Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 23 *Volume XXIII*
Number 4 *Volume XXIII Book 4*

Article 4

2013

Signs and Portents in Cyberspace: The Rise of Jus Internet as New Order in International Law

Roy Balleste
St. Thomas University - School of Law, rballeste@stu.edu

Joanna Kulesza
University of Lodz - Faculty of Law and Administration, joannakulesza@gmail.com

Signs and Portents in Cyberspace: The Rise of *Jus Internet* as a New Order in International Law

Joanna Kulesza, Ph.D.*
Roy Balleste, J.S.D.**

> The remarkable social impact and economic success of the Internet is in many ways directly attributable to the architectural characteristics that were part of its design. The Internet was designed with no gatekeepers over new content or services.
>
> —Vinton Cerf [1]

* Assistant Professor of International Law and International Relations, University of Lodz, Faculty of Law and Administration, Poland. Professor Kulesza is the Membership Committee Chair of the Global Internet Governance Academic Network (GigaNet).

** Professor of Law and Law Library Director, St. Thomas University School of Law, Miami Gardens, FL, USA. Professor Balleste is the Secretary of the Global Internet Governance Academic Network (GigaNet).

[1] Letter from Vinton Cerf, Chief Internet Evangelist, Google Inc., to Joe Barton, Chairman, Committee on Energy and Commerce, and John D. Dingell, Ranking Member, Committee on Energy and Commerce (Nov. 8, 2005), *available at* http://www.icann.org/en/biog/cerf.htm.

INTRODUCTION

We live in a new age of global communications. This technological age is now threatened by exaggerations that arise from fear of the unknown. What once was a free frontier of discovery has now become a source of contention. Governments around the world have continued to push toward greater surveillance in what should be an area of accessible knowledge. This recent governmental approach vis-à-vis the Internet is not only misguided, but also contrary to the values that supposedly guide democratic nations. This Article does not deny that threats exist in cyberspace, but it warns against fear-based actions that would encroach on the rights that human beings cherish. In particular, this Article observes that the regulation of the Internet must be aimed at the development of a cyberspace protected by governments, which must also maintain access to information for their citizens in light of a "world public order of human dignity," "one which approximates the optimum access by all human beings to all things they cherish."[2]

It is not irrelevant to point out that the Internet continues to be a vast frontier of information. The idea that it can be divided by virtual borders disregards the network's purpose and its value to society. "The benefits of the open and accessible Internet are nearly incalculable and their loss would wreak significant social and economic damage."[3] The Internet is of great significance at the international level because humanity has learned to appreciate the benefits of this technology, while also noticing the political challenges attached to it.

The nature of Cyberspace rests in its effective malleability, conceived of by the scientists and academics around the world that worked on its creation and made the decision to encourage the

---

[2] *See* W. Michael Reisman, Siegfried Wiessner & Andrew R. Willard, *The New Haven School: A Brief Introduction*, 32 YALE J. INT'L L. 575, 576 (2007) (defining "public order of human dignity" when discussing the New Haven School).

[3] Vinton Cerf, *Keep the Internet Open*, N.Y. TIMES (May 24, 2012), http://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html.

constant evolution of this medium.[4] Today, having sufficient access to the Internet's information has arguably become a prerequisite for the enjoyment of human life. The Internet has become a center for human literacy and has the potential to offer numerous kinds of instruction at lower costs and with higher quality than previous media could offer.[5]

This Article will argue that the concept of a "cybered Westphalian age,"[6] as a cure to all threats in the Internet, has the potential to do more harm than good. The international community is now faced with a possible policy shift from the current state of the Internet, which is one of shared knowledge, toward the active practice of censorship and filtered content, which will have devastating consequences.

The matter of alternative approaches to Internet regulation and the values surrounding human dignity brings the discussion back to the original consideration: the rights that human beings cherish. As has happened before in human history, when considering the benefits and threats found on the Internet, we are reminded that behind every new technology lurks someone's desire to exert control over it. Debates pertaining to the Internet, such as issues of personal privacy, equality of access, censorship, and computer crimes, center on the larger issue of control. There are no longer any doubts about the fact that whoever controls the Internet also controls access to information.

To see the Internet as something that must be controlled at any cost is self-defeating. Although there is a need for security measures in cyberspace, security ought to be achieved with due regard to the network's architecture and without destroying the openness obtained by the creators of the Internet.[7] Even though a

---

4 *See generally* KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE (2006) (telling the story of the inventors of the Internet).

5 *See* Frances Cairncross & Kaija Pöysti, *ICTs for Education and Building Human Capital*, *in* VISIONS OF THE INFORMATION SOCIETY (Lara Srivastava ed.), *available at* http://www.itu.int/osg/spu/visions/education/index.html (stating that many educators see the role of information and communications technologies as delivering a higher quality education at a lower cost).

6 S*ee* Chris C. Demchak & Peter Dombrowski, *Rise of a Cybered Westphalian Age*, STRATEGIC STUD. Q., Spring 2011, at 32, 32, 36–39.

7 *See generally* HAFNER & LYON, *supra* note 4.

growing number of nation-states are introducing content filtering,[8] excessive censorship of online content should not be seen as an exemplary practice now or in the future. The Internet has changed human history forever, and this technological marvel has brought challenges to recognized fundamental freedoms, the meaning of ethics, and human dignity.[9] Governments should not define their priorities based solely on the risks associated with cybercrime. Doing so would inevitably lead to a "fenced" cyberspace,[10] while ignoring the resulting harms of unequal access to information and undue surveillance.

This Article also argues that the historical importance of freely accessing information and the Roman legal concept of *jus gentium* may be used as signposts for the further development of cyberspace regulation. Instead of a "Westphalian" cyberspace order, an alternative regime is presented, one also originating from the core of international law but rooted in ancient times, rather than the beginning of the Age of Enlightenment.

The international law theory of *jus gentium* originated with the ancient Roman legal system, and it is based on the understanding that legal relationships and institutions are governed by a law common to all humanity.[11] This legal theory was revisited by legal scholars, who began to recognize the significance of the idea of "common good for the international legal order," particularly because this idea conceived of humanity as "a moral and political

---

[8] *See* Robert Faris & Nart Villeneuve, *Measuring Global Internet Filtering*, *in* ACCESS DENIED 5, 5 (Ronald Deibert, e.t. al. eds., 2008) (finding twenty-six of forty countries surveyed employed filtering and expecting that number to rise); s*ee also* ROBERT DEIBERT et al., ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE 3–15 (Ronald Deibert e.t. al. eds., 2010) (discussing the evolving scale of Internet filtering).

[9] Maud de Boer-Buquicchio, *Foreword* to DIVINA FRAU-MEIGS, MEDIA MATTERS IN THE CULTURAL CONTRADICTIONS OF THE INFORMATION SOCIETY—TOWARDS A HUMAN RIGHTS-BASED GOVERNANCE 5, 5 (2011).

[10] *See* Demchak & Dombrowski, *supra* note 6, at 32–35 (discussing the "fencing" of cyberspace in response to threats such as cybercrime).

[11] 1 R. W. DYSON, NATURAL LAW AND POLITICAL REALISM IN THE HISTORY OF POLITICAL THOUGHT, 127–28 (2005); *see also* DAVID J. BEDERMAN, INTERNATIONAL LAW IN ANTIQUITY 84–85 (2004).

entity, deducing therefrom certain basic obligations for States."[12] By 1749, it was argued that nation-states, bound together by nature, were required to maintain said bond.[13] The theologian St. Thomas Aquinas had identified Divine law within humanity, explaining that natural law represented how humanity took part of Divine Law.[14] As a result, St. Thomas Aquinas would have seen this bond among nation-states assured by Divine law. Hugo Grotius had already written about the law of all nations and its innate characteristic in every individual.[15] Grotius explained the law of all nations as the "law derived from nature, the common mother of us all, whose bounty falls on all, and whose sway extends over those who rule nations, and which is held most sacred by those who are most scrupulously just."[16] He inferred a characteristic of stewardship required of nations acting in trust for all humanity. Other writers moved their discussion to the human individual's rights and duties within the nation-state, and by 1754 *jus gentium* was also considered a "harmonizing process" between individuals and nation-states, providing a system of values in which peace was needed for their natural coexistence.[17]

Attempts to normalize the concept of a quasi-territorial delimitation of cyberspace will produce adverse results. A stronger case can be made that no territorially-based regime may be successfully applied to an aterritorial cyberspace.[18] Transboundary accord, based on the cultural common ground central to ancient legal and social philosophy, is better than a

---

12 Juliane Kokott & Frank Hoffmeister, *International Public Order*, *in* THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 2 (Heidelberg and Oxford Univ. Press 2013).

13 *Id*.

14 Thomas Aquinas, SUMMA THEOLOGICA, I-II, q. 91, art. 2–5 (Fathers of the English Dominican Province trans., Benziger Bros. 1947).

15 *See* HUGO GROTIUS, THE FREEDOM OF THE SEAS 5 (James Brown Scott ed., Ralph Van Deman Magoffin, Oxford University Press 1916).

16 *Id*.

17 Stephan Verosta, *History of International Law, 1648 to 1815*, *in* THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 62 (Heidelberg and Oxford Univ. Press 2013).

18 *See* David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367–76 (1996).

territorial regime for governance of the global phenomenon that is cyberspace.

