## DAFTAR PUSTAKA

**BUKU :**


Andrew Murray D. 2007. *The Regulation of Cyberspace, Control in the Online Environment*. Routledge-Cavendish. London.

Ambarwati, Denny Ramdhany, dan Rina Rusman. 2013. *Hukum Humaniter Internasional Dalam Studi Hubungan Internasional*. Rajawali Pers. Jakarta.

Amiruddin, dan Zainal Asikin. 2014. Pengantar Metode Penelitian Hukum. Rajawali Pers. Jakarta.

Arlina Permanasari et. al. 1999. Pengantar Hukum Humaniter Internasional. ICRC. Jakarta.

C.E. Brand. 1968. Roman Military Law. University of Texas. Austin.

Denny Ramdhany, Hibertus Jaka Triyani, dan Yustina Trihoni. 2015. Konteks dan Perspektif Politik Terkait Hukum Humaniter Internasional Kontemporer. RajaGrafindo Persada. Jakarta.

Frederick de Mullinen. 1987. Handbook on the Law of the War for Armed Forces. ICRC. Geneva.

G.P.H. Haryomataram. 1998. Bunga Rampai Hukum Humaniter (Hukum Perang). Bumi Nusantara Jaya. Jakarta.

----------. 1984. Hukum Humaniter. CV. Rajawali. Jakarta.

---------- (ed). 2005. Pengantar Hukum Humaniter. RajaGrafindo Persada. Jakarta.

----------. 2012. Refleksi dan Kompleksitas Hukum Humaniter. Pusat Studi Hukum Humaniter & HAM Fakultas Hukum Trisakti. Jakarta.

Gregory Reichberg. 1997. The Ethics of War. Blackwell Publishing. Massachusetts.

ICRC. 2012. Kekerasan dan Penggunaan Kekuatan. ICRC. Jakarta.

James Hillman. 2004. A Terrible Love of War. Penguin Book. New York.

Jayaswal. 1930. Manu and Yajnavalkya, a Comparison and a Contrast: a Treatise on the Basic Hindu Law. Butterworth. Calcutta.

Jean-Marie Henckaerts, dan Louise Doswald-Beck. 2009. Customary International Humanitarian Law Volume I: Rules. Cambridge University Press. New York.

Jean Pictet. 1985. Develepment and Principle of International Humanitarian Law. Martinus Niijhoff Publisher-Henry Dunant Institute.

J.G. Starke. 1977. Introduction to International Law. Butterworths. London.

J.G Starke. 2010. Pengantar Hukum Internasional Edisi Kesepuluh, Diterjemahkan oleh Bambang Iriana Djajatmaja. Sinar Grafika. Jakarta.

Joenadi Efendi, dan Johny Ibrahim. 2016. Metode Penelitian Hukum Normatif dan Empiris. Kencana. Jakarta.

John Keegan. 2001. War and Our World, Vintage Books. New York.

Josua Sitompul. 2012. Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana. Tatanusa. Jakarta

Kareen Jabre, Norah Babic, dan Antoine Bouvier. 2016. International Humanitarian Law: Handbook for Parliamentarians. ICRC dan IPU. Geneva.

Laurel Gisel, dan Lukasz Olejnik. 2016. The Potential Human Cost of Cyber Operations. ICRC. Geneva.

Lauterpacht,. 1955. International Law: a Treatise Vol. 1. Longmans, Green Co. London.

Maskun, *et al*. 2020. Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional. Nas Media Pustaka. Makassar.

Michael Howard, George Andreopoulos, dan Mark Shulman. 1994. The Laws of War. Yale University Press. New Haven.

Mochtar Kusumaatmadja. 1980. Hukum Internasional Humaniter dalam Pelaksanaannya di Indonesia. Bina Cipta. Bandung.

----------. 2002. Konvensi – Konvensi Palang Merah 1949. PT. Alumni. Bandung.

Nils Melzer. 2009. Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. ICRC. Geneva

Pietro Verri. 1992. Dictionary of the International Law of Armed Conflict. ICRC. Geneva.

Ria Wierma Putri. 2011. Hukum Humaniter Internasional. Penerbit Universitas Lampung. Bandar Lampung.

Richard A. Clarke, dan Robert Knake. 2010. Cyber War The Next Threat to National Security and What to Do About it. Imprint of HarperCollins. United State of America.

Ronny Hanitijo Soemitro. 1984. Masalah – Masalah Sosiologi Hukum. Sinar Baru. Bandung.

Soemaryono. 1993. Hermenutik Sebuah Metode Filsafat. Penerbit Kanisius. Yogyakarta.

Soerjono Soekanto. 1986. Pengantar Penelitian Hukum. UI-Press. Jakarta.

Steve Winterfield, dan Jason Andress. 2013. The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Syngress. Amsterdam

William Boothby. 2012. The Law of Targeting. Oxford University Press.

Zayyid bin Abdel. 2008. Hukum Humaniter Internasional dalam Islam. ICRC. Jakarta.

**JURNAL :**

Abd. Latif Bustami. Palang Merah di Negeri Bulan Bintang: Sebuah Kajian tentang Strategi Kebudayaan Internasional Committee of Red Cross (ICRC) di Indonesia. Sejarah dan Budaya. Vol. 8 Nomor 1 Juni 2014.

