Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Cyberspace: A new branch of international customary law?

Paul Przemysław Polański *

Kozminski University, Warsaw, Poland

Keywords:
Cyberspace law
International customary law
Opinio juris
Evidence of custom
Spam
Security
Privacy
Harmful speech
Accessibility

A B S T R A C T

International relations between countries increasingly take place in cyberspace. From concerns about cyber security and Internet surveillance to privacy to harmful speech – state and non-state actors developed practices and normative conceptions that could be regarded as international customary law *in statu nascendi*. The aim of this contribution is to present arguments supporting the thesis that research concerning international law should be broadened to include cyberspace. Due to lack of treaty law in this area, one shall resort to a second source of international law, namely custom especially, as one eminent researcher has noted: 'there are still numerous branches of international law regulated by customary law, and still more important, new rules of that law are raising'. The article presents the theory of custom as a source of international law and methods of evidencing it in the context of cyberspace and then outlines areas where such norms could have developed and therefore could be used to settle disputes between states.

1. Introduction

We live in the era of global, technological revolutions. Almost 200 countries are these days connected through a truly global, ubiquitous computer network that has enabled unparalleled in history mass interaction more than a half of all inhabitants of the planet Earth.[1] These revolutions have transformed not only the lives of ordinary people, but have also affected the functioning of organizations of any size and complexity, including states. These shifts have taken place very quickly, have been impossible to forecast and have had a global effect.

Information technology has accelerated the pace of societal communication in a way that clearly sets it apart from societal revolts of the past. For instance, the rapid exchange of messages via mobile phones and social networks, such as Twitter turned out to be the key differentiating factor in the Arab Spring that led to the collapse of *ancien regimes* in North Africa. The *Wikileaks* scandal that revealed diplomatic cables of the US government has created tensions between many allies of the United States and sparked long lasting controversies between the advocates of the freedom of speech and the supporters of the right of privacy and secrecy. The impact of using public mailboxes for private affairs was a key argument in the recent presidential election in the US. The last example has only confirmed that the Internet and technologies that underlie its day-to-day operations are not bullet-proof and one can expect many other scandals of that type to take place in the not too distant future.

Author Information: PhD (Melbourne University), a lawyer and a computer scientist, Professor at Kozminski University, Warsaw, Poland and the President of FREE Foundation.

This article has been financed by NCN grant nr DEC- 2014/15/B/HS5/03138.

* Kozminski University, ul. Jagiellonska 59, Warsaw, Poland.
E-mail address: polanski@kozminski.edu.pl.

[1] In June 2016 3,675,824,813 people had access to the Internet (50.1% of all people on our planet) according http://www.internetworldstats.com/stats.htm, last access: 28.10.2016.

http://dx.doi.org/10.1016/j.clsr.2017.03.007
0267-3649/

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007

All these unforeseeable events have taken place in a virtual reality that has had a direct and long-lasting impact in the real world. Due to its inherently global nature one might have expected that cyberspace would be of importance to the doctrine of international law. Sadly, this is still not the case. International law has not yet developed to embrace this new phenomenon. Jurisprudence of the ICJ has been dominated by traditional topics, such as interpretation of treaties, territorial disputes between states or the use of force in international relations. It is not hard to understand the reasons for it. Despite efforts concerning establishment of the Internet governance, an international community has failed to develop a working international framework for the administration of the Internet, which continues to be under the control of the US government. There is a paucity of international treaties concerning cyberspace. Those that have entered into force, such as the Council of Europe Convention on Cybercrime, the UN Convention on the Use of Electronic Communications in International Contracting or the WIPO Treaties related to international protection of copyright have a very limited scope of application, few signatory states and their subject matter is rather vague and unappealing to international lawyers. Consequently, international customary law doctrine has not been yet developed in this field.

It is not hard though to imagine that international customs pertaining to cyberspace have already been formed but are yet to be uncovered.[2] Let us take the example of spam. Do states have the obligation to fight spam sent from its territories and refrain from sending it to other states? Nearly all states seem to fight the influx of unsolicited communication, which is sent without users' consent, contains "junky" content, is very hard to block and is often used in cyberattacks to undermine the security of the target information system. It should not be particularly demanding to find evidence suggesting a consistent states' practice with respect to blocking spam content and or to prove conviction of states representatives that blocking such messages reflects the consensus or *opinio juris* of the international community. If this hypothesis is true, one could speak of an example of international customary norm concerning cyberspace.

The aim of this paper is to put forward arguments supporting the thesis that research concerning international customary law shall be broadened to include cyberspace. As Wolfke noted, "there are still numerous branches of international law regulated by customary law, and still more important, new rules of that law are raising".[3] It is argued that the Internet such distinct branch of international law where new rules of customary law are raising, and where international relations between states, international organizations and individuals could be observed and learnt from a new perspective. As Hardy rightly stated in 1994: "Customs are developing in cyberspace as they might in any community, and rapid growth in computer communications suggests that there may be a great many such customs before long."[4]

2. The contentious nature of international custom

Before investigating potential cyberspace customs, the paper will examine the nature of international custom. It is widely regarded to be one of the oldest and most difficult problems in international law: "Their difficulty lies the intangibleness of custom, in the numerous factors coming into play, in the great number of various views, spread over the centuries, and in the resulting ambiguity of the terms involved.'[5] This observation has not lost its accuracy in modern times.

Despite its debatable nature custom remains a prominent source of international law, which could be easily proved thanks to the jurisprudence of both the new and old International Court of Justice. Even the latest judgments of the ICJ are filled with states' argumentation referencing customary international law, be it with respect to such diverse subject matters as interpretation of international treaties, maritime disputes or the use of force in international relations. For the sake of illustration let us briefly touch upon the latest judgment in the case of 17 March 2016 *Alleged Violations of Sovereign Rights and Maritime Spaces in the Caribbean Sea (Nicaragua v. Colombia)*. Here the ICJ reaffirmed that articles 31–33 of the Vienna Convention on Treaties reflect norms of international customary law.[6] In addition, both states made their substantive arguments with reference to specific norms of international customs. In this very dispute, Colombia claimed that it was entitled to a maritime zone, which is governed by customary international law and Nicaragua maintained that Columbia had breached its obligation not to use or threaten to use force under Article 2, paragraph 4, of the Charter of the United Nations and customary international law.[7] Clearly, customary international law continues to thrive in the 21st century, despite some authors declaring it to be dead or at least in a mortal crisis.[8]

Unlike in domestic legal systems where customary norms have been almost entirely eradicated by acts of sovereigns' representatives, international custom continues to play a crucial role in international law. The term itself has been defined in the Statute of the International Court of Justice in a manner that continues to divide scholars: "The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: (. . .) international

[2] See author's own work in this area: P. Polański, Customary law of the Internet, T.M.C Asser Press, the Hague 2007.