There are noted national cyber-security interests that provoke the idea of reflecting the territorial mechanism of national self-defense within the "fifth battlefield" that is cyberspace in exactly the same way as in the other four fields of state confrontation.[19] But current international law analysis leaves much doubt as to the recognition of "digital territory" as an element of a state's national territory.[20] Such analysis makes it difficult to recognize most cyber-threats as attacks upon a state's territory, which would allow for self-defense and, what is more, the application of the appropriate law of war (*jus ad bellum*) mechanisms.[21] As a remedy, numerous legal scholars are attempting to introduce a plausible analogy that would apply territorially-based international law to aterritorial cyberspace.[22] One such recent attempt relies upon a direct analogy to one of the pillars of modern international law—the Westphalian order, which served as the stepping-stone for contemporary international law.[23]

I. ORIGINS OF THE SOVEREIGN NATION-STATES REGIME

All wars, whether in land, air, sea or cyberspace, spell certain doom. The era of the old kingdoms began its end on May 23, 1618 when Protestants from Bohemia threw two imperial governors from the window of the castle in Prague.[24] This marked the beginning of the Thirty Years' War.[25] This war, which involved both the Catholics and the Protestants, was a reflection of religious

---

[19] *See* Victoria Ekstedt, *Is the Swedish Territorial Defence Ordinance Applicable on the Fourth Arena?*, *in* 3RD INTERNATIONAL CONFERENCE ON CYBER CONFLICT 61, 61–68 (C. Czosseck, Ė. Tyugu & T. Wingfield eds. 2011), *available at* http://www.ccdcoe.org/publications/2011proceedings/2011_Proceedings.pdf.

[20] *Id*. at 65–66.

[21] *But see* Michael N. Schmitt, *Bellum Americanum Revisited: U.S. Security Strategy and the Jus ad Bellum*, 176 MIL. L. REV. 364, 415–20 (2003) (extending existing understandings of the application of *jus ad bellum* to cyber war).

[22] *See*, *e.g.*, Demchak & Dombrowski, *supra* note 6, at *32–35*.

[23] *Id*.

[24] GEOFFREY PARKER, THE THIRTY YEARS' WAR 48–49 (1987); C. V. WEDGWOOD, THE THIRTY YEARS WAR 12, 78–79 (1939).

[25] WEDGWOOD, *supra* note 24, at 12.

fanaticism and the ambitions of rulers.[26] The war involved kings, queens, the Holy Roman Emperor and the Pope.[27] The butchery and savagery of the Thirty Years' War were catastrophic and brought total misery, disease, famine, forced migration, devastated economies, and deaths that reduced the population of central Europe by one third.[28] The war (1618–1648) ended when European rulers agreed to a diplomatic solution.[29] It was in the year 1648 that a solution materialized with a series of treaties known as the Peace of Westphalia.[30] The peace process began in 1644 by representatives of nearly two hundred Catholic and Protestant rulers, camped in Münster and Osnabrück, in the northwestern German region of Westphalia.[31] The series of treaties, signed in Münster and Osnabrück, relied on a simple idea. Within the forum of a first ever diplomatic conference, sovereigns who had been fighting for three decades decided to recognize each other as equals, with equal rights and obligations resting upon each of them.[32] Thus the Westphalian concept of state sovereignty was born.

Most heads of states (i.e., sovereigns) agreed to govern the communities they led within certain territorial boundaries, as agreed upon in 1648.[33] Crucial for this accord was the issue of cultural values, as reflected in the religious beliefs underlying each of the communities. Protestants and Catholics were deemed equal, while Calvinism was legally recognized. In order to allow this peaceful coexistence to happen, the concept of "sovereign states"

---

26 CARL SAGAN, COSMOS 51 (Ballantine Books 1985) (1980).

27 1 THOMAS A. WALKER, A HISTORY OF THE LAW OF NATIONS, 147–48 (1899).

28 STROBE TALBOTT, THE GREAT EXPERIMENT: THE STORY OF ANCIENT EMPIRES, MODERN STATES, AND THE QUEST FOR A GLOBAL NATION 86 (2009).

29 *Id*. at 86–87.

30 WALKER, *supra* note 27, at 145–48.

31 TALBOTT, *supra* note 28 at 86.

32 Leo Gross, *The Peace of Westphalia, 1648–1948*, 42 AM. J. INT'L L. 20, 21–22, 40 (1948).

33 Stephen D. Krasner, *Compromising Westphalia*, 20 Int'l Security 115, 115 (1995); s*ee also* Jouni Häkli, *The Politics of Belonging: Complexities of Identity in the Catalan Borderlands*, 83 *GEOGRAFISKA ANNALER B : HUMAN GEOGRAPHY* 111, 112 (2001) (noting that it took France and Spain 11 more years to find a satisfying consensus, embodied within the Treaty of the Pyrenees of 1659).

was introduced.[34] The Westphalian accord allowed communities to be governed in accordance with the common interest of the state, understood as one separate and superior to those of the sovereign, the king or the community itself.[35] This idea was well reflected by the term "raison d'état" (national interest),[36] which sought, in part, to protect the overall interests of, say, the French state rather than those of the king or of the Catholic Church by finding "a mean between what conscience permits and affairs require."[37] Thus, state sovereignty meant that the nation-state interest, rather than religious or personal motives, was to be the guiding principle of all international relations.[38]

The Westphalian concept of sovereign states later developed into the sovereignty of "nation-states," laying the foundation for contemporary international relations. "Nation states" would be identified as communities formed by individuals with joint values, history and culture rather than solely by a single sovereign's exercise of power over a group of individuals, as was the case with "sovereign states."[39] The idea of "sovereign nation states," derived from the Westphalian order, required nation-states to coexist peacefully through allowing each community to exercise its common culture and beliefs, communicate in common languages and govern themselves in a way they found appropriate within certain territorial limits, as agreed upon by the nation-states.[40] It must be noted that the current evolution of international relations has led several political and legal writers to conclude that we are

---

34 *See* Juliane Kokott, States, Sovereign Equality, *in* THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 6 (Heidelberg and Oxford Univ. Press 2013).

35 *See* W. ANDY KNIGHT, A CHANGING UNITED NATIONS: MULTILATERAL EVOLUTION AND THE QUEST FOR GLOBAL GOVERNANCE 75–77 (2000). *See generally* Peace Treaty between the Holy Roman Emperor and the King of France and their respective Allies, the Avalon Project, Yale Law School, *available at* http://avalon.law.yale.edu/17th_century/westphal.asp.

36 *See generally* W.F. CHURCH, RICHELIEU AND REASON OF STATE (1973) (discussing the history and application of "raison d'état").

37 *Id*. at 168 (quoting Silhon).

38 *See id* at 171.

39 *See* J. Samuel Barkin & Bruce Cronin, *The State and the Nation: Changing Norms and the Rules of Sovereignty in International Relations*, 48 INT'L ORG. 107, 110 (1994).

40 See *id*. at 115–17.

experiencing the dusk of the Westphalian order.[41] Globalization and new media, as enabled primarily through the popularization of the global network, bringing instantaneous communication worldwide and promoting similar commercial and social trends all over the globe, clearly lead to the conclusion that a rigid Westphalian distinction among nations, communities and societies is no longer legitimate nor executable.[42] "Sovereignty"—a term crucial to the architecture of the Westphalian regime—is being substituted by its derivatives, such as "shared sovereignty," and amended to a much narrower scope with such international law instruments as peremptory norms or humanitarian intervention.[43] Therefore its re-introduction for the cyber-sphere seems particularly ill-suited.

II. ATERRITORIAL CYBERSPACE VS. WESTPHALIAN ORDER

The proposed legal concept of the "cybered Westphalian age" for the Internet is based on the perception that "no frontier lasts forever, and no freely occupied global commons extends endlessly where human societies are involved."[44] This concept is flawed for two main reasons: the analogy utilized is inaccurate, and its legal analysis is incomplete. The suggestion that a frontier must be subject to a limitative unit of measurement is a legacy of the old order of Westphalia. In our day and age, there are new frontiers that can be established and others that will never be crossed. For example, this "frontier" analogy cannot be easily applied to outer

---

41 *See* James A. Caporaso, *Changes in the Westphalian Order: Territory, Public Authority, and Sovereignty*, 2 *INT'L STUD. REV.*, 1 (2000); Mark Purcell, *Citizenship and the Right to the Global City: Reimagining the Capitalist World Order*, 27 INT'L J. URB. & REG'L RESEARCH 564, 571 (2003); John Gerard Ruggie, *Territoriality and Beyond: Problematizing Modernity in International Relations*, 47 INT'L ORG. 139, 139–40 (1993).

42 *See generally* Steven Wheatley, *Democratic Governance Beyond the State: The Legitimacy of Non-State Actors as Standard Setters*, *in* NON-STATE ACTORS AS STANDARD SETTERS 218 (2009) (explaining that in the realm of traditional sovereign law-making, international governance by non-state actors stands outside the Westphalian order). .

43 *See* Stephen D. Krasner, *The Case for Shared Sovereignty*, 16 J. DEMOCRACY 69, 70 (2005); Stephen D. Krasner, *The Hole in the Whole: Sovereignty, Shared Sovereignty, and International Law*, 25 MICH. J. INT'L L. 1075 (2004).

44 Demchak & Dombrowski, *supra* note 6, at *32*.

space.[45] Science has shown that the frontier of an infinite Universe may continue without end.[46] Indeed, the fact that we measure distances in outer space in billions of light years dwarfs any notion of a frontier, such as the American frontier, with recognized geographical limits. Similarly, any comparison of the Internet to the American frontier, as has been suggested,[47] would be too simplistic. On the other hand, the "cybered Westphalian age" proposition, as defined within the legal context of a frontier, is based on the idea that "good fences are erected to make good neighbors," even in cyberspace.[48] This premise ignores the value of the "global commons" recognized by legally designating regions of valuable resources as protected for the enjoyment of all peoples.[49] Outer space is an example.[50] Any model of governance designed to place national borders within the Internet only considers the practical aspects of governance, focuses too narrowly on the short-term, and fails to resolve the long-term conflict. While it is much easier to accept the benefits of "placing fences," the ultimate goal should be a promotion of the principles enshrined in natural law that direct governments to carefully study the benefits owed to humanity.

