16th BILETA Annual Conference

April 9th - 10th, 2001.
University of Edinburgh, Scotland.

Internet Governance and Territoriality Nationalisation of Cyberspace.

WOLFRAM PROKSCH
(Vienna University of Technology, Austria)

E. SCHWEIGHOFER
(University of Vienna, Austria)

Presented by WOLFRAM PROKSCH

Abstract. *The existing border-less cyberspace is mainly the result of the open network architecture of IPv4. This structure does not obey principles of territorial jurisdiction of states. The Yahoo! case demonstrates needs of states and existing limits of IPv4. IPv6 offers extensive geographic tracking allowing a nationalisation of cyberspace. In the future, content filtering may be replaced by blocking of groups of users. As privacy and non-discrimination are endangered the final IPv6 should minimise negative effects but also jurisdictions should enhance the application of these principles of civil liberties in cyberspace.*

1 Introduction

Cyberspace - the present Internet -[1]constitutes a new (virtual) space for communication and action that knows - with the protocol IPv4 - no governmental boundaries [Fidler 1999, Grewlich 1999, Lloyd 1997]. This space can be used for communication, as a discussion forum, as a market place and for leisure activities. As many services have a very high part of information and communication, the Internet's new economy presents an attractive alternative to the old economy allowing essential cost cutting for services.[2]

"Internet Governance" is the technical, political and legal keyword [Ischii/Lutterbeck 1998] for the global coordination and regulation of critical Internet infrastructure functions. Internet as a global information and communication network is logically linked together by its common protocols and i.e. its unique address-space. Main tasks of Internet governance therefore are the administration of the IP-address-space and the root server system, the DNS, the development and implementation of new protocols and applications.

The massive growth of the Internet is causing problems of address depletion and routing information. Besides solving these technical questions, IPv6 will offer various types of addresses, including geographic based addresses. This paper will deal with the question, whether the next generation protocols and applications might facilitate mapping, the implementation of virtual borders and especially if geographic based unicast addresses may offer the possibility of a nationalisation of cyberspace. As *Lessig* [Lessig 1999] has rightly stressed the code of the software will largely determine the cyberspace. At the moment, law-makers and courts have not discussed their needs for a more efficient cyberspace governance of states from a technical point of view. Recent developments in the European Union (e.g. the E-Commerce Directive) focus the principle of establishment or place of residence. Whereas in "Real World" the states attempt to maintain sovereignty over their territory, the Internet is regarded as border-less and therefore seems to threaten sovereignty. Our territorial based constitutional states and legal systems undoubtfully have certain problems to execute their country-specific laws in the global Internet. Monitoring, surveillance or questions of proof will be very facilitated if a geographic based unicast address is available. Strict governance of states with a less liberal and democratic approach will get a strong impetus.

2 Territoriality and Cyberspace Regulation

The Federal Networking Council (FNC) issued 1995 the following definition of the term "Internet"[3]:*"Internet" refers to the global information system that -- (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol / Internet Protocol*[4] *(TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein."* The American Supreme Court classified the Internet as *"a unique and wholly new medium of worldwide communication.* [...] *Taken together, these tools [email, mailing list servers, newsgroups, chat rooms, World Wide Web] constitute a unique new medium - known to its users as "cyberspace" - located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet." Menthe* [Menthe 1998] already tried to define the "Internet" or comparable nets as virtual spaces, that should be treated like other international spaces (the Antarctica, the universe or the oceans).

However, it seems helpful to distinguish the "Real World", the physical network "Internet" - consisting of its cables and satellite-mains connected to backbones and local networks - and finally the "Cyberspace" as the virtual space where people meet, things are happening and actions are taken - a virtual location for real conversation, connections and exchange just as for (cyber-) crime and war. Real world space is subdivided by topography, man-made architectonical and political borders whereas cyberspace seems to be border-less - arising from the open network architecture of the Internet and its unique, common address space. Communication in the virtual space is completely independent of physical location, there are no territorially-based boundaries. The location within cyberspace consists only of the IP-addresses of the computers in physical network. The transmission of messages and information within the Internet is fast and at low cost; the routing of data does not underlie geographical rules but follows computer-network-logic.