ICRC. The Evolution of Warfare. International Review of the Red Cross. Vol. 97 Nomor 900 2015.

Cordula Droege. Get off my cloud: cyber warfare, international humanitarian law, and the protection of civillians. International Review of the Red Cross. Vol. 94 Nomor 886 2012.

Farid Fad. Reformulasi Ius ad Bellum dan Ius ad Bello dalam Perspektif Hukum Islam dan Hukum Humaniter. Al Ahkam. Vol 16 No. 1 2020.

Iqbal Asnawi. Konsistensi Penegakan Hukum Humaniter Internasional dalam Hubungan Antar Bangsa. Jurnal Hukum Samudra Keadilan. Vol. 12 Nomor 1 Januari – Juni 2017.

Jean-Francois Queguiner. Precautions under the law governing the conduct of hostilities. International Review of the Red Cross. Vol. 88 Nomor 864 Desember 2006.

Jerry Indrawan. Konsep “Keikutsertaan Langsung dalam Permusuhan” dan “Prinsip Pembedaan” dalam Konflik Bersenjata”. Jurnal Hubungan Internasional. Vol. 4, Nomor 2 Oktober 2015.

John Merriam. Affirmative Target Identification: Operationalizing the Principle of Distinction for U.S. Warfighters. Virginia Journal of International Law. Vol. 56 Nomor 1 Maret 2016.

John Richardson. *Stuxnet as Cyberwarfare: Distinction and Proportionality on the Cyber Battelfield*. Journal of Information Technology & Privacy Law. Vol. 9 Nomor 1 2011

Levina Yustitianingtyas. Perlindungan Orang Sipil dalam Hukum Humaniter Internasional. Jurnal Komunikasi Hukum. Vol. 2 Nomor 1 Februari 2016.

Michael N. Schmitt. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. Harvard International Law Journal. Vol. 54 2012.

Rain Liivoja. Technological Change and the Evolution of the Law of War. International Review of the Red Cross. Vol. 97 Nomor 900 2015.

Rubiyanto. Perkembangan Hukum Humaniter dalam Konflik Militer Internasional. Serat Acitya. Vol. 5 Nomor 2 2016.

Vincent Bernard. Tactics, Techniques, Tragedies: A Humanitarian Perspective on the Changing Face of War. International Review of the Red Cross. Vol. 97 Nomor 900 2015.

Vincent Chetail. The contribution of the International Court of Justice to international humanitarian law. International Review of the Red Cross. Vol. 85 Nomor 850 2003

**SKRIPSI DAN MAKALAH :**

Alfira Nurliliani Samad. 2015. Analisis Instrumen Cyber-terrorism dalam Kerangka Sistim Hukum Internasional. Skripsi. Fakultas Hukum Universitas Hasanuddin, Makassar.

Dinul Haq Qayyim. 2017. Penerapan Prinsip Pembedaan dalam Konflik Bersenjata di Suriah Menurut Hukum Humaniter Internasional. Skripsi. Fakultas Hukum Universitas Hasanuddin, Makassar.

Kartini Eliva Angel Tampubolon. 2018. Kedudukan Cyber Warfare dalam Hukum Internasional. Skripsi. Fakultas Hukum Universitas Airlangga. Surabaya

Mochammad Arief Agus. 2018. Tinjauan Hukum Humaniter Internasional Terhadap Pengeboman Masjid Umar Ibn Khattab oleh Militer AS di Suriah. Skripsi. Fakultas Hukum Universitas Hasanuddin, Makassar.

Sukma Indrajati. 2014. TInjauan Hukum Internasional Terhadap Cyber Espionage Sebagai Salah Satu Bentuk Cybercrime". Skripsi. Fakultas Hukum Universitas Hasanuddin, Makassar.

Umesh Kadam. 2006. Political and Social Science and International Humanitarian Law. Makalah. Seminar Hukum Humaniter Internasional, Universitas Gadjah Mada. Yogyakarta.

**BERITA DAN ARTIKEL :**

Anshel Pfeffer. "*Israel Suffered Massive Cyber Attack During Gaza Offensive*", diakses dari https://www.haaretz.com/1.5065382 Pada 14 Januari 2021.

Cyberwire. "*Cyber Vandalism*", diakses dari https://thecyberwire.com/glossary/cyber-vandalism Pada 6 Februari 2021.

ICRC. 2019. International Humanitarian Law and Cyber Operations during Armed Conflicts. (ICRC Position paper)

ICRC. "*Direct participation in hostilities: questions & answers*", diakses dari https://www.icrc.org/en/doc/resources/documents/faq/direct-participation-ihl-faq-020609.htm Pada 28 April 2021.

ICRC. "*Direct participation in hostilities*", diakses dari https://www.icrc.org/en/document/civilian-direct-participation-hostilities Pada 28 April 2021.

ICRC. "*Internal Disturbance and Tensions*", diakses dari https://casebook.icrc.org/glossary/internal-disturbances-and-tensions Pada 22 Januari 2021.