The ultimate benefits for humanity are clearly delineated in the Universal Declaration of Human Rights.[51] This declaration asserts that a new respect is needed to promote greater opportunities for humanity, by reshaping the classical nation-state sovereignty and focusing on developing a global society.[52] While the Internet must be understood as operating within the realities of our present legal world, existing positive laws must be formulated in accordance

---

45 *Cf.* FRANCIS LYALL & PAUL B. LARSEN, SPACE LAW: A TREATISE 164–65 (2009) (discussing the absurdity of having state sovereignty extend infinitely into space, pointing out the difficulty in establishing a border, and questioning whether a border is necessary).

46 *See generally* ARCHIVES OF THE UNIVERSE (MARCIA BARTUSIAK ed., 2004).

47 *See, e.g.*, DOROTHY E. DENNING & PETER J. DENNING, INTERNET BESIEGED, at vii (1997).

48 Demchak & Dombrowski, *supra* note 6, at 32.

49 *See* SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 1–2 (1998).

50 *Id.* at 1.

51 Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/(III) (Dec. 10, 1948).

52 *Id.*

with the ultimate benefit to humanity.[53] New laws are needed to promote greater opportunities for humanity, by stepping away from classical nation-state sovereignty and looking at developing a global public trust.[54]

Cyber attacks open up the nation-state to questions of state responsibility in international human rights law. The "cybered Westphalian age" proposition argues that cyberspace is experiencing the beginnings of an international "border-making process."[55] The fact that the Internet has experienced increased government activity seeking to "control access" or exert censorship, depending on the circumstances, including a rise of Internet filtering, does not necessarily reflect a positive exercise of sovereignty over the virtual world.[56] Government responses to cyber-attacks require a careful understanding of the attribution element and constant recognition that the Internet is a peaceful instrument of global communications.[57]

As the right to free expression is not imposed through a peremptory norm, restrictions thereto should only be introduced within the limits set out by international law. The U.N. Human Rights Council Resolution 12/16[58] on freedom of opinion and expression prohibits States Parties from imposing restrictions on the right to access and use information on the Internet. Nevertheless, it must be emphasized that actively protecting the right to free speech online might be somewhat of a challenge. The current procedures (international complaints procedure and special procedures) created within the United Nations for the protection of human rights are initiated in principle by the Human Rights

---

53 KEMAL BASLAR, THE CONCEPT OF THE COMMON HERITAGE OF MANKIND IN INTERNATIONAL LAW 21 (1998).

54 *Id*. at 371.

55 Demchak & Dombrowski, *supra* note 6, at 32.

56 *Id* at 47.

57 *See* Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 A.F. L. REV. 167, 205–06 (2012) (discussing what the author calls the "sixth element strategic initiative" and the importance of attributing a cyber-attack correctly).

58 Human Rights Council Res. 12/16, Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development, 12th Sess., Oct. 12, 2009, U.N. GAOR, A/HRC/RES/12/16, 5(p)(iii) (Oct. 12, 2009).

Council, which currently is dominated by African and Islamic countries,[59] which are often supported by Russia and China,[60] both of which restrict freedom of speech. In this context, the chance of obtaining international sanctioning authority for actions against extensive censorship practices appears slim. Without such authorization, any action aimed at those extensively limiting freedom of speech online would be deemed inconsistent with international law.

At the same time, one can identify a growing accord that excessive filtering is contrary to the globally agreed free speech standard, as per Article 19 of the Universal Declaration of Human Rights,[61] and discussions are being initiated to identify the details of that standard for the online environment. The Universal Declaration of Human Rights, which provides that "all human beings are born free and equal in dignity and rights,"[62] is the point of departure for Internet governance (IG). For example, the U.N. Human Rights Council's resolution on promotion, protection and enjoyment of human rights on the Internet was based, in part, on article 19 of the Universal Declaration of Human Rights.[63] Further, during the 2007 Internet Governance Forum in Brazil, the Council of Europe noted that "[f]reedom of expression and security on the Internet are not contradictory but complementing values in the information society."[64]

Proponents of a cybered Westphalian age argue, "As cyberspace is profoundly man-made, no impossible barriers hinder

---

[59] Robert Evans, U.N. Chief Tells Rights Body Drop Rhetoric, Blocs, REUTERS (Dec. 12, 2008, 2:27 PM), http://www.reuters.com/article/2008/12/12/us-un-rights-idUSTRE4BB67820081212; *see also Membership of the Human Rights Council*, OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS (OHCHR), http://www.ohchr.org/EN/HRBodies/HRC/Pages/Membership.aspx (last visited May 10, 2013) (listing the council's current membership).

[60] Evans, *supra* note 59.

[61] G.A. Res. 217 (III) A, *supra* note 51, art. 19.

[62] *Id.* art. 1.

[63] Human Rights Council Res. 20/8, The Promotion, Protection and Enjoyment of Human Rights on the Internet,20th Sess., June 29, 2012, U.N. Doc. A/HRC/20/L.13 (July 7, 2012).

[64] *Freedom of Expression and Security on the Internet*, UNESCO (Nov. 14, 2007), http://www.unesco.org/new/en/media-services/single-view/news/freedom_of_expression_and_security_on_the_internet-2.

the growth of national borders in cyberspace. They are possible technologically, comfortable psychologically, and manageable systematically and politically."[65] In spite of this, the recent report from the U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, contended that the Internet is key to the exercising of the right to freedom of opinion and expression, as guaranteed by article 19 of the Universal Declaration and the International Covenant on Civil and Political Rights (ICCPR).[66] The ICCPR states that the right to freedom of expression includes the freedom to receive and impart information of all kinds, regardless of frontiers, through any media of choice.[67] Human Rights Committee *General Comment 10* has emphasized the obligation of nations to protect the right to freedom of expression, which includes freedom to "impart information and ideas of all kinds," and the freedom to seek and receive them regardless of frontiers and the medium utilized.[68] A common understanding ought to be developed that filtering or privacy-limiting measures should be limited as potential violations of human rights, in particular the right to freedom of expression in the cyber-world.[69] It must be acknowledged that the right to freedom of opinion and expression functions as an "enabler" of other rights,

---

65 Demchak & Dombrowski, *supra* note 6, at 35.

66 *See* Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Key Trends and Challenges to the Right of all Individuals to Seek, Receive and Impart Information and Ideas of all Kinds Through the Internet*, Human Rights Council, U.N. Doc. A/HRC/17/27 (May 16, 2011) [hereinafter Report on Internet Freedom] (by Frank La Rue).

67 International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), art. 19(2), U.N. Doc. A/6316 (Dec. 16, 1966).

68 U.N. Human Rights Comm., CCPR General Comment No. 10: Freedom of Expression (Art. 19), 19th Sess. (June 29, 1983), *available at* http://www.unhchr.ch/tbs/doc.nsf/0/2bb2f14bf558182ac12563ed0048df17.

69 The right to access information is an essential element of the right to free speech. According to Article 19 of the Universal Declaration of Human Rights, the right of free expression consists of three constitutive elements: 1) the freedom to hold opinions without interference, 2) the right to receive information and ideas expressed by others and 3) the right to impart information and ideas. *See supra* note 51, art. 19. Freedom of speech, in all these respects, can be exercised, according to the cited document, through "any media and regardless of frontiers." *Id*. In the same way the freedom of speech is defined in hard documents of international law (i.e., Article 19 of the International Covenant on Civil and Political Rights). Report on Internet Freedom, *supra* 66, ¶ 20.

including the right to education necessary for the enjoyment of the benefits of scientific progress, as well as civil and political rights.[70]

To recognize the changing nature of the Internet, the Cybered Westphalian proponents chose the crossing of the Rubicon as a metaphor evoking Julius Caesar's famous river crossing on his way to Rome from Gaul.[71] For the proponents, the phrase "crossing the Rubicon" seems to mean a new historical landmark, and one pointing toward warfare.[72] The political landscape of the Roman Republic certainly changed after Julius Caesar crossed the Rubicon River with his army in 49 BCE.[73] The Cybered Westphalian proponents noted a change in the landscape of the Internet and compared it with the story of the Stuxnet worm attack, branded as the "modern" Rubicon.[74] But if the crossing of the Rubicon must be the metaphor, then the Stuxnet worm is not the other landmark that we must embrace. Certainly, the Stuxnet technological sophistication, although memorable, dwarfs in comparison with the events in Italy that would define human history for at least five hundred years.[75] But it is rather by opening the Internet forever that humanity will cross the Rubicon, by making the hard choices that will define our global civilization.

While the past reflects an image of a Westphalian model of multilateralism where the nation-state has enjoyed a privileged and unquestioned position, the present reminds of a rising model of governance—multistakeholderism. Multistakeholder systems take a step back and seek to improve an atmosphere of endless military conflicts, lack of educational opportunities, the disregard for human innovation, censorship, and other threats such as spam, phishing and DDoS attacks. These threats have damaged somewhat the credibility of the Internet as a platform for human development and have called into question governments' ability to protect the citizens they claim to protect.

