute covers the crime of aggression, which in paragraph 1 of the Article is defined as the planning, preparation, initiation or execution of an act of aggression which constitutes a manifest violation of the UN Charter. Paragraph 2 references the Definition of Aggression resolution and repeats the 7-point list of acts that qualify as an act of aggression. It would thus seem that it would be possible for the Article to cover certain cyber attacks as well.

421 Rome Statute of the International Criminal Court, 17 July 1998, in force 1 July 2002, 2187 UNTS 90.

7 Conclusions

The emergence of cyber attacks is the newest part in the evolution of war and in the continuum of changes in warfare brought on by technological changes.[422] These changes inevitably challenge the framework on the use of force, as well as other relevant facets of international law, such as international humanitarian law. The regulation of the use of force is one of the most controversial aspects of international law,[423] and the ambiguity of the notions of force and armed attack is neither a new phenomenon nor limited to the context of cyber operations. It is thus no wonder that the introduction of such an ambiguous concept as cyber attacks into the picture has caused some commotion.

An enormous amount of exaggeration and misconception revolves around the issue of cyber operations. Many of the examples used in this thesis have been hypothetical, and not all of them are likely to materialize in the near future. As for the worse ones, we can only hope that they remain on a hypothetical level. It is easy to agree with Thomas Rid that it seems unlikely that we will see a pure cyber war in the foreseeable future.[424] This, however, does not mean that cyber attacks will not happen at all or that international law does not need to concern itself with them. In fact, as cyber operations may very well be used to prepare the battlefield for a more traditional attack, the question of when a state may respond to a cyber operation in self-defence is of utmost importance.[425]

It is clear that cyber operations may constitute a use of force if the scale and effects of the attack are sufficiently extensive. Considering *lex lata*, the best criteria in assessing whether or not the attack constitutes force is the effects-based model. The target-based one would be rather effortless to apply to cyber operations, but it would expand the notion of force, and especially that of an armed attack, too far. It also seems to lack support compared to the effects-based approach. The instrument-based model seems outdated, and its application to the context of cyber operations is difficult.[426]

---

422 Generally on technical developments and war see Arquilla and Ronfeldt, *Cyberwar is Coming!*, *supra* note 7 at 24.
423 Gray, *International Law and the Use of Force*, *supra* note 214 at 7.
424 Rid, *Cyber War Will Not Take Place*, *supra* note 53 at 174.
425 The Tallinn Manual describes a cyber operation against the air defence of a state in preparation of an air campaign as a paradigmatic case. Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 63.
426 Hathaway *et al.*, *The Law of Cyber-Attack*, *supra* note 36 at 846.

Applying the effects-based model does then bring up the question of what kind of effects are enough to constitute a use of force. The Tallinn Manual argues that operations that cause death, injury, damage or destruction are unambiguously uses of force.[427] This, subjected to a *de minimis* rule at least on the criterion of damage, is a reasonable and justified starting point. The harder question involves the attacks with less obvious and significant consequences. Closely related to this issue is the question of economic force. The prevailing view is that Article 2(4) does not concern economic force, but as cyber operations make it very much possible for attackers – be that states or non-state actors – to inflict even severe economic consequences without any physical damage, the debate might well be far from concluded. It may even be asked whether or not we are one cyber attack with catastrophic economic consequences away from the thoughts of Grigorij Tunkin propelling back to the core of the discussion, this time endorsed by the highly networked western states who arguably are the most vulnerable to cyber attacks against the financial system. In other words, the very states who previously argued for the exclusion of economic force from the ambit of Article 2(4).[428]

The prevailing view distinguishes between uses of force and armed attacks. It is unclear where the threshold of an armed attack lies, yet the attack need not necessarily be an extremely destructive and wide-ranging one: the International Court of Justice did not exclude the possibility of an attack on a single military ship constituting an armed attack in *Oil Platforms*.[429] It is also entirely possible for a cyber attack to rise to the level of an armed attack, and the consensus seems to be that at least attacks with lethal results or significant property damage do indeed cross the threshold of an armed attack and justify self-defence on the basis of Article 51 of the UN Charter. It is again the effects-based view that is the most logical means of assessing the attack. Cyber attacks that would cross the threshold of an armed attack are exceptional, and it seems that no attack has thus far done so.

The question of attribution is especially relevant to cyber attacks due to the technical nature of the internet and the possibility to mask the origin of the attack. Even if subsequent analysis would reveal the attacker, the investigation might take months, if not

427 Schmitt (ed.), *Tallinn Manual*, *supra* note 21 at 48.
428 Bowett, *Economic Coercion and Reprisals by States*, *supra* note 148 at 1.
429 *Oil Platforms*, *supra* note 227 at para. 72 and *supra* at 62.

longer. It should be kept in mind, though, that while a hacker who steals credit card information very much has an incentive to hide the origin of the attack and cover his or her traces, the same does not necessarily apply to states carrying out attacks on each other or non-state actors carrying out attacks on states. Another issue involves quickly recognizing and distinguishing the cyber attacks which aim to cause damage from those which aim to gather information and constitute espionage.

There have been calls for a treaty that would regulate the issue of cyber attacks conducted by states. It remains to be seen whether such a treaty will materialize, but even if it does and even if it would bring clarity to the inter-state cyber operations, the question of non-state actors is likely to remain. And as disagreement remains over the essential issues outside the context of cyber operations as well, it seems unlikely that states would be able to reach a convention that would prove to be a panacea. It thus seems that cyber operations are no exception in this sense either, and the international law concerning them is likely to evolve in the usual manner, through state practice, scholarly opinions and possible resolutions of the United Nations Security Council and the General Assembly, as well as possible judgments or advisory opinions on the issue by the International Court of Justice.