ICRC. "*Iran, Victim of Cyber warfare*", diakses dari https://casebook.icrc.org/case-study/iran-victim-cyber-warfare Pada 14 Januari 2021.

ICRC. "*Sejarah International Committee of Red Cross*", diakses dari https://blogs.icrc.org/indonesia/tentang-icrc/sejarah/ Pada 18 Januari 2021

Jake Frankenfield. "*Artificial Intelligence (AI)*", diakses dari https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp Pada 11 Mei 2021

Malahayati. 2015. Hukum Humaniter Internasional: Konflik Bersenjata Non – Internasional. (Project Report)

Mitch Tanenbaum. "*Kinetic War vs Cyber War: The Potential Battlefield Ahead*", diakses dari https://www.msspalert.com/cybersecurity-breaches-and-attacks/cyber-war-vs-kinetic-war-explained/ Pada 14 Januari 2021.

Nato Review Magazine. "*The History of Cyber Attacks*", diakses dari https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm Pada 14 Januari 2021.

Nicole Urban. "*Direct and Active Participation in Hostilities: The Unintended Consequences of the ICC's decision in Lubanga*", diakses dari https://www.ejiltalk.org/direct-and-active-participation-in-hostilities-the-unintended-consequences-of-the-iccs-decision-in-lubanga/ Pada 28 April 2021.

Steve Ragan. "*Ransomware takes Hollywood Hospital offline, $3.6M demanded by attackers*", diakses dari https://www.csoonline.com/article/3033160/ransomware-takes-

hollywood-hospital-offline-36m-demanded-by-attackers.html Pada 14 Januari 2021.

Tom Uren, Bart Hagoyen, dan Fergus Hanson. "*Defining offensive cyber capabilities*", diakses dari https://www.aspi.org.au/report/defining-offensive-cyber-capabilities Pada 20 Januari 2021

UNTERM. "*Cyberwarfare*", diakses dari https://unterm.un.org/unterm/DGAACS/unterm.nsf/WebView/BFDE24673F1B1F6E85256AFD006732A3?O Pada 20 Januari 2021.

Yunita Maya Putri, Rehulina, dan Ria Wierma Putri. 2020. Perlindungan Terhadap Korban Perang dalam Penegakan Hukum Humaniter Internasional. (Working Paper)

**INSTRUMEN HUKUM INTERNASIONAL :**

Charter of the United Nations 1945.

Convention on Cybercrime 2001.

Convention on the Prohibition or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, 2001

Commentary on the Additional Protocol of 8 June 1977 to the Geneva Convention of 12 August 1949,

Department of Defence, *The National Military Strategy for Cyberspace Operations*, 2006.

Laws and Customs of War on Land (Hague, II) 1899

Legalitiy of the Threat or Use of Nuclear Weapons, Advisory Opinion July 8, 1966, ICJ Rep. 1996

Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol 1),

Rome Statute of the International Criminal Court, 1998

Statute of the International Court of Justice 1945.

Taliin Manual on the International Law Applicable to Cyber Warfare, 2013

Vienna Convention on the Law of Treaties 1969.

# LAMPIRAN

# A. LAMPIRAN 1 (VIENNA CONVENTION ON THE LAW OF TREATIES PASAL 2(1))

*Article 2*
*Use of terms*

1. For the purposes of the present Convention:

(*a*) "treaty" means an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation;

(*b*) "ratification", "acceptance", "approval" and "accession" mean in each case the international act so named whereby a State establishes on the international plane its consent to be bound by a treaty;

(*c*) "full powers" means a document emanating from the competent authority of a State designating a person or persons to represent the State for negotiating, adopting or authenticating the text of a treaty, for expressing the consent of the State to be bound by a treaty, or for accomplishing any other act with respect to a treaty;

(*d*) "reservation" means a unilateral statement, however phrased or named, made by a State, when signing, ratifying, accepting, approving or acceding to a treaty, whereby it purports to exclude or to modify the legal effect of certain provisions of the treaty in their application to that State;

(*e*) "negotiating State" means a State which took part in the drawing up and adoption of the text of the treaty;

(*f*) "contracting State" means a State which has consented to be bound by the treaty, whether or not the treaty has entered into force;

(*g*) "party" means a State which has consented to be bound by the treaty and for which the treaty is in force;

(*h*) "third State" means a State not a party to the treaty;

(*i*) "international organization" means an intergovernmental organization.

2. The provisions of paragraph 1 regarding the use of terms in the present Convention are without prejudice to the use of those terms or to the meanings which may be given to them in the internal law of any State.

*Article 3*
*International agreements not within the scope of the present Convention*

The fact that the present Convention does not apply to international agreements concluded between States and other subjects of international law or between such other subjects of international law, or to international agreements not in written form, shall not affect:

## B. LAMPIRAN 2 (UNITED NATIONS CHARTER PASAL 2(4) DAN 51)

# CHAPTER I

## PURPOSES AND PRINCIPLES

### *Article 1*

The Purposes of the United Nations are:

1. To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;

2. To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace;

3. To achieve international cooperation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and

4. To be a center for harmonizing the actions of nations in the attainment of these common ends.

### *Article 2*

The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.