---

70 Report on Internet Freedom, *supra* note 66, ¶ 22.

71 H. H. SCULLARD, FROM THE GRACCHI TO NERO: A HISTORY OF ROME FROM 133 B.C. TO A.D. 68, 121–22, 134–35 (2007).

72 Demchak & Dombrowski, *supra* note 6, at 32.

73 SCULLARD, *supra* note 71, at 121–22.

74 Demchak & Dombrowski, *supra* note 6, at 32.

75 SCULLARD, *supra* note 71, at 121–23.

The future, however, offers humanity a multistakeholder order rising to face new challenges and to open new opportunities. It is here that cyberspace encounters the reality of a new landscape in international law, requiring that as a process of decision and participation, not only nation-states, but now a much wider range of actors should require consideration.[76] Legal multistakeholder actors[77] exist as participants stemming from the analysis based on past decisions, while attempting to participate in the course of future decisions.[78] If history is to be utilized as a cyberspace analogy, then we must look toward ancient times for illumination. It was the Roman Empire that offered the world the foundations of the contemporary international legal regime, *jus gentium* (later developed into the law of the nations).[79]

III. CYBERSPACE AS A REGULATORY CHALLENGE

The wave of demonstrations in countries across the Middle East and North Africa in 2011 showed that the Internet now plays a mobilizing role in the population regarding "justice, equality, accountability and better respect for human rights."[80] It is here that we face the reality of a renewed international dimension where a much wider range of actors now have a voice within the decision-

---

[76] *Id* at 19 (Those actors "included national and international officials, the elites of non-governmental organizations running the gamut from those concerned with wealth through to those concerned with religious rectitude, transnational business entities, gangs and terrorists, and individuals.").

[77] The stakeholders represent the participants or actors in the Internet governance debate: governments, private sector, civil society, United Nations family agencies, and international organizations (NGOs).

[78] *See* W. Michael Reisman, *The Democratization of Contemporary International Law-Making Process and the Differentiation of Their Application, in* DEVELOPMENTS OF INTERNATIONAL LAW IN TREATY MAKING 15–19 (Rüdiguer Wolfrum & Volker Röben, eds. 2005).

[79] *See* MANFRED LACHS, THE TEACHER IN INTERNATIONAL LAW 39–44 (1987) (on *jus naturale* genesis). *See generally* Stanislas F. Belch, *Paulus Vladimiri and his Doctrine Concerning International Law and Politics*, 176 REVUE DE L'HISTOIRE DES RELIGIONS 225 (1969); LUDWIK EHRLICH, WORKS OF PAUL WLADIMIRI (1969); Mark Goldie, *Edmund Bohun and Ius Gentium in the Revolution Debate, 1689–1693*, 20 THE HIST. J. 569 (1977).

[80] Report on Internet Freedom, *supra* note 66, ¶ 2.

making process.[81] The legal power of the individual, enhanced by new communication technologies, has created the opportunity for meaningful individual participation in key aspects of international decisions, even where these individuals are not affiliated with governments.[82] By focusing on the "nation-state," the Cybered Westphalian approach is less likely to appreciate and more likely to interfere with the roles that are played by individuals and groups in the formation and continuation of the Internet governance process. Governments should avoid isolation and must strive for an international consensus of joint cooperation for the benefit of the "citizens" of the Internet. Governments must accept that the Internet is not a source in itself of "moral decline."[83] The main contours of contemporary societal confusion are based on "fears, which take form in dystopian rhetorics," bringing about moral panic "in which anxieties over uncontrollable social forces become the focus of efforts to understand a new cultural trend."[84] Indeed, good arguments support the view that the Universal Declaration of Human Rights has had a constitutional quality *ab initio*.[85] Human rights concepts may be identified within the Internet as a cultural necessity of progression toward a common good, and one that seeks out strategies to balance the weight of power while identifying greater degrees of participation within the decision-making process for all "citizens" of the Internet: the netizens.[86] As a result, the fraught relationship between national sovereignty interests and common practices of cyber-communities deserves to be analyzed through the prism of international law before the predictions of a cybered Internet can be fully validated. Therefore, it is the nation-state that ultimately must prove its legitimacy as the good steward and protector of the most interesting and sustained grand development of inspiration: the international law of the

---

81 *See* Reisman, *supra* note 78, at 19.

82 *See* Reisman, Wiessner & Willard, *supra* note 2.

83 *See* NANCY K. BAYM, PERSONAL CONNECTIONS IN THE DIGITAL AGE 41–44 (2010).

84 *Id*. at 41, 43.

85 *See* Hurst Hannum, *The Status of the Universal Declaration of Human Rights in National and International Law*, 25 Ga. J. Int'l & Comp. L. 287, 289–290 (1996).

86 The term introduced by Michael Hauben to describe an active participant of the global electronic exchange. *See* MICHAEL HAUBEN & RONDA HAUBEN, NETIZENS: ON THE HISTORY AND IMPACT OF USENET AND THE INTERNET (1997).

Internet. This law, one that must, as has been discussed, incorporate human dignity, "is surely inseparable from the question of what it is to be human."[87]

The netizen, it could be argued, exists in an environment that has witnessed the evolution of rules that continue to limit the old Westphalian order. To broaden the basis of the decision-making process within the Internet requires that netizens be given uninhibited control over their roles according to their responsibilities within the world community. Thus, the practical aspect of any new regime needs to be based on established legal practices of international relations that enshrine human dignity.

These factors, as well as the *sui generis* aspects of the Internet, were considered in the 1997 United States Supreme Court case of *Reno v. ACLU*, where the Court recognized the distinctiveness of the Internet as a structure that provides "a wide variety of communication and information retrieval methods."[88] The Court noted that all of these methods, taken as a whole, constituted a unique medium, known to its users as cyberspace, and "located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."[89] Two years later, the concept of cyberspace as a community was explored.[90] In this environment of netizens, cooperation has produced public goods that benefit the collective.[91] This new cyber-person, the netizen, has been represented by all stakeholder groups.[92] This cyber-environment acquired a new identity after the 2003 first phase of the World Summit on the Information Society, under the name of "the Information Society."[93] This environment is one of

---

87 *See* Jeff Malpas, *Human Dignity and Human Being, in* PERSPECTIVE ON HUMAN DIGNITY 19 (2007).

88 *Reno v. ACLU*, 521 U.S. 844, 851, 117 S. Ct. 2329, 2334 (1997).

89 *Id* at 851, 117 S. Ct. at 2334–35.

90 *See* Marc Smith & Peter Kollock, *Communities in Cyberspace, in* COMMUNITIES IN CYBERSPACE 16–18, (Marc Smith & Peter Kollock eds., 1999).

91 Peter Kollock, *The Economies of Online Cooperation: Gifts and Public Goods in Cyberspace, in* COMMUNITIES IN CYBERSPACE 225–31, (Marc Smith & Peter Kollock eds., 1999).

92 *See* Rolf Weber, *Accountability in Internet Governance*, 13 Int'l J. Comm. L. & Pol'y 152, 159 (2009).

93 *Id*.

unique properties and unique social relationships.[94] It is here that the netizens continue to explore this electronic frontier living by rough consensus and running code.[95] Indeed, it is a global social system of coexistence and interactions.[96]

The democratic ideals of cyber-communities are directly related to the realities of the legal order of the Internet. Without a doubt, open cyber-communities are likely to be extremely diverse, and it is within their own inner workings that the management of the Internet takes center stage.[97] The fact is that short of disconnecting a nation completely from the Internet, all other measures would fail to achieve an over-all defense without sacrificing the technological benefits owed to the people of the nation.

Yet, what is the purpose of any defensive policy? Should this policy be one where the nation-state agrees to subscribe to recognized precepts of international law, but later disregard them when faced with having to adjust its domestic law to be consistent with international law? The answer should be that any policy of national cybersecurity that claims legitimacy must first subscribe to international human rights standards, which possess a global quality empowered by natural law as the foundation of the human trait that continues to give international law its direct connection to the well-being of both the human person and the nation-state.[98] It is not surprising then that legitimacy is inextricably linked with power.[99]

For the nation-state, legitimacy is based on a system of asymmetric power, in which "the actions of those who rule are accepted voluntarily by those who are ruled because the latter are convinced that the actions of the former conform to pre-established

---

94 Hans Klein, *The Right to Political Participation and the Information Society*, in HUMAN RIGHTS IN THE GLOBAL INFORMATION SOCIETY 190 (Rikke Frank Jørgensen ed., 2006).

95 *Id*.

96 *Id*.

97 HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER 340 (2000).

98 *See* GROTIUS, *supra* note 15, at 53.

99 M. Patrick Cottrell, *Hope or Hype? Legitimacy and US Leadership in a Global Age*, 7 FOREIGN POLICY ANALYSIS 339 (2011).

norms."[100] Although it would be quite easy to visualize the Internet as a chaotic environment replete with visions of vandals and pirates, the truth is that the Internet is not as chaotic or as critically lawless as these visions would suggest. The impression that the threat to the nation-state is centralized in cyber-attacks is a fiction. The truth is that it is unscrupulous individuals serving their own interests that abuse the Internet and create the threats that need to be stopped. The truth is that cyberspace continues to operate as expected, first as a source of information, and second as a potential promoter of human dignity.[101] Cyberspace has its own set of rules and principles, in the majority of cases reflect the "real-life" laws. This phenomenon helps it to keep its integrity and coherence, although real-world rules often show to be insufficient, when confronted with the challenges posed by cyberspace. The majority of those challenges reflects the global system of human rights and underlines the urgent need for their efficient protection.[102]

The idea of the netizen is a direct consequence of the very nature of cyberspace. The Internet, being a network of peers, runs based on equal participation of all stakeholders.[103] This basic truth, recognized by the WSIS within its 2003 Declaration of Principles (item 17) is known at the principle of multistakeholderism.[104] WSIS defined it by confirming that "building an inclusive Information Society requires new forms of solidarity, partnership and cooperation among governments and other stakeholders (i.e., the private sector) civil society and international organizations."[105] Deriving from the WSIS declaration, the 2005 WSIS Tunis Agenda sets the stage for the creation of the Internet Governance Forum as "a new forum for

---

[100] *Id.* at 339–40.

[101] Report on Internet Freedom, *supra* note 66.