[3] K. Wolfke, Custom in Present International Law, Prace Wrocławskiego Towarzystwa Naukowego, Wroclaw 1964, p. 10.

[4] Hardy, I.T. (Summer 1994), The Proper Legal Regime For Cyberspace, p. 1010.

[5] K. Wolfke, Custom in Present International Law, Prace Wrocławskiego Towarzystwa Naukowego, Wroclaw 1964, p. 9.

[6] Citing earlier judgments, such as: Avena and other Mexican Nationals (Mexico v. United States of America), Judgment, I.C.J. Reports 2004 (I), p. 48, para. 83; LaGrand (Germany v. United States of America), Judgment, I.C.J. Reports 2001, p. 502, para. 101; Oil Platforms (Islamic Republic of Iran v. United States of America), Preliminary Objection, Judgment, I.C.J. Reports 1996 (II), p. 812, para. 23; Territorial Dispute (Libyan Arab Jamahiriya/Chad), Judgment, I.C.J. Reports 1994, p. 21, para. 41; Arbitral Award of 31 July 1989 (Guinea-Bissau v. Senegal), Judgment, I.C.J. Reports 1991, p. 70, para. 48.

[7] *Alleged Violations of Sovereign Rights and Maritime Spaces in the Caribbean Sea (Nicaragua v. Colombia)*, para. 35 and 75.

[8] G.J. Postema, *Custom in international law: a normative practice account* [in:] *The Nature of Customary law* [eds] A. Perreau-Saussine, J.B. Murphy, Cambridge 2007, p. 279.

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007

custom as evidence of general practice accepted as law."[9] Many authors have noticed the poor quality of Article 38's definition.[10] The redaction of this Article was criticised on a number of grounds. Firstly, many authors noticed poor logic of the definition as manifested by the observation that only general practice could serve as the evidence of custom.[11] Secondly, the ICJ cannot apply a custom, but only customary law.[12] Thirdly, the definition eliminated local or particular practices that are of importance in international law.[13] Finally yet importantly, the definition omits many peculiar features of international custom and does not require it to be old, moral or reasonable, consistent or universally accepted.[14]

Despite the criticism, the aforementioned definition has been widely accepted and there seems to exist a consensus among the majority of justices and scholars at least with respect to the fact that it distinguishes two elements of international custom: practice and its acceptance as law, also known as *opinio juris sive necessitatis*. Writers differ, however, with respect to nearly all possible modalities of these two constituting elements. Furthermore, views diverge even with respect to the very nature of custom, namely whether both aforementioned elements are indeed required or whether *usus* or *opinio juris* suffice alone to prove the existence of custom.[15]

2.1. *Material element*

Several aspects of the material element of custom have not been mentioned in its definition yet continue to be analyzed in legal jurisprudence. The notion of practice has been examined from the perspective of its duration, generality, consistency, persistent objections to it, morality, reasonableness as well as its semantic meaning. One must also underline the liberal tendency noted by many prominent scholars concerning requirements for the material element of custom, particularly a short period of time required for its formation or lack of need for absolute consistency of practice.[16]

The cornerstone of the material element is the notion of practice. Particularly with respect to states' practice one must try to draw a clear borderline between the actual conduct and mere verbal acts: "repeated verbal acts are also acts of conduct in their broad meaning and can give rise to international customs, but only to customs of making such declarations, etc., and not to customs of the conduct described in the content of the verbal acts."[17]

This narrow interpretation of the notion of practice is of significance to the proper analysis of the formation of customary norms in cyberspace. State officials use public websites or services, such as Twitter, repeatedly these days to communicate with the world and their statements are being momentarily echoed on social networks. There is such an overload of official and unofficial communication in cyberspace that it is easy to find contradictory pronouncements. Yet such analysis needs to be conducted and it seems to fit into the scope of work of the modern international lawyer. In our times, more than ever before, one must look for the evidence of customary norms in the actual conduct of states' representatives. One can clearly see the importance of this distinction particularly when applied to states' practices concerning the freedom of speech or information security and privacy in cyberspace, where as one might expect, states' conduct often collides with their official positions.

The notion of practice also embraces abstentions from acts. In such cases, states manifest their behaviour through conscious inactions, as might be the case with abstentions from hacking networks of other states or organizing cyberattacks. This example also demonstrates that a practice does not need to be entirely consistent to be regarded as customary. Dangerous cyberattacks do take place and might even endanger the critical industrial infrastructure of a given state, as was the case with the virus *Stuxnet*, which partially destroyed Iran's nuclear program by attacking controllers used to control centrifuges for separating nuclear material.[18] Such attacks might be attributed to one or more states but such incidental practices shall be regarded as exceptions to a general rule of customary nature that prohibits the use of malicious code against the infrastructure of another state or a private organization there localized.

Practice is widespread. Historically, two measures where used to assess this factor: the passage of time and its geographical scope. The time factor has gradually lost its significance that it enjoyed throughout history. In Middle Ages customs had to be practiced for 100 years before they could be recognized as binding legal rules[19], yet the 20th century brought technological revolutions that have liberalized the perspective of justices and scholars in this regard.

Already in the *North Sea Continental Shelf case* the ICJ pronounced that "the passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law."[20] Judge Tanaka went a step further and set the foreseeable time limit for the duration of

[9] See Art. 38 para. 1(b) in United Nations Conference on International Organization at San Francisco (26 June 1945), *Statute of the International Court of Justice*. A similar definition was included in the Statute of the Permanent Court of Justice, which was the predecessor of the International Court of Justice in the inter-war period.