1. The Organization is based on the principle of the sovereign equality of all its Members.

2. All Members, in order to ensure to all of them the rights and benefits resulting from membership, shall fulfil in good faith the obligations assumed by them in accordance with the present Charter.

3. All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.

4. 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.

5. All Members shall give the United Nations every assistance in any action it takes in accordance with the present Charter, and shall refrain from giving assistance to any state against which the United Nations is taking preventive or enforcement action.

6. The Organization shall ensure that states which are not Members of the United Nations act in accordance with these Principles so far as may be necessary for the maintenance of international peace and security.

7. Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII.

# CHAPTER II

## MEMBERSHIP

### *Article 3*

The original Members of the United Nations shall be the states which, having participated in the United Nations Conference on International Organization at San Francisco, or having previously signed the Declaration by United Nations of January 1, 1942, sign the present Charter and ratify it in accordance with Article 110.

represented on it to provide armed forces in fulfillment of the obligations assumed under Article 43, invite that Member, if the Member so desires, to participate in the decisions of the Security Council concerning the employment of contingents of that Member's armed forces.

*Article 45*

In order to enable the United Nations to take urgent military measures, Members shall hold immediately available national air-force contingents for combined international enforcement action. The strength and degree of readiness of these contingents and plans for their combined action shall be determined, within the limits laid down in the special agreement or agreements referred to in Article 43, by the Security Council with the assistance of the Military Staff Committee.

*Article 46*

Plans for the application of armed force shall be made by the Security Council with the assistance of the Military Staff Committee.

*Article 47*

1. There shall be established a Military Staff Committee to advise and assist the Security Council on all questions relating to the Security Council's military requirements for the maintenance of international peace and security, the employment and command of forces placed at its disposal, the regulation of armaments, and possible disarmament.

2. The Military Staff Committee shall consist of the Chiefs of Staff of the permanent members of the Security Council or their representatives. Any Member of the United Nations not permanently represented on the Committee shall be invited by the Committee to be associated with it when the efficient discharge of the Committee's responsibilities requires the participation of that Member in its work.

3. The Military Staff Committee shall be responsible under the Security Council for the strategic direction of any armed forces placed at the disposal of the Security Council. Questions relating to the command of such forces shall be worked out subsequently.

4. The Military Staff Committee, with the authorization of the Security Council and after consultation with appropriate regional agencies, may establish regional subcommittees.

*Article 48*

1. The action required to carry out the decisions of the Security Council for the maintenance of international peace and security shall be taken by all the Members of the United Nations or by some of them, as the Security Council may determine.

2. Such decisions shall be carried out by the Members of the United Nations directly and through their action in the appropriate international agencies of which they are members.

*Article 49*

The Members of the United Nations shall join in affording mutual assistance in carrying out the measures decided upon by the Security Council.

*Article 50*

If preventive or enforcement measures against any state are taken by the Security Council, any other state, whether a Member of the United Nations or not, which finds itself confronted with special economic problems arising from the carrying out of those measures shall have the right to consult the Security Council with regard to a solution of those problems.

*Article 51*

Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Mem-

ber of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

## CHAPTER VIII

### REGIONAL ARRANGEMENTS

*Article 52*

1. Nothing in the present Charter precludes the existence of regional arrangements or agencies for dealing with such matters relating to the maintenance of international peace and security as are appropriate for regional action, provided that such arrangements or agencies and their activities are consistent with the Purposes and Principles of the United Nations.

2. The Members of the United Nations entering into such arrangements or constituting such agencies shall make every effort to achieve pacific settlement of local disputes through such regional arrangements or by such regional agencies before referring them to the Security Council.

3. The Security Council shall encourage the development of pacific settlement of local disputes through such regional arrangements or by such regional agencies either on the initiative of the states concerned or by reference from the Security Council.

4. This Article in no way impairs the application of Articles 34 and 35.

*Article 53*

1. The Security Council shall, where appropriate, utilize such regional arrangements or agencies for enforcement action under its authority. But no enforcement action shall be taken under regional arrangements or by regional agencies without the authorization of the Security Council, with the exception of measures against any enemy state, as defined in paragraph 2 of this Article, provided for pursuant to Article 107 or in regional arrangements directed against renewal of aggressive policy on the part of any such state, until such time as the Organization may, on request of the Governments concerned, be charged with the responsibility for preventing further aggression by such a state.

2. The term enemy state as used in paragraph 1 of this Article applies to any state which during the Second World War has been an enemy of any signatory of the present Charter.

*Article 54*

The Security Council shall at all times be kept fully informed of activities undertaken or in contemplation under regional arrangements or by regional agencies for the maintenance of international peace and security.

## CHAPTER IX

### INTERNATIONAL ECONOMIC AND SOCIAL COOPERATION

*Article 55*

With a view to the creation of conditions of stability and well-being which are necessary for peaceful and friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, the United Nations shall promote:

a. higher standards of living, full employment, and conditions of economic and social progress and development;

b. solutions of international economic, social, health, and related problems; and inter-

## C. LAMPIRAN 3 (*TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE* ATURAN 1 DAN 13)

***Section 1: Sovereignty, Jurisdiction, and Control***

*RULE 1 – Sovereignty*

**A State may exercise control over cyber infrastructure and activities within its sovereign territory.**

1. This Rule emphasizes the fact that although no State may claim sovereignty over cyberspace *per se,* States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure.