[102] *Id*.

[103] *See About the Internet Governance Forum*, INTERNET GOVERNANCE FORUM, http://www.intgovforum.org/cms/aboutigf (last visited April 16, 2013).

[104] WSIS, Geneva 2003, Declaration of Principles, U.N. Doc. WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003), *available at* http://www.itu.int/wsis/docs/geneva/official/dop.html.

[105] *Id*.

multi-stakeholder policy dialogue."[106] Today the principle of multistakeholderism may be defined as an equal involvement of all groups participating in the Internet's evolution: state authorities (whether acting directly or through intergovernmental organizations), individuals or organizations acting on behalf of the civil society, and last but not least the business sector (including not only the ICT sector but any other market segment).[107] The multi-stakeholder character of Internet governance makes it unique in the world of international relations. This basic characteristic determines any possible corresponding legal regulation. In the IG field it is no longer governments alone that have to come to a consensus. It is the nation-state engendered with authority, but tempered by responsibility, that must apply that authority holding in mind the best interests of humanity and without resort to any use of coercion.[108]

Multi-stakeholderism necessitates the re-composition of the stakeholders involved in the global consensus-seeking processes. Territoriality is no longer an issue nor can it serve as criteria for the composition of such stakeholder groups, unlike a shared opinion or agenda.[109] Cyberspace also allows for more versatile but equal participation. In the "real-world," two citizenships held simultaneously are usually considered more than enough, while in cyberspace the common standard is for all "netizens" to participate in numerous communities at the same time, fluctuating among and between them. Therefore, the nature of the cyber-realm is far different in its composition and governance regime than the traditional, historic political world-order decided upon in 1648.

The concept of replacing the global cyberspace with a web of small, well-guarded national networks seems appealing for a number of reasons. Not only might it enable more security, but it

---

[106] WSIS, Tunis 2005, Tunis Agenda for the Information Society, U.N. Doc. WSIS-05/TUNIS/DOC/6(Rev. 1)-E, item 72 (Nov. 18, 2005), *available at* http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

[107] The Tunis Agenda introduced the concept of the multi-stakeholder process as the future standard for Internet governance.

[108] *See* Harold D. Lasswell & Myres S. McDougal, Jurisprudence for a Free Society 1245 (1992).

[109] *See supra* note 78.

could also enable the more efficient enforcement of human rights. Human rights such as freedom of speech or privacy, although enshrined in numerous international documents and clarified in court decisions, still differ in application at the national legislative and judicial level. Ineffective international privacy protection, resulting from divergent interpretations of the content of the privacy right in various legal systems, points to the need to intensify international collaboration in times of global electronic exchange, which continuously expose new risks to privacy. Making cyberspace just one more element of national territory, guarded with (electronic) frontiers would allow exercise of those national human rights standards efficiently, and solve the growing problem of finding a global standard for free speech or online privacy. The challenge of successfully protecting individual privacy might serve to demonstrate the shortcoming of the cyber-Westphalian order.

The problem with privacy protection online is twofold. First, there is the abovementioned lack of a universal accord on the status of personal data protection. Since the scope of the right to privacy is primarily shaped by the acknowledged scope of protected personal data, the diverse status of privacy regimes in various jurisdictions leads to the actual ineffectiveness of any national or international personal data protection online because it may not be effectively exercised.[110] The second problem with protecting privacy online is the very definition of "privacy." Even the EU states, proud of their human right protection regime, find it difficult to define the scope of privacy protection when faced with such new challenges as the legal status of data presented by Google Street View or other geolocation data[111] and Google's possible legal responsibility in Europe for infringing users' privacy.

Introducing national, territorial jurisdiction over particular "spaces" in cyberspace would not only help solve those difficult

---

110 *See generally*, Frank La Rue, supra note 66.

111 *See* Data Protection Working Party, *Article 29: Opinion 13/2011 on Geolocation Services on Smart Mobile Devices*, 881/11/EN WP 185 (May 16, 2011), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

problems, but would also make the work of ISPs much easier. They would no longer have to make difficult decisions on their own company standards for protecting privacy of their users at a "sufficient" (from a legal and moral point of view, in the global context) level. All they would have to do would be to meet the national standards in "national" networks, a challenge international companies have successfully faced for decades in the "real" world, operating in multiple state territories through their branch offices.

What is wrong with this—optimistic, as it might seem—scenario? Cyber-balkanization is a term used to describe the process of the global network falling into a set of smaller, community-based groups of users. The Westphalian order for cyberspace proposes to make this process the official practice. The Westphalian order for cyberspace represents a point in Internet history of losing the freedom and interoperability of the information exchange, while gaining security of individual users—one granted by national laws of the state of their residence. National authorities would have the tools to effectively protect their residents' rights (e.g., privacy), but those residents would lose most of their freedom within the process.

What is however most problematic is that under a Westphalian regime the network would lose its interoperability. In the Westphalian cyber-world there no longer is a global "cloud" of information, only separate spaces guarded with electronic tools and governed by national laws. They are connected through narrow, scrupulously controlled "gates," where exchange of information takes place, just as is the case with traditional borders or postal packages today. The cyber-Westphalian era would take us back to a seventeenth century Internet. It would strip us of the very value of the information society we are now trying to protect, since there would no longer be a global space for intellectual exchange, despite allegedly offering a sense of security. Benjamin Franklin's thought rings true once more: "The man who trades freedom for security does not deserve nor will he ever receive either."[112] Should we give up the potential for free thought that the global

[112] Quote attributed to Benjamin Franklin, POOR RICHARD'S ALMANACK (1738).

information society provides us for a false pretense of "national" security, we are actually bound to lose both.

IV. A RECOMMENDATION: *JUS INTERNET*—THE *JUS GENTIUM* FOR CYBERSPACE

The assertion that territorial law does not fit the transnational nature of cyberspace is not new. In 1996, D. R. Johnson and D. G. Post stated that as a fact, traditional jurisdiction and democracy are not fit for regulating cyberspace.[113] They accurately noted that the Internet "radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules."[114] With their controversial observation they added to the rising wave of cyberspace law criticism.[115] Not discouraged, they amended their concept in a 1998 follow-up entitles "The New 'Civic Virtue' of the Internet."[116] They described a detailed proposal for governing the ungovernable—a deeply democratic "Complex Systems Model for the Governance of Cyberspace" based on a common "civic virtue,"[117] instead of using statutory law and territorial state jurisdiction for governing the transboundary and international cyberspace.[118] The model rose to the challenge posed by cyberspace by offering a new, tailor-made regulatory solution rather than an analogy-based application of traditional laws.[119]

---

113 *See generally supra* note 18.

114 *Id*. at 1370.

115 *See, e.g.*, Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207–08 (1996).

116 David R. Johnson & David G. Post, *The New "Civic Virtue" of the Internet; A Complex Systems Model for the Governance of Cyberspace, in* THE EMERGING INTERNET (C. Firestone ed., 1998), *available at* http://www.temple.edu/lawschool/dpost/Newcivicvirtue.html.

117 *Id.* They derive their concept from the idea of "civic virtue" underlying representative democracy. Paraphrasing Jeffrey Abramson, the authors conclude that the core of civic virtue is the ennobling of men and women, when included in democratic processes. Those men and women "(whether acting as voters or representatives) are . . . casting aside narrow, selfish, or factional interests and putting themselves in the special frame of mind known as 'good citizenship.'" *Id*.

118 *Id*.

119 *Id*.

Post and Johnson identified particular principles reflected in all online communities and recognized the legal and practical meaning of electronic (rather than physical) boundaries.[120] This combined legal and practical approach could help identify and separately govern "areas" of cyberspace. Such areas, "occupied" by cyber-communities, understood as groups of Internet users sharing common ethical standards, would resemble traditional societies in cyberspace.[121] Rather than seeking a universal compromise for a statutory law consensus, the authors offered "a form of civic virtue that can tolerate continuous conflict and can reside in the very architecture of a decentralized, diverse, complex adaptive system."[122] Values common to all the communities would constitute a narrow catalog of globally shared principles, created "from the bottom up."[123] Community members would be bound by the values shared by the individual online communities they decide to join, just as residents are obliged to respect the national laws of their countries of residence upon crossing a border.[124] Rules shared by all of the communities would then allow identification of a narrow set of characteristics defining the "civic virtue." Such set of standards, based on practical and applicable consensus, would be the foundation for online governance.

Critics, however, blamed the authors for lacking a sense of reality.[125] Post and Johnson argued that the system would work based solely on the internalization and legitimization of the values enshrined within the civic virtue.[126] They argued that once the governed accepted the values as their own (internalized them) and recognized them as law that rightfully could be enforced in the name of the community (legitimized them) the system would work.[127] The critics claimed there was no power, authority or motivation to safeguard the execution of these ethical principles,

120 *Id*.
121 *Id*.
122 *Id*.
123 *Id.*
124 *Id.*
125 *E.g.*, A. L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703, 709 (1998).
126 *See* Johnson & Post, *supra* note 116.
127 *Id*.

and therefore no possibility to raise them to the level of an efficiently working legal system.[128]

It would be difficult, one might admit, to conceive of online communities that could be governed by individuals so morally stringent as not to give into the temptations authority brings.[129] And the civic virtue concept partook of one crucial flaw—it was against the egotistic human nature. However, time brought a practical solution to this crucial challenge: the future brought the "hybrid economy." This concept is discussed in detail by Lawrence Lessig in his latest book, *Remix* (with a revealing subtitle: *Making Art and Commerce Thrive in the Hybrid Economy*),[130] and by Benkler[131] in *Wealth of Networks*.[132] Lessig argues that the hybrid economy is the economic model best suited to reflect current trends in global online interaction.[133] According to him, a hybrid economy combines elements of two well-established economic models: the commercial economy, which conceives of the value of goods or services only in terms of money, and the sharing economy, exemplified by love or friendship, invaluable in hard currency.[134] The originally dichotomous classification, where an individual relationship would be either commercial or sharing, was severely disrupted by the activities "netizens" undertook.[135] Online communities organized in ways completely foreign to the off-line reality.[136] Netizens "shared" their free time, knowledge, ideas, offered each other

---

128 *See, e.g.*, Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1200 (1998).