[10] K. Wolfke, *Custom in Present International Law*, 1993, pp. 1–8 and the literature cited there. See also, e.g., Cheng, B. (1965), *United Nations Resolutions on Outer Space: 'Instant' International Customary law?*, p. 36.

[11] Kunz, J.L. (October 1953), *The nature of customary international law*, p. 664; Sőrensen, M. (1960), *Principes de droit international public: Cours général*, p. 35.

[12] Villiger, M.E. (1997), *Customary International Law and Treaties. A Manual on the Theory and Practice of the Interrelation of Sources*, p. 15.

[13] See classic *Asylum* case *(Columbia/Peru)* (1950); *Case Concerning Right of Passage Over Indian Territory (Portugal* v. *India)* (1960).

[14] Based on P. Polanski, Customary law of the Internet, The Hague 2007, p. 147.

[15] See e.g. G.J.H van Hoof, Chapter VI. Customary international law [in:] Rethinking the sources of international law, Deventer 1993.

[16] K. Wolfke, *Some persistent controversies regarding customary international law,* Netherlands Yearbook of International Law vol. XXIV – 1993 – p3. *Cf.* Hudson, M.O. (3 March 1950), *Article 24 of the Statute of the International Law Commission. Working Paper. Document A/CN.4/16*, p. 26.

[17] Wolfke, K. (1993), *Custom in Present International Law*, p. 42, citing Judge Radhabinod Pal.

[18] See, e.g. https://en.wikipedia.org/wiki/Stuxnet, last visit: 22.10.2016.

[19] Bouscaren, L.T. and Ellis, A.C. (1957), *Canon Law: A Text and Commentary*, pp. 40–41.

[20] *North Sea Continental Shelf (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands)* cases (1969) para. 74.

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007

custom: "the speedy tempo of present international life promoted by highly developed communication (. . .) had minimized the importance of the time factor and has made possible the acceleration of the formation of customary international law. What required a hundred years in former days now may require less than ten years."[21] The doctrine of 'instant custom' proposed by Cheng that preceded the aforementioned judgement of the ICJ went even further and prepared a ground for the relaxation of the examination of this element.[22] In fact, 'instant customary law' might be viewed as a concept, which is irreconcilable in itself, as customary law simply presupposes the existence of durable and not instantaneous *usus*.

Having said that, it is of no surprise that customary norms can be formed in the digital space. *Usus* in cyberspace can be established quickly as state agencies often adopt a uniform practice developed in a private sector to protect sensitive information or fight illegal content. Alternatively, as often is the case, governmental bodies employ private actors in order to assure the highest possible level of technological expertise. This practice might also swiftly evolve in the light of the changing technological landscape. The nexus between state actions and industry practice is stronger and more visible than in any traditional branch of international law.

One could therefore look at the element of duration from a different perspective and adopt more fine-grained measures to assess it. One approach when assessing the passage of time with respect to cyberspace norms would be to take not only the actual duration of a given practice, as measured in years or even months, but also its intensity. This could be evidenced by e.g. the number of downloads and installation of software packages, security or privacy settings or actions taken to block illegal content. One could take into account the volume of occurrences of a given practice within a unit of time, as evidenced in computer logs, expert databases or technology reports.[23]

For the sake of illustration, one could cite the example of international customs concerning the encryption of financial transactions, which has been almost universally adopted by financial institutions and governmental organizations as soon as the need for transmission of sensitive data over open networks became the norm. This usage evolved with time and currently the expected level of encryption is a lot higher than 10 to 20 years ago, but it is clear that the custom has been nearly universally accepted despite the lack of developed written laws in this area on international, regional or even national level. Over the past 20 years states have not been able or willing to define precisely what "secure" really means, and ineffective legislative efforts have been filled by common *usus* and a consensus that the current level of encryption is sufficient and shall be applied by every entity obliged to provide secure communication channel. Furthermore, one can measure and observe practices of this kind on a regular basis in cyberspace. This is also a distinct feature of research concerning Internet practices.

There are many other elements of the material element that deserve attention in the context of cyberspace. The doctrine of persistent objector, whether one could speak of regional customary norms in the global digital world or morality of practices, could be further discussed. However, such discussion would exceed the scope of this paper`.

2.2. *Opinio juris*

Most judges and scholars agree that one needs a method to differentiate between a mere habit and a legal duty. As Brierly puts it: "customary international law results from a general and consistent practice of states followed by them from a sense of legal obligation."[24] In the *North Sea Continental Shelf* case the Court ruled that:

> "Not only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it. The need for such a belief, i.e., the existence of a subjective element, is implicit in the very notion of the *opinio juris sive necessitatis*. The States concerned must therefore feel that they are conforming to what amounts to a legal obligation. The frequency, or even habitual character of the acts is not in itself enough. There are many international acts, e.g., in the field of ceremonial and protocol, which are performed almost invariably, but which are motivated only by considerations of courtesy, convenience or tradition, and not by any sense of legal duty." [25]

As in the case of the modalities subsisting in the material element, there are numerous views with respect to whether rules of international law can come into being solely on the basis of *opinio juris*. As Cheng puts it: "Not only is it unnecessary that the usage should be prolonged, but there need also be no usage at all in the sense of repeated practice, provided that the *opinio juris* of the states concerned can be clearly established. Consequently, international customary law has in reality only one constitutive element, the *opinio juris*."[26] Wolfke claimed that both elements are necessary but underlined the fact that one might "(. . .) speak of the fulfilment of the *opinio juris* in its traditional sense only when a custom already exists, and not during the process of its formation".[27] Van Hoff, in turn, argued that such "instant" rules are not the manifestation of custom, where the material element is simply necessary, but rather a new source of international law.[28] On the other hand, other authors, such as Kopelmanas, Kelsen, Guggenheim and Williams, played down the importance of *opinio juris*, arguing

[21] Judge Tanaka (1969), *Dissenting opinion of Judge Tanaka on Continental Shelf case*, p. 177.

[22] B. Cheng, "*United Nations Resolutions on Outer Space: 'Instant' International Customary Law?*", 5 *IJIL* (1965), p. 36.