2. The accepted definition of 'sovereignty' was set forth in the *Island of Palmas* Arbitral Award of 1928. It provides that "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State".[21]

3. It is the sovereignty that a State enjoys over territory that gives it the right to control cyber infrastructure and cyber activities within its territory. Accordingly, cyber infrastructure situated in the land territory, internal waters, territorial sea (including its bed and subsoil), archipelagic waters, or national airspace is subject to the sovereignty of the territorial State.[22]

4. Sovereignty implies that a State may control access to its territory and generally enjoys, within the limits set by treaty and customary international law, the exclusive right to exercise jurisdiction and authority on its territory. Exceptions include the use of force pursuant to the right of self-defence (Rule 13) and in accordance with actions authorized or mandated by the United Nations Security Council (Rule 18).

5. A State's sovereignty over cyber infrastructure within its territory has two consequences. First, that cyber infrastructure is subject to legal and regulatory control by the State.[23] Second, the State's territorial sovereignty protects such cyber infrastructure. It does not matter whether it belongs to the government or to private entities or individuals, nor do the purposes it serves matter.

6. A cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty. It certainly does so if it causes damage. The International Group of Experts could achieve no consensus as to whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty.

---

[21] Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

[22] On sovereignty over waters and airspace above waters, see Law of the Sea Convention, art. 2; on sovereignty over airspace, see Chicago Convention, arts. 1-3. With regard to cyber infrastructure in outer space, see Rules 3 and 4 and accompanying Commentary.

[23] In the 1949 Corfu Channel Case, Judge Alejandro Alvarez appended a separate opinion in which he stated: "By sovereignty, we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States. Sovereignty confers rights upon States and imposes obligations upon them." Corfu Channel Case at 43 (individual opinion of Judge Alvarez).

3. It is generally accepted that threats by States and officials in a position to make good those threats are lawful if the threatened action is itself lawful.[117] There are two recognized exceptions to the international law prohibition on the use of force: the exercise of the right of self-defence and actions implementing a United Nations Security Council resolution under Chapter VII of the United Nations Charter (Rules 13 and 18). For instance, it would be lawful to threaten that a State will defend itself forcefully if attacked. Threatening other actions that do not violate international law would likewise be lawful.

4. Although threats are usually intended to be coercive in effect, there is no requirement that a specific 'demand' accompany the threat. The essence of a threat is that it is explicitly or impliedly communicative in nature. Actions which simply threaten the security of the target State, but which are not communicative in nature, do not qualify. For example, consider the case in which tensions between State A and State B are high. State A begins aggressively to develop the capability to conduct massive malicious cyber operations against State B. The mere acquisition of such capabilities that can be used to conduct uses of force does not constitute a threat. However, if the leader of State A announces, either on a conditional basis or otherwise, that the capabilities will be used for that purpose against State B, State A will be in violation of this Rule.

5. The International Group of Experts was divided as to whether a State manifestly lacking any capability to make good its threat, can violate this Rule. Despite the difference of opinion, it must be noted that cyber capability is not as dependent on a State's size, population, or economic and military capacity of a State as is the capacity to use conventional force. This means that it may be more difficult for a State to evaluate the capacity of another State to make good on its threat to use force by cyber means. Therefore, this issue plays a diminished role in evaluating cyber threats.

6. Similarly, no consensus could be achieved regarding a State that possesses the capability to carry out the threat but which clearly has no intention of doing so. An example would be that of a State that possesses an offensive cyber capability whose leader utters threats against other States for purely domestic political reasons.

## ***Section 2: Self-Defence***

*RULE 13 – Self-Defence Against Armed Attack*

**A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects.**

1. According to Article 51 of the United Nations Charter, "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has

[117] By distinguishing lawful from unlawful threats, the International Court of Justice conceded the existence of the former: "[I]f it is to be lawful, the declared readiness of a State to use force must be a use of force that is in conformity with the Charter." Nuclear Weapons Advisory Opinion, para. 47.

taken the measures necessary to maintain international peace and security". This article recognizes and reflects the customary right of self-defence.

2. An armed attack must have a trans-border element. This criterion is always met when one State engages in a cyber operation otherwise qualifying as an armed attack against another State, or directs non-State actors, wherever they may be, to do so. The more difficult case involves cyber operations by non-State actors against one State that are not conducted on behalf of another State. The issue of whether non-State actors not acting on behalf of a State can initiate an armed attack is dealt with below. With regard to acts organized, conducted, and directed solely from within a State's own territory, States may use force in accordance with their own domestic laws (informed by international law standards such as human rights law and, in situations of non-international armed conflict, the law of armed conflict).