129 *See* KATHY BOWREY, LAW AND INTERNET CULTURES 24–31 (2005) (discussing the "mapping" of cybercommunities); *cf.* ROLF H. WEBER ET AL., SHAPING INTERNET GOVERNANCE 22 (Springer 2010) (pointing to the problem of "free riders" not ready and unwilling to collaborate on equal basis within the egalitarian society).

130 LAWRENCE LESSIG, REMIX: MAKING ART AND COMMERCE THRIVE IN THE HYBRID ECONOMY (2008).

131 Yochai Benkler, *Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production*, 114 YALE L.J. 273, 341 (2004).

132 YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006).

133 LESSIG, *supra* note 130, at 248–49, 294.

134 *Id.* at 118.

135 *See id.* at 177–85.

136 *See id.* at 225–26.

companionship and support—free of charge.[137] However, as time proved and experience showed, such free sharing also brought tremendous *commercial* success. Wikipedia and Linux, for example, were initiated by few enthusiasts with some free time and now are flourishing enterprises operating on hard currency. That's how a hybrid economy works.[138] It combines the uncombinable—what once was "sharing" could now be evaluated "commercially."

Benkler adds to this concept by redefining the role of price in a world ruled by a hybrid economy.[139] In sharing economies price does not play any part—that role had to be adopted by a different feature.[140] Deriving from his earlier work, in *Wealth of Networks*,[141] Benkler envisioned a new phase in social evolution: the era of network information economy, based upon what he calls "peer production."[142] The concept covers generating new resources, ones not calculable with money.[143] According to his diagnosis, peer production will soon rule world markets.[144] Benkler and Lessig argue that neither laws nor commercial barriers can halt this unfolding revolution.[145] As Lessig rightfully points out, the "past survives only if it can beat out the future."[146] As he goes on to reassume, national authorities and certain professional lobbies clinging to outdated legal concepts cannot succeed.[147] Not only because their demands are irrational, but mainly, because they're not pragmatic. Among those concepts, the reintroduction of territorial jurisdiction in cyberspace may be named. A similar notion seems noticeable in the new mapping of cyberspace provided for by David Post in his latest work.[148]

---

137 *See id*.

138 *See generally id.* at 226–49.

139 Benkler, *supra* note 131, at 275–76.

140 *See id*. at 282.

141 BENKLER, *supra* note 132.

142 Benkler, *supra* note 131, at 330–31, 334.

143 BENKLER, *supra* note 132, at 115–16.

144 *Id.* at 131.

145 *See, e.g.*, LESSIG, *supra* note 130 at 266–68 (discussing these limitations in copyright law).

146 *Id*. at 142.

147 *Id*.

148 *See* DAVID POST, IN SEARCH OF JEFFERSON'S MOOSE – NOTES ON THE STATE IN CYBERSPACE (2009).

Benkler rightfully points out that the goal of a contemporary government is to assess the needs of and values crucial to its community.[149] Since that community is reaching beyond state borders, corresponding solutions must be sought. In times of economic and cultural globalization it is necessary to look for global solutions, and one might be offered by looking into the ancient concept of universal *jus naturale*. It was thought of as combining rules and values recognized throughout all communities.[150] Benkler sees the era of globalization and peer production as a unique opportunity to reassess the values universally recognized.[151] This implication may be considered a reference to the turning point in international law history. As already mentioned, a hybrid economy covers both commercial and sharing economies. A mechanism best suited for governing it ought therefore to derive from two sets of values, specific to each of them respectively. Statutory law governs monetary exchange in commercial economies, while ethics and codes of conduct allow for the even operation of sharing economies. Since a hybrid economy comprises both, commercial and free, therefore both law and ethics respectively must be considered when drafting a regulatory standard for the hybrid economy in cyberspace. *Jus Internet* is just that proposal, realistically combining both the areas.

Jus Internet derives from Roman *jus gentium*, built upon values recognized by all people, originating from natural law (*jus naturale*).[152] Created as a fundamental framework, *jus gentium* was designed to govern interactions among and between individuals from numerous diverse provinces of the Roman Empire.[153] All inhabitants of the Roman Empire—much like all

---

149 *See generally* BENKLER, *supra* note 132.

150 *See, e.g.*, A. ARTHUR SCHILLER, ROMAN LAW: MECHANISMS OF DEVELOPMENT 560 (1978); Brian Tierney, *Vitoria and Suarez on* Ius Gentium, *Natural Law, and Custom*, *in* THE NATURE OF CUSTOMARY LAW 110–16 (Amanda Perreau-Saussine & James B. Murphy eds., 2007).

151 *See* Benkler, *supra* note 131, at 328.

152 Kokott & Hoffmeister, *supra* note 12, ¶ 2.

153 The principles of *jus gentium* were applied to relations between foreigners (ones not holding Roman citizenship) and Roman citizens. Roman citizens' interactions were regulated by the statutory law—*jus civile*. *See* Roderick A. Macdonald, *Metaphors of Multiplicity: Civil Society, Regimes and Legal Pluralism*, 15 Ariz. J. Int'l & Comp. L. 69, 74–75 (1998); *see also* Berta Esperanza Hernández-Truyol, *International Law, Human*

netizens—came from different cultural and historical backgrounds.[154] They had to coincide while entering economic transactions or otherwise interacting. *Jus gentium* served as a basic set of references for settling disputes arising out of such interactions.[155] The system relied on a basic, humane sense of justice and fairness.[156] Its theory derived from two values: trust (*fides)* and equity (*aequitas*).[157] When identifying particular norms two regulatory systems were evoked: *jus naturale* and religious law.[158] Initially *jus gentium* operated as a common custom, eventually taking on the role of binding customary law.[159] The general character of its norms and its versatile application brought it authority among various cultures and social systems.[160] Although the Roman Empire failed, *jus gentium* survived and evolved into the law of nations, known today as public international law.[161]

The *jus gentium* lesson may well be used for regulating the universal and heterogeneous cyberspace. One would need to start by identifying the principles recognized as common to all the

Rights, and Latcrit Theory: Civil and Political Rights—An Introduction, 28 U. Miami Inter-Am. L. Rev. 223, 227 n.17 (1997).

[154] Frederick Bird, *Moral Universals as Cultural Realities*, *in* ETHICAL UNIVERSALS IN INTERNATIONAL BUSINESS 97, 110 (F. Neil Brady ed., Springer-Verlag 1996).

[155] *See* Heinrich Rommen, DIE STAATSLEHRE DES FRANZ SUAREZ S.J. 275 (1926); DYSON & STIRK, *supra* note 11, at 127–30.

[156] See DYSON & STIRK, *supra* note 11, at 130.

[157] *See* Martin Josef Schermaier, Bona Fides *of Roman Contract Law*, *in* GOOD FAITH IN EUROPEAN CONTRACT LAW 63, 77 (Reinhard Zimmermann & Simon Whittaker eds., 2000); DYSON & STIRK, *supra* note 11, at 130–31; 1 COLEMAN PHILLIPSON, THE INTERNATIONAL LAW AND CUSTOM OF ANCIENT GREECE AND ROME 119–20 (MacMillan & Co. 1911).

[158] *See* BRIAN TIERNEY, THE IDEA OF NATURAL RIGHTS: STUDIES ON NATURAL RIGHTS, NATURAL LAW, AND CHURCH LAW 25–30, 51–55 (Wm. B. Eerdmans Publishing Co. 2001).

[159] *See* JAMES BROWN SCOTT, THE CATHOLIC CONCEPTION OF INTERNATIONAL LAW: FRANCISCO DE VITORIA, FOUNDER OF THE MODERN LAW OF NATIONS, FRANCISCO SUÁREZ, FOUNDER OF THE MODERN PHILOSOPHY OF LAW IN GENERAL AND IN PARTICULAR OF THE LAW OF NATIONS: A CRITICAL EXAMINATION AND A JUSTIFIED APPRECIATION 157–60 (1934).

[160] *See id.*

[161] On the evolution of *jus gentium*, see generally EHRLICH, *supra* note 79. On the *jus naturale* genesis, see generally LACHS, *supra* note 79, at 39–44; Goldie, *supra* note 79, at 569–86; Belch, *supra* note 79, at 225–27.

governed. Present day deliberations on what's fair and just, once upon a time the exclusive domain of religious law, are left to ethics.[162] Just as religious law was used to ascertain the contents of *jus naturale*, nowadays the very same set of values is the subject of the global human rights dispute, with the UDHR representing the current compromise on their scope.[163] An analysis of the rules and principles recognized by numerous multinational and multistakeholder cyber-communities could efficiently stimulate this difficult debate, taking the universal consensus embodied in the UDHR as its starting point. By identifying universal ethical standards and particularities unique to the cyber realm and common to all (cyber-) communities, a global consensus could be reached. This basic ethical standard could be considered a reflection of what Post and Johnson once called "civic virtue." With the development of a hybrid economy, the civic virtue concept would no longer seem utopian. Rather, the common goal, strived for by all the governed, would be that of the profits of peer production, whether monetary or not expressible through price. A practical example would be the current rivalry between Facebook and Google+, focused on attempting to attract forever more users with user-friendly privacy policies, regardless of the fact that the existing international privacy laws decrease economic efficiency.