[23] Based on P. Polanski, Customary law of the Internet, T.M.C Asser Press, The Hague 2007.

[24] Brierly, J. L. *The Law of Nations: An Introduction to the International Law of Peace*, 6th ed. Oxford; New York 1963. p. 59.

[25] See e.g. *North Sea Continental Shelf (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands) cases* (1969), p. 44, para. 77.

[26] B. Cheng, "*United Nations Resolutions on Outer Space: 'Instant' International Customary Law?*", 5 *IJIL* (1965), p. 36.

[27] K. Wolfke, *Some persistent controversies regarding customary international law, NYIL* vol. XXIV-1993, p. 5.

[28] G.J.H van Hoof, Rethinking the sources of international law, Deventer 1993, p. 86.

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007

that it was either superfluous, difficult to prove or simply unnecessary and therefore destined to be eliminated.

Leaving aside the doctrinal tensions concerning the nature of *opinio juris* one could argue that, given the fact that customary norms can be formed very quickly, or even instantaneously, it is this element that might become more important than the element of practice. The need for a belief that one is acting lawfully is of special relevance to these customary norms that consist of abstentions from acts. In fact, since there is no discernible material element, the proof of such negative custom may actually be tantamount to evidencing prevailing *opinio juris*. For instance, we may witness the formation of an entirely new set of norms concerning the rules of war in cyberspace in the near future. Even today, a consistent state practice with respect to cyberattacks would probably best be analyzed with reference to the immaterial element of custom, as states generally and consistently abstain from engaging in such acts.

3. The role of non-state actors

The next aspect worth examining deals with a question whose practice must be taken into account in order to establish the existence of customary law. It is beyond doubt that states and international organizations have traditionally been the sole actors in the law-making efforts of the international community, and therefore the formation of international customary law was only incidentally analyzed from the perspective of other potential stakeholders.

Not surprisingly, the question whether practice may emanate only from competent organs of state is also subject to doctrinal debate. Some authors maintain that only the conduct of states could be regarded as relevant for the formation of international customary law.[29] Others, on the other hand, have argued that that practice "may originate from other organs or even private persons: fishermen, for example, who by their conduct can contribute to the evolution of the customary law of the sea".[30]

This latter broader view is more universal and seems to have been confirmed within yet another branch of international law, namely humanitarian law. The study of 161 rules of customary humanitarian law[31] underlines the importance of researching the conduct of individuals, be it soldiers or civilians. In fact, the first area analyzed in the aforementioned study concerns the principle of distinction, which describes the customary norms relating to the distinction between civilians and combatants, civilian objects and military objectives, indiscriminate attacks, proportionality and precautions in and against attacks. One could therefore argue that, with the expansion of the doctrine of international law beyond states and international organizations, international custom has become a source of law in international relations involving ordinary individuals. As witnessed within the emergence of humanitarian international law, we may observe that the proliferation of customary norms in the sphere of global international relations is enabled by the Internet.

The positive answer to the question of whether practices of individuals and private entities in cyberspace can also be included in the analysis of future customary law of the Internet, is of great significance to this potentially new branch of international law. There are additional arguments in favour of such expansion. Firstly, the importance of states and traditional international organizations has been diminished in relation to rulemaking in cyberspace and been overshadowed by the power of private Internet intermediaries, such as Google, Facebook and Amazon. Secondly, the initial reluctance of traditional international organizations has led to the establishment of Internet self-regulatory, community-driven supranational bodies, such as W3C, IETF or ICANN that function outside the UN system. Yet these bodies oversee the functioning and further development of technical standards, without exercising actual control over the way digital content is transmitted globally. Last but not least, grassroots initiatives, such as the Open Source Movement and Creative Commons have created truly global communities of developers and artists. These folks create and distribute software and artwork based on self-developed and strictly adhered to copyright license models that often lead to results that are at odds with national copyright laws.

One must be mindful, however, of the fact that such expansion can lead to unexpected problems, particularly of an evidentiary nature. In the case of a conflict, the question is whose *usus* should be regarded as prevailing: that of individuals, private corporations or states? Furthermore, whose *opinio juris* should be regarded as authoritative? Is it only states that are capable of accepting a widespread practice as an international custom? Alternatively, could individuals or private entities object to such norms, acting as persistent objectors or perhaps as addressees of regional customary norms? States would probably prevail and enforce their *opinio juris*, but Internet communities have already demonstrated their uncanny ability to work around states' laws pertaining to cyberspace.

4. Evidentiary challenges

4.1. *Ways and means of evidencing international custom*

Evidencing international custom has proved to be just as challenging as reaching a consensus about its fundamental nature. Both *usus* and *opinio juris* are of a sociological and psychological pedigree. This makes international custom inherently difficult for justices and legal scholars to uncover, prove, classify and then re-examine again to test whether it continues to exist in its original form or no longer exists at all. In short, as Janis puts it: "the determination of customary international law is more of an art than a scientific method."[32]

[29] G.M. Danilenko, "The Theory of Customary International Law", 31 GYIL 1988, p. 21.

[30] K. Wolfke, *Some persistent controversies regarding customary international law, NYIL* vol. XXIV-1993, p. 4.

[31] Henckaerts, J.-M. and Doswald-Beck, L. (2005), *Customary International Humanitarian Law, 2 volumes, Volume I. Rules, Volume II. Practice (2 Parts)*. See also Henckaerts, J.-M. (March 2005), *Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict*.

[32] M. Janis, An introduction to International Law, 4th ed., New York 2003, p. 44.

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007

Historically, the following sources have been examined to determine the existence of international customs: texts of international instruments, decisions of international courts, decisions of national courts, national legislation, and diplomatic correspondence, opinions of national legal advisors and practice of international organizations.[33] Various digests of state practice often published for more than two centuries by some countries had to be analyzed. These sources continue to be made available in the on-line form today.[34] Modern research in customary international law continues to emphasize a variety sources of research, including treaties, state law, pronouncements of states, digests of state practice, the practice of international organizations, jurisprudence of international courts etc. The US restatement emphasizes pronouncements of states that undertake to state a rule of international law, when such pronouncements are not seriously challenged by other states.[35]

What might be striking to a social scientist is the lack of a well-defined methodology as to how to prove international custom or even a simplified classification of evidentiary methods concerning both elements of international custom. The collection of decisions of international and national courts on issues related to international law could be regarded, as Judge Hudson puts it, as: a "useful indication of *opinio juris* of States"[36]. However, one lacks a convincing and comprehensive methodology as to how to prove the existence of international custom.