3. The right to employ force in self-defence extends beyond kinetic armed attacks to those that are perpetrated entirely through cyber operations. The International Group of Experts unanimously concluded that some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter. This conclusion is in accord with the International Court of Justice's insistence in its *Legality of Nuclear Weapons* Advisory Opinion that the choice of means of attack is immaterial to the issue of whether an operation qualifies as an armed attack.[118] Moreover, the position is consistent with State practice.[119] For example, it is universally accepted that chemical, biological, and radiological attacks of the requisite scale and effects to constitute armed attacks trigger the right of self-defence. This is so, despite their non-kinetic nature, because the ensuing consequences can include serious suffering or death. Identical reasoning would apply to cyber operations.

4. The International Group of Experts was divided as to whether the notion of armed attack, because of the term 'armed', necessarily involves the employment of 'weapons' (Rule 41). The majority took the position that it did not and that instead the critical factor was whether the effects of a cyber operation, as distinct from the means used to achieve those effects, were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack.

5. In the view of the International Group of Experts, the term 'armed attack' is not to be equated with the term 'use of force' appearing in Rule 11.[120] An armed attack presupposes at least a use of force in the sense of Article 2(4). However, as noted by the International Court of Justice, not every use of force rises to the level of an armed attack.[121] The scale and effects required for an act to be characterised as an armed attack necessarily exceed those qualifying the act as a use of force. Only in the event that the use of force reaches the threshold of an armed attack is a State entitled to respond using force in self-defence.

6. The phrase "scale and effects" is drawn from the *Nicaragua* Judgment.[122] In that case, the Court identified scale and effects as the criteria that distinguish actions qualifying as

[118] Nuclear Weapons Advisory Opinion, para. 39.
[119] *See, e.g., White House Cyber Strategy*, at 10, 13.
[120] However, not all States accept this view. *See* discussion in Commentary accompanying Rule 11.
[121] Nicaragua Judgment, para. 191.
[122] Nicaragua Judgment, para. 195.

an armed attack from those that do not. It noted the need to "distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms", but provided no further guidance in this regard.[123] Therefore, the parameters of the scale and effects criteria remain unsettled beyond the indication that they need to be grave. That said, some cases are clear. The International Group of Experts agreed that any use of force that injures or kills persons or damages or destroys property would satisfy the scale and effects requirement. They also agreed that acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks.

7. The Experts took the view that the law is unclear as to the precise point at which the extent of death, injury, damage, destruction, or suffering caused by a cyber operation fails to qualify as an armed attack. In the *Nicaragua* Judgment, the International Court of Justice distinguished between an armed attack and a "mere frontier incident".[124] This distinction has been criticised by numerous commentators who adopt the view that only inconsequential actions are to be excluded.[125] In this regard, the International Court of Justice has itself indicated that an attack on a single military platform or installation might qualify as an armed attack.[126]

8. An important issue is whether a State may exercise the right of self-defence in response to a series of cyber incidents that individually fall below the threshold of an armed attack. In other words, can they constitute an armed attack when aggregated? The determinative factor is whether the same originator (or originators acting in concert) has carried out smaller scale incidents that are related and that taken together have the requisite scale. If there is convincing evidence that this is the case, the International Group of Experts agreed that there are grounds for treating the incidents as a composite armed attack.[127]

9. The case of actions that do not result in injury, death, damage, or destruction, but which otherwise have extensive negative effects, is unsettled. Some of the Experts took the position that harm to persons or physical damage to property is a condition precedent to the characterisation of an incident as an armed attack. Others took the view that it is not the nature (injurious or destructive) of the consequences that matters, but rather the extent of the ensuing effects. The classic scenario illustrating this division of opinion is a cyber incident directed against the New York Stock Exchange that causes the market to crash. The International Group of Experts was divided over the characterisation of such an event. Some of the Experts were unprepared to label it as an armed attack because they were not satisfied that mere financial loss constitutes damage for this purpose. Others emphasized the catastrophic effects such a crash would occasion and therefore regards them as sufficient to characterise the cyber operation as an armed attack. By the same approach, a cyber operation directed against major components (systems) of a

[123] Nicaragua Judgment, para. 191.
[124] Nicaragua Judgment, para. 195.
[125] *See, e.g.*, YORAM DINSTEIN, WAR, AGGRESSION AND SELF DEFENCE 210-211 (5th ed. 2011); William H Taft, *Self Defense and the Oil Platforms Decision*, 29 YALE JOURNAL OF INTERNATIONAL LAW 295, 300 (2004).
[126] Oil Platforms Judgment, paras. 57, 61.
[127] This approach has been labelled the 'pin-prick' theory, the 'accumulation of effects' theory, and 'Nadelstichtaktik'.

State's critical infrastructure that causes severe, albeit not destructive, effects would qualify as an armed attack.

10. A further challenging issue in the cyber context involves determining which effects to consider in assessing whether an action qualifies as an armed attack. The International Group of Experts agreed that all reasonably foreseeable consequences of the cyber operation so qualify. Consider, for example, the case of a cyber operation targeting a water purification plant. Sickness and death caused by drinking the contaminated water are foreseeable and should therefore be taken into account.