A customary regulation for cyberspace could follow the trail set by the Roman *jus gentium*. Once a set of general principles was identified as having community acceptance and being obeyed as a common custom, it could be raised to the status of customary law, having legally binding power.[164] The crucial challenge to overcome would be rising to the multistakeholder model of Internet governance. International customary law would prove to be insufficient, as it binds only one of the three crucial groups of stakeholders shaping the way the Internet is governed: customary law would bind only governments as international law subjects,

---

[162] *See* Jochen von Bernstorff & Ingo Venzke, *Ethos, Ethics, and Morality in International Relations*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 1, ¶ 4 (Heidelberg and Oxford Univ. Press 2013).

[163] *See generally* OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, http://www.ohchr.org/EN/Pages/WelcomePage.aspx (last visited Apr. 7, 2013).

[164] *See* N. Sea Cont'l Shelf (Ger./Den.; Ger./Neth.), Judgment, 1969 I.C.J. 3 (Feb. 20).

disregarding business and the information society of users. Therefore the concept of *jus Internet* differs substantively from international customary law in one crucial aspect. According to the Statute of the International Court of Justice, international custom is defined as "evidence of a general practice accepted as law."[165] Therefore international customary law requires two elements to coexist. First there must be an international custom (Latin: "*usus*"), which describes the existence of a uniform practice of state authorities. For an international custom to become customary law, that practice must be accompanied by a conviction on the behalf of state authorities that the particular behavior—one depicted in the customary practice—is recognized by other states as possessing the force of law, an element described by the Latin term of "*opinio iuris*."[166] The current definition of international customary law leaves no room for considering the practice of individuals or non-state entities (such as Internet service providers) as constitutive of an international customary norm. What is required to assess the evolution of a customary practice is the activity on behalf of state authorities, including its executive, legislative or judicial organs. What is more, the "*opinio iuris*" element is assessed based on decisions of international courts, supported by the opinions of renowned legal scholars.[167] Also, this prerequisite is impossible to meet for common practice of cyber-communities.

For example, although few national court decisions may be identified when it comes to Creative Commons ("CC") licenses,[168] raising those national judicial examples to the rank of a possible international compromise on the copyright challenge in cyberspace

---

[165] Statute of the International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1055, 1060 [hereinafter I.C.J. Statute], *available at* http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0.

[166] *See* Malcolm N. Shaw, INTERNATIONAL LAW 58 (1997).

[167] I.C.J. Statute art. 38(1)(d), June 26, 1945, 59 Stat. 1055, 1060.

[168] *See, e.g.*, Lichôdmapwa v. L'asbl Festival de Theatre de Spa (Le Tribunal de Premiere Instance de Nivelles 2010) (Belg.), *available at* http://wiki.creativecommons.org/images/f/f6/2010-10-26_A%27cision-trib.-Nivelles-Lichodmapwa.pdf; Curry v. Audax (D. Ct. Amsterdam 2006), *available at* http://wiki.creativecommons.org/images/3/38/Curry-Audax-English.pdf; SGAE v. Fernández (Lower Ct. No. 6 Badajoz 2006) (Spain), *available at* http://wiki.creativecommons.org/images/0/03/Sentencia_metropoli.pdf.

would be too far-reaching. For one, international courts dealing with public international law are not in the position to assess the compromise on copyright protection proposed within the private law CC licenses. Therefore, the contemporary meaning of international customary law will not suffice to meet the needs of the global network of peers, as it does not include a mechanism to introduce the international peer-consensus into national legal systems. At the same time, national legal systems may only be shaped through international law consensus. The existing global consensus on forever more controversial ethical issues, reached within the fora of cyber-communities, must not be disregarded by the international community and ought to be introduced into the traditional international law system through soft-law instruments, such as recommendations or declarations, reflecting current developments.[169] For instance, child pornography was declared undesirable by the majority of cyber-communities, and privacy policies were introduced by world's largest ISPs in the absence of international consensus on the protection of personal data. Following this example, the international community should focus on identifying the consensus already achieved by cyber-communities and encourage states to introduce harmonized national legislations envisaging that consensus, rather than supporting states in their efforts to enforce forever more stringent regulations, efforts contrary to the transboundary nature of cyberspace, such as the stupendous fiasco of the Anti-Counterfeiting Trade Agreement (ACTA) treaty in Europe, opposed by netizens who took their online consensus onto the street of European capitals, cities and towns.[170]

While the contemporary mechanism of customary law has little to offer the cyberspace dilemma, the Roman analogy does. It offers a solution derived from individual practice and prospectively

[169] *See generally The Core International Human Rights Instruments and Their Monitoring Bodies*, OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, http://www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx (last visited May 13, 2013).

[170] *See* Kevin Rawlinson, *Controversial Anti-Counterfeiting Trade Agreement Proposals Rejected by European Parliament*, INDEPENDENT (July 4, 2012), http://www.independent.co.uk/news/uk/crime/controversial-anticounterfeiting-trade-agreement-proposals-rejected-by-european-parliament-7912065.html.

raises it to the rank of law, just as the Roman "ius" (as opposed to statutory "lex")[171] offered the possible codification of a custom exercised in private (peer-to-peer) relations. Mid-twentieth century scholarship identified the trend described above as "applied jurisprudence." Instead of introducing elaborate legal theories into regulatory acts and futilely attempting to execute them, Professor Sidney Post Simpson and Ruth Field proposed basing legal regulation on a thorough case-law study.[172] Recognizing the shortcoming of the argument that law enforcement is the sole explanation for why rules are obeyed and learning which methods worked best, they argued, would allow communities to propose more effective laws.[173]

The global challenges posed by transboundary and transnational cyberspace, reflecting all the dogmatic differences in national jurisprudence, make any dogmatic consensus unachievable. It is only through a thorough analysis of the *status quo* and a practical approach to problem solving that the current gridlock in Internet regulation may be solved. One of the most important considerations is the recognition of individuals and corporations as particular groups subject to international law with legal personality and limited yet existent authority to invoke the responsibility of other subjects of international law in the realm of human rights.[174] Any model proposed for the management of the Internet must acknowledge, for example, that civil society and businesses have made valuable contributions to the debate and require a share in the decision-making process. This is the true essence of an efficient model for the management of the Internet.

Cyberspace has shown that the traditional pattern of international lawmaking no longer suffices. Traditional diplomatic tools for settling international law challenges are too slow to meet

---

171 *See, e.g.*, Franz Wieacker, *Ius Civile und Lex Publica in der Römischen Frühzeit*, *in* FESTSCHRIFT FÜR HEINZ HÜBNER 357–76 (Heinz Hübner & Gottfried Baumgärtel eds., Walter de Gruyter & Co. 1984).

172 *See* Sidney Post Simpson & Ruth Field, *Social Engineering Through Law: The Need for a School of Applied Jurisprudence*, 22 N.Y.U. L.Q. REV. 145, 170–71 (1947).

173 *See id.* at 162.

174 *See* Alain Pellet, *The Definition of Responsibility in International Law*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 3, 5–7 (James Crawford, Alain Pellet, & Simon Olleson eds., 2010).

the demands of the age of cyberspace. At the same time, an international diplomatic consensus is not sufficient in the multistakeholder era of Internet governance. A new approach is needed. According to the *jus Internet* concept, the role of the national lawmaker would be limited to amending national regulations according to the consensus identified in international fora—to recognize, that is, the elements of international common practice as fitting with national laws.

The question of a forum appropriate for such consensus-seeking on standards common to all cyberspace remains open, although numerous options may be used: from the IGF, through Council of Europe Parliamentary Assembly, ITU, to the U.N. International Law Commission deliberating a set of Draft Articles on International Internet Law. The growing global trend of increasing involvement and influence of non-state actors on global politics is nowhere more blatant than in cyberspace.[175] Therefore the international community has no choice but to find a solution enabling non-state actors to join the negotiating table. While the role of nation-states would be to introduce appropriate national laws, non-state actors would take it upon themselves to introduce the resulting consensus through their terms of service or rules of conduct, enforced through declining to render their services to or blocking the IP addresses of notorious violators. The question of an appropriate consensus-seeking mechanism also remains open. One could opt for the traditional diplomatic tools, but for the reasons named above, one could also seek new democratic decision-making models. As already mentioned, without a doubt all known soft-law instruments should come into play. Deriving from the successful model of the large online community that is Wikipedia, Zittrain proposes a model of democracy altered to meet the particulars of cyber-communities—a "semiotic democracy."[176] It does not operate based on a simple majority of votes, but as a more elaborate scheme it values decisions based on the strongest,

[175] CHRISTOPHER T. MARSDEN, INTERNET CO-REGULATION: EUROPEAN LAW, REGULATORY GOVERNANCE AND LEGITIMACY IN CYBERSPACE 221–41 (2011).

[176] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 147 (2008).

most convincing arguments.[177] Arguments recognized and supported by the majority of the community should be acknowledged as the new community standards.[178]

Jus Internet offers an alternative to international custom, as evidence of a general practice accepted as law. International law in its present shape is non-binding to non-state actors. Introducing a system flexible enough to include willing participants from outside governmental circles would be to envision and to encourage the multistakeholder nature of the IG community. It would open up the possibility of introducing regulations directly within company terms of service or community internal rules. Rules constitutive of *jus Internet* would reflect the existing consensus among communities, both off and online.