The ICJ, in its jurisprudence, has rarely sought to define the proof of custom resorting to in-depth research covering separately state practice and *opinio juris*. In fact, justices have usually either (1) declared the existence of international custom (declarative approach) or (2) inferred its existence based on the evidence of state practice (inferential approach).[37] The declarative approach prevails and presupposes the existence of custom where the *opinio juris* is established. This approach is clearly visible in landmark cases of the ICJ, such as the 1986 Case Concerning Military and Paramilitary Activities in and Against Nicaragua (the Nicaragua case)[38] where the examination of the principle of non-use of force or self-defence was not accompanied by any attempt to analyze states' *usus* in these areas. On the other hand, the inferential approach, which examines states' practice and omits a separate proof of *opinio juris* is clearly demonstrated in the *Right of Passage* case[39], *S.S. Wimbledon* case[40], the *Nottebohm* case[41] and the *Fisheries Jurisdiction* case[42] where the psychological element was not proven.

Summarizing, the lack of uniformity concerning the proof of international custom could be regarded as the most striking challenge to the practicality of the dual theory of international custom in its prevailing form. Furthermore, the propensity of legal scholars to develop elaborate theories of international custom could be characterized as inversely proportionate to their efforts to improve ways and means of proving its existence. If one accepts the prevailing dual theory of international custom, then one must also realize that the proof of repetitive conduct of competent states' organs and the proof of psychological element ought to be – whenever possible – clearly separated, rather than declaring or inferring its existence from one of the elements.

4.2. *New possibilities concerning proof of* usus and opinio juris *in cyberspace*

The digital domain offers new opportunities for rethinking the approach to evidencing international customary norms. If one accepts the view of the necessity of clear and rigorous separation of evidentiary methods concerning *usus* and *opinio juris*, then cyberspace offers some unique opportunities to develop this concept further.

Firstly, examination of state practice could now embrace, not only digests of practice or official pronouncements, but also unofficial documentation that can be found in cyberspace. *YouTube* alone contains billions of videos that alone could serve as the monstrous database of evidence of state practice. There are numerous cyberspace resources which are distinct from official governmental websites and enable rich and in-depth analysis of state practice, such as social networks or information portals. Living in the age of *Wikileaks*, begs the question whether research on state practices could ignore diplomatic cables and other documents made available by Internet activists. These documents, however controversial, could shed new light on state practices and therefore inform international law scholars as to the real motives behind state actions or inactions.

Secondly, *usus* of states and non-state actors can be examined using in an entirely new methodology, not easily available in the offline world. New methods could include automatic and semi-automatic ways and means of establishing repetitive conduct. Examples are: *Web Server/Browser Analysis* (or Web Infrastructure Analysis), which aims at the identification of

[33] Hudson, M.O. (3 March 1950), Article 24 of the Statute of the International Law Commission. Working Paper. Document A/CN.4/16, pp. 26–30.

[34] See e.g. Digest of United States Practice in International Law available from 1989 in the digital form at: http://www.state.gov/s/l/c8183.htm, last access: 26.10.2016.

[35] §103 (2) (d) of the Restatement of the Law, Third, the Foreign Relations Law of the United States, St. Paul, Minn.: American Law Institute Publishers, 1987. See also e.g. S. Sahl, Researching Customary International Law, State Practice and the Pronouncements of States regarding International Law, June / July 2007, available at: http://www.nyulawglobal.org/globalex/Customary_International_Law.html#_edn1, last access: 26.10.2016.

[36] Hudson, M.O. (3 March 1950), p. 3.

[37] See, P. Polanski, Customary law of the Internet, p. 190.

[38] Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) (1986).

[39] *Case Concerning Right of Passage Over Indian Territory (Portugal* v. *India)* (1960), p. 40.

[40] *The S.S. 'Wimbledon'* (1923), para. 25, also noted by Kirgis, F.L.J. (1987), *Custom on a sliding scale*, p. 149.

[41] *Nottebohm* case *(Liechtenstein* v. *Guatemala)* (1955), paras. 22–23, also noted by Akehurst, M. (1974–1975), *Custom as a Source of International Law*, p. 32; Kirgis, F.L.J. (1987), *Custom on a sliding scale*, p. 149, citing Jenks, C.W. (1964), *The Prospects of International Adjudication*, pp. 253–258.

[42] *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights (Advisory Opinion)* (29 April 1999), paras. 24–26, also noted by Akehurst, M. (1974–1975), *Custom as a Source of International Law*, p. 32.

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007

common configuration and operation patterns of the Internet communication channel; *Website Traffic Analysis,* which refers to the establishment of habits of providing invisible information by web applications; *Developer Tools Analysis,* that seeks to establish common functionalities inside web development software and frameworks that 'force' a designer to accommodate given functionality in an end product.

Opinio juris, in turn, could go beyond well-known methods concerning the analysis of state digests or the jurisprudence of international courts and national courts. This would apply in cases involving international subject matter and embrace possibilities hidden in the open nature of resources available on the Internet. *Website Content Analysis* could be used to establish habits of providing certain kinds of visible information on the site and *Web Participants Opinion Poll* could help to gather evidence on the perceived legality or illegality of a practice in question.[43]

New methods could be developed that utilize powerful neural networks and other technological advances of artificial intelligence that have matured over last two decades. We are just beginning to see the potential impact of information technologies on analysis of large volumes of textual and non-textual data. The application of these methods might require the involvement of expert witnesses. However, if used with caution, these new methods could help to prove both the existence of new customs as well as help to broaden our understanding concerning the intricacies of traditional rules of international customary law. The abundance of information concerning state and non-state practice, if collected and examined methodically, could lead to the development of new, digital observatories of state practices, enabling legal scholars to gain insights into vast repositories of diverse customary norms over time.