11. The International Group of Experts was divided over the issue of whether the effects in question must have been intended. For instance, consider the example of cyber espionage by State A against State B that unexpectedly results in significant damage to State B's cyber infrastructure. Some Experts were not willing to characterize the operation as an armed attack, although they acknowledged that measures could be taken to counteract the negative effects of the operation (especially in accordance with principle of necessity discussed in Commentary to Rule 9). The majority of the International Group of Experts took the view that intention is irrelevant in qualifying an operation as an armed attack and that only the scale and effects matter. However, any response thereto would have to comport with the necessity and proportionality criteria (Rule 14); the former would prove a significant hurdle in this respect. All the Experts agreed that the lawfulness of the response would be determined by the reasonableness of State B's assessment as to whether an armed attack was underway.

12. A cyber armed attack by State A against State B may have bleed-over effects in State C. If those effects meet the scale and effects criteria for an armed attack, the majority of the International Group of Experts would conclude that State C is entitled to resort to the use of force in self-defence, so long as the defensive action complied with the necessity and proportionality criteria. Indeed, even if the cyber operations against State B do not qualify as an armed attack, this would not preclude the bleed-over effects from amounting to an armed attack against State C. As to the issue of unintended bleed-over effects, see the discussion of intent above.

13. No international cyber incidents have, as of 2012, been unambiguously and publically characterised by the international community as reaching the threshold of an armed attack. In particular, the 2007 cyber operations against Estonia, which were widely referred to as 'cyber war', were not publicly characterised by either Estonia or the international community as an armed attack. The International Group of Experts agreed with this assessment on the basis that the scale and effects threshold was not reached. A closer case is the 2010 Stuxnet operations. In light of the damage they caused to Iranian centrifuges, some members of the International Group of Experts were of the view that the operations had reached the armed attack threshold [unless justifiable on the basis of anticipatory self-defence (Rule 15)].

14. It is also necessary to consider the issue of the 'originator' in determining whether an act qualifies as an armed attack. It is incontrovertible that an act conducted by organs of a State may so qualify. It is equally indisputable that the actions of non-State actors may sometimes be attributed to a State for the purpose of finding an armed attack. In the *Nicaragua* Judgment, the International Court of Justice stated that

> [a]n armed attack must be understood as including not merely action by regular forces across an international border, but also 'the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to' (*inter alia*) an actual armed attack conducted by regular forces, 'or its substantial involvement therein'.[128]

15. For instance, if a group of private individuals under the direction of State A undertakes cyber operations directed against State B, and the consequence of those actions reaches the requisite scale and effects, State A will have committed an armed attack. This same conclusion would apply to cyber operations conducted by a single individual at the direction of a State.

16. The issue of whether acts of non-State actors can constitute an armed attack absent direction by a State is controversial. Traditionally, Article 51 and the customary international law of self-defence were characterised as applicable solely to armed attacks undertaken by one State against another. Violent acts by non-State actors fell within the law enforcement paradigm. However, the international community characterised the 9/11 attacks by Al Qaeda on the United States as an armed attack triggering the inherent right of self-defence.[129] Such State practice appears to signal a willingness of States to apply the right of self-defence to attacks conducted by non-State actors. Moreover, while Article 2(4) addresses the actions of States, Article 51 contains no such limitation vis-à-vis armed attacks (although the text does make it clear that only States enjoy the right of self-defence). For its part, the International Court of Justice does not seem to have been prepared to adopt this approach.[130]

16. The majority of the International Group of Experts concluded that State practice established a right of self-defence in the face of armed attacks by non-State actors, such as terrorist or rebel groups. They would extend this right to self-defence against cyber operations conducted by information technology corporations or internet service providers if the operations reached the armed attack threshold. As an example, the majority of the International Group of Experts would consider a devastating cyber operation undertaken by a group of terrorists from within State A against critical infrastructure located in State B as an armed attack by those cyber terrorists against State B. A minority of the Group did not accept this premise.

17. The members of the International Group of Experts acknowledged the significant uncertainty that exists within the international law community regarding such matters as the degree of requisite organization a group must have (if any) to be capable of mounting an armed attack as a matter of law and any geographical limitations that may bear on this issue. Additionally, those Experts who took the position that a non-State group unaffiliated with a State could conduct an armed attack were split over the issue of

---

[128] Nicaragua Judgment, para. 195.

[129] The Security Council adopted numerous resolutions recognizing the applicability of the right of self-defence. *See, e.g.*, S.C. Res 1368 (Sept. 12, 2001); S.C. Res. 1373 (Sept. 28, 2001). International organizations such as NATO and many individual States took the same approach. See, e.g., Press Release, NATO, Statement by the North Atlantic Council (Sept. 12, 2001); Terrorist Threat to the Americas, Res. 1, Twenty-fourth Meeting of Consultation of Ministers of Foreign Affairs, Terrorist Threat to the Americas, OAS Doc. RC.24/RES.1/01 (Sept. 21, 2001); Brendan Pearson, *PM Commits to Mutual Defence*, AUSTRALIAN FINANCIAL REVIEW, Sept. 15, 2001, at 9.

[130] Wall Advisory Opinion, para. 139; Armed Activities in Congo Judgment, paras. 146-147.

whether a single individual mounting an operation that meets the scales and effects threshold could do so.