Why should *jus Internet* work? For the same reason public international law does. It originates from a strong customary background (e.g., the evolution of the law of the sea or the law of treaties).[179] What is now a self-contained regime was once a diversified set of principles applied by sailors or diplomats respectively in their everyday endeavors. There are few theories as to why international law works. The prevailing one is quite simple: states observe international law because it pays off. *Pacta sunt servanda*, a principle fundamental to international law, encourages states to respect their obligations toward one another because that they can reasonably expect the same in return, granting the foreseeability of the other states' actions.[180] The same mechanism may be used for the global cyberspace. Trans-boundary communities and international companies have proven the common interest concept true online.[181] Wikipedia or Linux developers play by the community rules not in fear of sanctions but because of a chance to participate in something bigger. Their power is that of the group, while for that group to have this power, it needs to operate smoothly. That is achievable solely through

---

177 *Id*.

178 *Id*.

179 *See* Vienna Convention on Diplomatic Relations, Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95 (1961).

180 *See, e.g.*, Hans Wehberg, *Pacta Sunt Servanda*, 53 Am. J. Int'l L. 775 (1959).

181 *Cf*. ZITTRAIN, *supra* note 176, at 141.

setting solid foundations for collaboration: that means setting clear rules, principles and procedures. Just as is the case with international law, the process of setting such rules and procedures is never finished, but the more complete it is, the stronger the community.

Jus Internet includes two crucial elements of the global hybrid economy. It begins as a soft law proposal, operating on universal ethical standards common to netizens worldwide. Through judicial recognition as a part of codes of professional conduct or good will, it evolves into a legal model fit to meet the economic challenges inherent in peer-production. It offers the flexibility of ethical rules developed in a democratic process, built upon the "civic virtue" proposed by Post and Johnson. Yet it also reflects the needs of the commercial economy, providing a perspective of statutory law regulation—it could serve as the stepping-stone for a treaty-based regulation of cyberspace. The customary rules identified within *jus Internet* might serve as an element for building an Internet Framework Convention, putting cyberspace next to the open sea, outer space or natural environment—all initially regulated by international custom, and presently through self-contained treaty-based regimes. Thus, the community-based standard of *jus gentium* seems better fit to regulate the multi-national cyber-society than the nation-based Westphalian order. Even though the history of state sovereignty highlights the importance of nation-states as major global players, the Internet Governance rule[182] and international Internet law principle[183] of multistakeholderism renders it ill-suited for cyberspace regulation.

A global consensus on human rights is the contemporary core of *jus naturale*. UDHR is the stepping-stone for seeking this consensus. What is needed now are a thorough analysis of the human rights catalogue in its present state in light of cyber-activities currently practiced online, as well as a proposal of its possible application to netizens. Such efforts can be successfully

---

[182] See WSIS, supra note 106.

[183] *See* R. Uerpman-Wittzack, *Principles of International Internet Law*, 11 German L.J. 1245, 1245–47 (2010).

made by both the United Nations and NGOs.[184] The role of national authorities and governments would be to use their power to support the new (altered) protection standards. The analysis of the human rights catalogue online should be conducted by professionals with experience in the field—both legal and technical. The work provided by the United Nations Conference on the Law of the Sea (UNCLOS III) or the United Nations Convention on the Law of the Sea might serve as a good example of such a wide, multifaceted cooperation. At the same time, it is the role of the human rights organizations to actively participate in the debate and raise the awareness of governments and individuals on this crucial issue as soon as possible, and to use their experience to support the negotiating parties in the collaboration of drafting - a Human Rights On-Line Framework Convention.

CONCLUSION

The Westphalian order is ill-fitted for the cyberspace environment, given that this vast frontier is composed of peers, physically located within all geographical locations simultaneously, rather than a group of individuals (citizens), physically located within nation states. Therefore a sensible way of delimiting cyberspace—thus regulating and securing it—would be through its communities.[185] Current developments demonstrate that law, as a tool used by states to regulate individual behaviors, proves forever less competent to regulate online activities. Cyber communities successfully shape their internal relations with non-legal tools, such as codes of ethics, terms of use, and self-regulation.[186]

---

[184] *See* Human Rights Council Res. 20/8, supra note 63 (outlining the body's approach to promotion, protection and enjoyment of human rights on the Internet); *Internet Rights and Principles Charter*, INTERNET RIGHTS & PRINCIPLES COALITION, http://internetrightsandprinciples.org/wpcharter/ (last visited May 13, 2013) (demonstrating the successful efforts of the Internet Rights and Principles Dynamic Coalition with its Charter of Human Rights and Principles for the Internet and related 10 Rights and Principles for Internet Governance).

[185] *See generally* THE CYBERCULTURES READER (David Bell & Barbara M. Kennedy eds., 2000).

[186] *See, e.g.*, Paul Hoffman, *The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force*, IETF, http://www.ietf.org/tao.html (last visited Apr. 16, 2013)

The Internet as a community should be governed in light of a human dignity that appreciates the sum of all humanity and allows all to enjoy the wealth available to everyone.[187] Such a scenario ought not to be deemed a utopian one. The global cooperation achieved through pacific means is the leitmotif of Henry Kissinger's recent book.[188] In *On China*, he begins with a stunningly simple yet true recognition that neither of the contemporary (neither the U.S. nor China) superpowers are nation states.[189] They are conglomerates of multiple communities, nations, cultures, and values.[190] Yet it is through cooperation where possible and the continuous search of compromise that they manage to achieve world leadership.[191] Kissinger, an experienced and supreme diplomat, saw the future of international development not in the military confrontation of superpowers (as history witnessed on numerous occasions), but in a "Pacific Community"—an economic and political cooperation between the United States and China.[192] The pursuit of a compromise, intensified through commercial and economic competition, exchange of ideas and favors, will prove beneficial to both and will lead to a harmonization of joint values.[193] It is not through economic or political sanctions, nor through humanitarian interventions, that human rights recognition will be enforced worldwide. It is rather through dialogue and compromise. According to Kissinger, direct pressure on human rights issues

(showing important elements that could be incorporated into a future overall model of Internet governance). Although not suggested as an overall model for Internet governance, Avri Doria tapped into her expertise and knowledge to remind us of these guidelines. (Avri Doria was a member of the Working Group on Internet Governance, a civil society participant in the WSIS and was a Non-Commercial appointee to the GNSO council within ICANN. She served as chair of the GNSO council from 2007–2009.) *See* Avri Doria, *The IETF as a model for the IGF*, INTERNET GOVERNANCE FORUM, http://www.intgovforum.org/contributions/IETF-as-model.pdf (last visited Apr. 16, 2013).

187 *See* Reisman, Wiessner & Willard, *supra* note 2, at 576.

188 *See* HENRY KISSINGER, ON CHINA 527 (2011).

189 *Id*.

190 *Id*.

191 *Id*.

192 *Id*.

193 *Id*.

ought to be replaced with economic cooperation and subtle molding of Chinese policy.[194]

The hope of achieving a global common ground for human rights was also expressed by Rosalyn Higgins, the former President of the International Court of Justice.[195] Establishing the core of such a compromise may be done solely through an analysis of values common to the whole global community represented in modern-day cyberspace.[196] "Arguments about human uniqueness based on what computers can't do leave us vulnerable to technical progress and what clever engineers might come up with."[197] The true source of success lies on a borderless Internet where "the sum of all its parts" brings about valuable outcomes. The efforts of the Global Network Initiative show that the community no longer looks to states as the only capable and authorized entities to regulate the cyberspace and protect citizens.[198]

What is more, recent events in North Africa proved that cyberspace is an efficient tool to oppose state authorities, should individuals represented within cyber communities, find state actions too oppressive.[199] Therefore, aware of it or not, cyber communities (with or without the encouragement of governments) are defining the current shape of the human rights catalogue on their own. The existing international law regime obliges every nation state to promote and respect the observance of human rights

---

194 *Id.*

195 Rosalyn Higgins, Former President, International Court of Justice, speech presented at the American Association of International Law on International Law and the Human Condition (March 5, 2010), *available at* http://www.dailymotion.com/video/xhv1lr_rosalyn-higgins-on-international-law-and-the-human-condition_lifestyle.

196 First steps towards achieving that goal are being taken by different community groups. A recent example of a successful global cooperation would be that of the RIPE NCC community self-regulation done in cooperation with governments and enforcement agents. *See* Wout de Natris, *Internet and Self-Governance? An Example*, CIRCLEID (Sep. 13, 2011, 10:28 AM PDT), http://www.circleid.com/posts/internet_and_self_governance_an_example.

197 SHERRY TURKLE, THE SECOND SELF: COMPUTERS AND THE HUMAN SPIRIT 283 (20th ed. 2005).

198 *See generally* GLOBAL NETWORK INITIATIVE, http://www.globalnetworkinitiative.org (last visited Apr. 17, 2013).

199 *See, e.g.*, Bianca Bosker, *Despite Social Media Block, "Egypt" Surges On Twitter*, HUFFINGTON POST (May 25, 2011, 7:30 PM), http://www.huffingtonpost.com/2011/01/31/twitter-egypt-protests_n_816542.html.

and fundamental freedoms in accordance with the United Nations Charter. The aforementioned Human Rights Council resolution on freedom of expression (2009) (A/HRC/12/16) obliges states to respect the freedom of expression also when exercised through ICTs.[200] Recognizing the "importance of all forms of the media, including . . . the Internet," the resolution recognizes the rights enshrined in the ICCPR, including "the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds . . . through any other media of their choice."[201]

The current challenge of the international community is to identify the contents of human rights catalogue, and in particular the right to free speech, online. That challenge may be well-faced when the mechanism described as *jus Internet* is deployed. There is no doubt that it is the duty of all law-abiding nation states of our planet to avoid spreading fears in the name of righteousness. The application of a territorial legal instrument to assess the limits of human rights online (as pertaining to the Westphalian order) is bound to defeat the idea crucial not only to the composition of the global human rights catalogue, but also to the global network. In the end, the defense of human rights is not for the timid.

[200] Human Rights Council Res. 12/16, *supra* note 58.

[201] *Id*. at 2.