4.3. *Evidencing cyberspace custom concerning prohibition of spam*

It is commonly understood these days that spam is not only a nuisance for individuals or an illustration of a privacy invasion but also a method used by malicious hackers to break into computer systems. Hackers use spam as a method of overflowing a target server with spam in order to weaken its security measures and break into the system. States have adopted a generally negative attitude towards the practice of sending spam, understood as an unsolicited communication via email or similar means of distant communication, which is difficult or impossible to block. However, there is no international agreement covering prohibition of spam[44] and therefore international custom seems to be the only source of law that can be applied.

In this very case, the psychological element could play a dominant role, as one deals with prohibitory custom. The negative *opinio juris* could be inferred, *inter alia*, from legislative acts adopted in the United States and the European Union, which have influenced statutory standards in other parts of the world. Both the US Communications Decency Act as well as EU directive 2002/58/EC on e-privacy, contain an outright prohibition of sending mails which disguise the identity of the sender. For instance, according to article 13(4) of the aforementioned directive, the practice of sending electronic mail for the purposes of direct marketing, which disguise or conceal the identity of the sender on whose behalf the communication is made, is prohibited.[45] This is because they do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene information requirements set out in Article 6 of E-commerce directive.

The evidence of state practice is a lot harder to gather because one is dealing with negative or prohibitory customs. Abstentions from an act are much harder to prove than in the case of states' actual conduct, which can be manifested by the actions of its representatives. Nevertheless, one can provide examples of states conduct resulting in the establishment of spamboxes or technologies aimed at blocking spam content flowing from other countries. Furthermore, establishment of special task forces could also be used as evidence of state practice aimed at fighting unwanted communication. Finally yet importantly, there are already court cases, which penalize this kind of behaviour.

One must also realize that there are states which are weak in controlling spam flowing from their territories. China, Russia and Ukraine are notorious places for organizations that launch spam attacks and even openly offer their services on a commercial basis.[46] In any case, it would be hard to classify these states as persistent objectors to customary norms prohibiting sending spam, due to the fact that these states officially support anti-spam policies; hence the element of *opinio juris* would be missing in this case.

Finally, spam is often understood broadly to embrace, not only communication that hides the identity of the sender, but also unsolicited commercial communication, which makes it clear who sent it or on whose behalf a given email was sent. In this very case, there are divergent practices among states, which make it hard to conclude that a custom has emerged. For instance, the EU directives 2000/31/EC on e-commerce and the aforementioned directive 2002/58/EC have adopted a mixed approach towards such communication and do not ban it outright. The US approach is even clearer and permits, in broad terms, this form of utilizing individual means of distant communication. Consequently, one can clearly differentiate this kind of practice from a global customary norm prohibiting sending spam *sensu stricte*.

[43] For more details, see P. Polanski, Customary law of the Internet, p. 254.

[44] The 2001 Budapest Convention on Cybercrime does not expressly address the problem of spam, although Articles 4 and 5 dealing with data and system interference respectively, could have addressed this problem in a much clearer manner.

[45] The amended version of this provision reads as follows: "In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited."

[46] Although the leading country in this domain is the United States. See https://www.spamhaus.org/statistics/countries/, 28.10.2016.

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007

5. New domains of international customary law?

In his earlier work on customary norms in cyberspace the author of this contribution has assembled a list of potential trade usages[47] that could form the basis for research into customary international rules for cyberspace. The following list was assembled from the perspective of trade usages visible in international e-commerce[48] and is therefore broad enough to cover areas of law traditionally foreign to international lawyers, such as copyright or contract law. However, many of them could also be observed in relations between states themselves, as well as between states and non-state actors:

- Freedom of registration of a domain name based on the first-in first-served principle.
- Obligation of an online business to support non-trivial username and password authentication.
- Obligation of an online business to support strong encryption of all web-based transactions.
- Obligation of an online business to deny a service if client's web browser does not support strong encryption.
- Obligation of an online business to automatically sign the user out if a web browser is not used for some time (timeout).
- Obligation of an online bank to use valid digital certificates issued by trusted authorities.
- Obligation of an online business to display steps that follow to conclude an electronic contract.
- Obligation of an online business to provide a means of identifying and correcting input errors.
- Obligation of an online business to summarise the transaction before accepting payment.
- Obligation of an online business to confirm an online order instantly and by electronic means.
- Obligation of an online business to refrain from sending spam.
- Right of search engines to block *spamdexed* websites.
- Obligation of an online business to enable closure of interactive advertising.
- Freedom of linking without authorisation to resources made available online.
- Right to copy certain online materials without permission (e.g. crawling).
- Right to explore user's behaviour.

This list is by no means exhaustive and, as one might expect, new customary norms are evolving. One must stress that the aforementioned rules are mostly trade usages, as they were uncovered in the process of examining non-state practices in relation to electronic commerce. However, some of them have potentially broader appeal and have, in all probability, been followed in the domain of international law. Of particular relevance would be potential international customs in the area of data security, privacy as well as harmful and accessible content. Therefore, the section below will attempt a brief examination of potential new domains of international customary law pertaining to relations between states and non-state actors in cyberspace.

5.1. *Cyber security*

One of the most important concerns of policymakers today are issues related to the security of communication and cyber terrorism. Since commercialization of the Internet historically preceded involvement of states in the regulatory efforts, non-state actors faced similar challenges and developed practices that gained widespread appeal. For instance, ensuring secrecy of transactions has been a largely unregulated area, yet banks and other financial institutions could not wait for governments to step in and take action and therefore, around 20 years ago, developed mechanisms ensuring confidentiality of communication. Wide adoption of standards, such as use of the Secure Sockets Layer, has been followed by other institutions, leading to the emergence of trade usages obliging service providers to adopt secure communication using strong encryption. Yet secrecy of communication is just one, albeit important, aspect of the complex world of cyber security.

It is hard to imagine that states would not adhere to such customary practices in their communication with other states or non-state actors. For instance, ensuring security of communication requires analysis that goes beyond traditional analysis of primary or secondary sources of law or state pronouncements. State officials rarely, if ever deal with such matters. The analysis of actual state practice would involve the technical analysis of configuration of servers in order to gain a better understanding how states secure the contents of their communication in cyberspace.[49] The topic is becoming increasingly important in the age of raging cyberwars that might not only influence results of elections in countries such as the United States, but also trigger the application of Article 5 of the North Atlantic Treaty[50].