18. The object of an action meeting the scale and effects requirement may also determine whether it qualifies as an armed attack. If the object of action satisfying the trans-border and scale and effects criteria consists of property or persons within the affected State's territory, the action is an armed attack against that State. It must be noted that the International Group of Experts did not achieve consensus on whether further criteria must be met in order to bring into operation the right of self-defence. While some took the position that attacks solely motivated by purely private interests would not trigger the right of self-defence, others were of the view that motives are irrelevant. This issue is likely to be resolved through State practice.

19. If the object in question consists of property or citizens situated outside the State's territory, it is sometimes uncertain in international law whether the cyber operation can qualify as an armed attack. Attacks against non-commercial government facilities or equipment, and government personnel, certainly qualify as armed attacks so long as the above-mentioned criteria are met. For instance, a cyber operation undertaken by State A to kill State B's head of State while abroad would amount to an armed attack. The determination of whether other operations are armed attacks depends on, but is not limited to, such factors as: the extent of damage caused by the operation; whether the property involved is State or private in character; the status of the individuals who have been targeted; and whether the operations were politically motivated, that is, conducted against the property or individuals because of their nationality. No bright line rule exists in such cases. Consider a cyber operation conducted by State A to kill the CEO of one of State B's State-owned corporations abroad. Opinions among the members of the International Group of Experts were divided as to whether the operation amounted to an armed attack.

20. The exercise of the right of self-defence is subject to the requirements of necessity, proportionality, imminence, and immediacy (Rules 14 and 15). Of course, the exercise of self-defence is also subject to the existence of a reasonable determination that an armed attack is about to occur or has occurred, as well as to the identity of the attacker. This determination is made *ex ante*, not *ex post facto*.

21. Self-defence measures may be conducted from, and directed against entities on or in, the territory of the originator State, the victim-State's territory, the high seas, international airspace, or outer space (subject to applicable space law).

22. When defensive cyber operations are initiated from, or employ assets located in, a State to which the attack cannot be attributed, the principle of sovereignty must be carefully considered. It is indisputable that self-defence actions may be taken on foreign territory with that State's consent without violating its sovereignty. Therefore, the key issue with regard to defensive action on another State's territory is how to characterize non-consensual actions. The International Group of Experts was divided. The majority concluded that self-defence against a cyber armed attack in these circumstances is permissible when the territorial State is unable (e.g., because it lacks the expertise or technology) or unwilling to take effective actions to repress the relevant elements of the cyber armed attack. In particular, they emphasized that States have a duty to ensure their territory is not used for acts contrary to international law (Rule 5). By contrast, a

minority of the Group took the position that using force in self-defence on the territory of a State to which the armed attack is not attributable is impermissible, although other responses, such as an action based on the plea of necessity (Rule 9), might be appropriate. This, of course, presumes the absence of either the consent of that State or an authorization by the United Nations Security Council (Rule 18).

23. Those Experts who accepted the legality of cross-border defensive actions emphasized that the victim-State must first demand that the territorial State put an end to the activities comprising the armed attack. The victim-State must also afford the territorial State an opportunity to address the situation. These requirements derive from an international law obligation to respect (to the greatest extent possible) the sovereignty of the State on which the defensive actions are to take place. Additionally, they are procedural safeguards against a mistaken (or premature) conclusion as to the unwillingness or inability of the territorial State to address the situation. There may be exceptional situations where there is no time to convey a demand to the latter or for the latter to resolve the situation. If immediate action to repel a cyber armed attack is required to defeat the attack or minimize its consequences, the targeted State may act immediately in self-defence. Thus, these requirements are context-specific.

### *RULE 14 – Necessity and Proportionality*

**A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate.**

1. Actions in self-defence must meet two criteria — necessity and proportionality. The International Court of Justice acknowledged both in the *Nicaragua* Judgment and later confirmed them in its *Oil Platforms* Judgment.[131] The Nuremberg Tribunal also recognized the criteria.[132] As illustrated by these decisions, they undoubtedly reflect customary international law. It is important to note that the concepts of necessity and proportionality in the *jus ad bellum* are distinct from the concept of military necessity and the rule of proportionality in the *jus in bello*.

2. Necessity requires that a use of force, including cyber operations that amount to a use of force (Rule 11), be needed to successfully repel an imminent attack or defeat one that is under way. This does not mean that force has to be the only available response to an armed attack. It merely requires that non-forceful measures be insufficient to address the situation. Of course, the forceful actions may be combined with non-forceful measures such as diplomacy, economic sanctions, or law enforcement.

3. The key to the necessity analysis in the cyber context is, therefore, the existence, or lack, of alternative courses of action that do not rise to the level of a use of force. Should passive (as distinct from active) cyber defences like firewalls be adequate to reliably and completely to thwart a cyber armed attack, other measures, whether cyber or kinetic, at the level of a use of force are impermissible. Similarly, if active cyber operations not rising to the level of use of force are adequate to deter or repel armed attacks (imminent

[131] Nicaragua Judgment, paras. 176, 194; Nuclear Weapons Advisory Opinion, para. 41; Oil Platforms Judgment, paras. 43, 73-74, 76.
[132] Nuremburg Tribunal Judgment at 435 (referring to the *Caroline* formula).