Opinio juris of states could be sought in primary and secondary sources of law, although this area is not heavily

[47] P. Polański, *Customary law of the Internet*, T.M.C. Asser Press, The Hague 2007.

[48] See also P. Polanski, *Trade usages under the Electronic Communications Convention*, in *The United Nations Convention on the Use of Electronic Communications in International Contracts: An In-Depth Guide and Sourcebook*, A.H. Boss and W. Kilian, Editors. 2008, Wolters Kluwer International: AH Alphen aan den Rijn. s. 423–437.

[49] The 2001 Budapest Convention on Cybercrime has been drafted by the Council of Europe and entered into force in 2004. See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, last access: 26.10.2016.

[50] Art. 5 The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007

regulated. States usually expect an "appropriate level of security" leaving specialists some leeway in relation to filling this deliberate normative gap – a promising area in fact for the development of *consuetudo secundum legem*. Other aspects concerning security of Internet communication relevant to international lawyer would involve potential customary norms related to such issues as cyber espionage, hacking attacks against other governments or distributed denial of service attacks aimed at paralyzing victim's infrastructure. *Opinio juris* of states could be inferred from primary law sources, such as the Budapest Convention on Cybercrime[51], which is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with violations of network security and computer-related fraud.

5.2. *Privacy*

Privacy of communication in cyberspace continues to be one of the most important topics, not only for states and regional organizations, but also for non-state actors, particularly Internet users. Given the exponential rise in processing power of computer chips and the decreasing cost of storage devices, the possibilities for unrestrained data collection and analysis seems endless. We have entered into a new phase of the 'computer revolution', the age of 'Big Data', where vast amounts of data are being gathered, processed, combined and re-combined, leading to a serious threat to the privacy of individuals, including government officials, who are themselves just regular Internet users.

Research into state practices cover a broad spectrum of activities. These range from the permissibility of processing personal data overseas or acquisition of personal data concerning foreigners to technological concerns pertaining to the use of first-party and third-party cookies. Then there are other surveillance technologies such as drones, CCTV cameras or GPS, the use of unsolicited communication covering also political speech as well as anonymization and retention practices. This area is closely related to the aforementioned cyber security issue, particularly with respect to practices concerning data security breaches or ways and means of protecting personally identifiable data.

With respect to *opinio juris* the common point of departure could be the American FIPS principles, developed in the 1970-ies and the OECD guidelines formulated in the next decade, which paved the way for a more comprehensive regulation of privacy protection at least in the European Union. Today, differences in the approach of the Americans and Europeans towards privacy are probably one of the most hotly discussed topics in legal jurisprudence, yet one must acknowledge that, at least initially, the most basic principles were very similar. The entry into force of the new EU General Data Protection Regulation (GDPR)[52] is going to create even more divergence, yet other countries will follow either one or the other system. Some mutually working solutions will exist too, akin to the EU–US Privacy Shield Agreement – successor of the Safe Harbour Agreement – or Binding Corporate Rules or development of Standard Contractual Clauses. Consequently, in many areas a true *opinio juris* will be identifiable, as the aforementioned case on the prohibition of spam exemplifies.

Going forward, the area of privacy protection could become one of the major issues in international relations, particularly in the context of massive personal data leaks that pertain, not only to financial information, but also to health or insurance data. The global nature of computer networks and the relative ease of illegal data acquisition, or processing from the territory of another state, might stimulate at some point growing international tensions and disputes and therefore the doctrine of international law might seriously have to start thinking about developing some working solutions in this area.

5.3. *Harmful speech*

Illegal speech is one of the most controversial areas of international law, where it is very hard to come up with a universal set of norms that define what is allowed or alternatively what is forbidden. In fact, freedom of speech is of one of those grounds where limitations of international customary law can most easily be noticed. So much is dependent upon the cultural and religious background that it seems almost impossible to discern a global custom concerning the content of freedom of speech on the Net.

What in fact deserves particular attention is the special role played by Internet intermediaries in curbing illegal content. Many states have developed legal frameworks facilitating the management of illegal content and even set up specialized agencies to deal with the influx of illegal messages; but still a significant number of states have decided not to adopt any specific legal framework and instead rely on "general rules" in this regard. In a recently published report of the Swiss Institute of Comparative Law, commissioned by the Council of Europe, the authors mentioned the following European countries, which have not adopted any specific legal framework related to the Internet: Germany, Austria, the Netherlands, the United Kingdom, Ireland, Poland, the Czech Republic and Switzerland.[53] Countries that have adopted a specific legal framework concerning the Internet include Finland, France, Hungary, Portugal, Spain as well as the Russian Federation and Turkey. Other states, such as China, have even developed country-wide firewalls, such as the Great Firewall of China to control the information flow inside the country.[54]

Little international harmonization has been achieved in this area to date. The most important international instrument developed so far is the Council of Europe Convention on Cybercrime, which includes some provisions for dealing with

[51] Convention on Cybercrime signed in Budapest on 23 November 2001, ETS No.185.

[52] Regulation (EU) 2016/679.

[53] See, Swiss Institute of Comparative Law, Comparative Study on Blocking, Filtering and Take-down of illegal Internet content, p. ii of the Executive Summary, available at: https://www.coe.int/en/web/cybercrime/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet, last access: 24 August 2016.

[54] See the Golden Shield Project, which is a surveillance network aimed at controlling contents coming from other states. For an introduction, see: https://en.wikipedia.org/wiki/Golden_Shield_Project, last visit: 19.8.2016.

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007

harmful and illegal content.[55] Certain kinds of harmful content are more uniformly treated in the actual practices of states. In relation to child abuse material, terrorism, criminality (in particular, hate crimes) and national security, many states have adopted obligations to block such content immediately and without court order and in some jurisdictions even without the knowledge of the hosting service provider.[56] One could speak of *opinio juris* of the international community as to the need to block access to the aforementioned types of online content. Many countries also maintain a special blacklist registry, where blocked domain names are stored and regularly updated.

Infringements of intellectual property, privacy or defamation are treated less seriously and usually states either require a court order to effect the takedown of the content or provide procedures for 'notice-and-takedown'. [57] The US Millenium Copyright Act served as a blueprint for the development of such procedures in many states and not only in relation to infringements of intellectual property. The EU, however, has not followed this approach as Directive 2000/31/EC only 'encourages' Member States to adopt such procedures.

In reality therefore, Internet intermediaries, or companies operating on the Internet, whose services are being used by millions of Internet users, have played the greater role. These Internet intermediaries span a wide and diverse range of commercial organizations. These include Internet Service Providers (ISPs), who connect households and business premises to the Internet infrastructure, to information intermediaries, such as Google, Facebook or Twitter. There are vast numbers too of Internet companies of various sizes that handle user-generated content (e.g. blogs, discussion groups, web shops or auction sites with comment functionalities etc.). In August 2016, for example, it was reported that Twitter had blocked 360 thousands accounts for spreading terrorist-related content.[58]

Internet intermediaries operate in a largely unregulated sphere, although many states, including US and the EU states, have developed legal frameworks offering safe harbours to special categories of intermediaries, such as mere conduit, caching or hosting service providers. Therefore, many intermediaries act unilaterally and block content they consider to be illegal. Such voluntary blocking is problematic if it is carried without a legal basis as it raises due process concerns.[59] Such practices may lead to the so called "chilling effect" on the freedom of speech, particularly if a given jurisdiction makes the liability of hosting service providers dependent upon knowledge of the service provider.

In summary, there are some patterns emerging in this area at the international level that are worth closer examination. Of particular importance would be state practices concerning Internet intermediaries and their actual actions and inactions in this field, which might have far-reaching consequences upon international relations between states and non-state actors. In addition, although countries differ in their understanding of what can be expressed publicly and what not, they often undertake similar actions to fight illegal content. From this perspective one could research emerging state practices concerning the ways in which illegal content is being blocked. Furthermore, one could also consider the application, for example, of the doctrine of regional custom[60] to certain areas of freedom of speech and harmful content.

5.4. *Accessible content*

There are also less contentious areas where international consensus is growing as to content that all people should be able to access in cyberspace. The focus is upon the ability of all to read digital content, with a special focus on those with disabilities. As the founder of the World Wide Web observes: "The power of the Web is in its universality. Access by everyone regardless of disability is an essential aspect."[61] And indeed, the World Wide Web Consortium (W3C), which "(. . .) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards"[62], continues to develop technical norms and standards for making the content of websites accessible for people with disabilities.

Although "traditional" international organizations have made some effort in this area, imposing a general regulatory framework, the actual details were established many years ago by the W3C. It is worth underlying that W3C could be regarded as a modern type of international body, which consists of 430 member organizations. These include universities, governmental bodies and commercial entities, such as computer firms, publishers and non-for-profit organizations, but does not include states or international organizations composed of state representatives.

The departure point for *opinio juris* of states could be the UN Convention on the Rights of Persons with Disabilities, which obliges states: "(. . .) to take appropriate measures to ensure to persons with disabilities access, on an equal basis with others, to the physical environment, to transportation, to information and communications, including information and communications technologies and systems (. . .)."[63] Parties to the Treaty have agreed, in particular, to: "promote access for persons with disabilities to new information and communications technologies and systems, including the Internet and promote the design, development, production and distribution of accessible information and communications technologies and systems at an early stage, so that these technologies and

[55] See especially, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, which entered into force in 2006.

[56] The aforementioned report cited Greece, France, Portugal, the Russian Federation, Serbia and Turkey as the examples. One could also mention the EU states that implemented the directive 2011/93/EC on child pornography, OJ UE L 335, p.1.

[57] See the Report, p. III.

[58] https://www.theguardian.com/technology/2016/aug/18/twitter-suspends-accounts-terrorism-links-isis, last access: 19.08.2016.

[59] See Report, p. III–IV. The authors underline the importance of the assessment of the legal basis used for blocking websites under Article 10(2) ECHR.

[60] Prof. Wolfke used to call them "particular customary rules", See, Custom. . ., p. 84.

[61] https://www.w3.org/standards/webdesign/accessibility, last access: 17.9.2016.

[62] https://www.w3.org/Consortium/, last access: 17.9.2016.

[63] See art. 9(1).

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007

systems become accessible at minimum cost."[64] Furthermore, the EU is currently working on a new directive concerning accessibility and many states around the globe have enacted specific legal frameworks and case law in this area.

What needs researching is the state practice in relation to web accessibility. Here, of particular relevance to a researcher could be existing technologies that enable unobtrusive analysis of conformance of public websites with W3C standards. Again, this is a potentially fruitful area for the application of new methodologies of evidencing state practice.

6. Conclusion

International relations between states offer one of those rare cases where lack of clear sovereignty gives rise to a prominent role for customary international law. As a rule of thumb, the limitations of international treaties that bind only states that are parties thereto and their paucity with regard to the Internet, could mean that international custom potentially becomes a truly global source of law in cyberspace between states. This is especially so given that some states have adopted practices that might conceivably be characterized as customary international law *in statu nascendi*.

However, the doctrine of international public law has not yet endorsed this possibility. Reading textbooks on international public law does not create an impression that this area of law has attracted any degree of interest in rules pertaining to cyberspace. Yet in the past, international law has embraced technological revolutions that have led to the development of the customary law of the sea, air and cosmos.

This stagnation cries out for change. The Internet showed its darker side a long time ago and has led to tensions between the major economic powers in the world. These have accused each other of cyberattacks, espionage as well as the theft of intellectual property and trade secrets. Such disputes are not fundamentally different from traditional ICJ cases concerning violations of established principles of (customary) international law. Much needs to be done, therefore, in order to prepare the doctrine of international law as a mechanism for adjudicating such disputes. In particular, this is so with regard to improving research methods and opening legal education to these new aspects of international relations.

[64] See art. 9(2)(g) and (h).

Please cite this article in press as: Paul Przemysław Polański, Cyberspace: A new branch of international customary law?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.007