Up till now the globality and border-less-ness of cyberspace has raised a lot of political and legal questions - especially in the field of conflict of law, execution of (national) law, law enforcement and the regulation of cyberspace in general. As *D. Johnson* and *D. Post* [Johnson/Post 1996a, Johnson/Post 1996b] put it best, "*cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location."* They argue i.e. that the rise of the global computer network is destroying the link between geographical location and the power of local governments to assert control over online behaviour, the effects of online behaviour on individuals or things, the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena and finally the ability of physical location to give notice of which sets of rules apply. In the last couple of years, various theories have been developed, if and how cyberspace should be regulated and governed. However, undoubtfully cyberspace already is regulated by national laws, supranational rules and international aggreements, the mechanisms of the market, self-regulation and de-fact-rules - and finally and especially by software code: According to *L. Lessig* [Lessig 1999, 30] "*the nature of the Net is set in part by its architecture"*. Code is law - software not only makes cyberspace what it is but also regulates cyberspace as it is. Technology does not need to be free of values and definitely is able to design and structure real space - virtual spaces seemingly even more effective.

3 Public International Law and the Internet

As the Internet forms an international space for information, communication, markets and services, the question of the future administration *(Internet governance)* is an evidently important one. *"Governance is the sum of the many ways individuals and institutions, public and private, manage their common affairs. It is the continuing process through which conflicting or diverse interests may be accommodated and cooperative action may be taken. It includes formal institutions and regimes empowered to enforce compliance, as well as informal arrangements that people and institutions have agreed to or perceive to be their interest."*[5]

If one would follow traditional approaches of public international law [Brownlie 1998], the solution of Internet governance would be an international treaty establishing an international governmental organisation. However, it will not come to this. The strong role of universities and civil society in establishing the Internet has paved the way for a new form of multi-level governance [Engel 1999, Grewlich 1999].

The well-founded analysis of *Perritt jr.* [Perritt 1998, Perritt 2000] shows that Internet will change the concept of sovereignty of states. The role of territorial sovereignty will be reduced leaving space for a more liberal approach.

The Westphalian system of realism sees states as territorial powers with sovereignty. Now, the steady concentration of power in the hands of states is over [Mathews 1997]. The absolutes of the Westphalian system have to be adjusted to a system of sharing powers with international organisations, citizens' groups of the civil society, especially non-governmental organisations (NGOs) and transnational corporations (TNCs). Even in large states, not everything of value lies within its state's borders. The single authority governing each territory and representing it outside its borders - the government of the state - has to address strong interference in resources and things that matter, including money, information, pollution, culture or leisure activities. To cut oneself off the practice of other states, becomes more and more difficult or even impossible. "Sovereignty, the power of a nation to stop others from interfering in its internal affairs, is rapidly eroding" [Wriston 1997]. However, the state's central task of assuring internal and external security is the least affected. Territorial regulation will remain a central component of Internet governance with problematic of inevitable spillover effects [Goldsmith 1998].

Liberal internationalists still see a need for international rules and institutions [Slaughter 1995, Slaughter 1997]. Characteristics of this model are the strengthening of law both at the national one as at the international level, peaceful settlement of disputes, a stabilisation of the role of non-governmental actors in the international relations and the stress of collective security and other forms of multilateral safety. Man and not the state is in the centre of international relations giving space to self-regulation that is facilitated and supported by states. This new transnational order in characterised by increased international networking of persons, private organisations, commercial enterprises and various entities of government [Slaughter 1995]. The enhanced communication of government institutions of different states leads to a new form of mutual work-sharing and support in regulation. The liberal model supports the self-regulation of citizens in the international space of the Internet.

The new medievalism [Mathews 1997] of a dissolving state and evolving importance of local government, transnational, regional and global entities may miss the point that private power cannot substitute the still very important role of the territorial state for maintenance of law and order. The power shift to non-state actors does not necessarily imply a loss of power for the state [Slaughter 1997].

In the very end of quality of governance and sanctions for violations of rules, the role of territorial state is still indispensable. The functions of adjudication and execution of the state are also required in this cyberspace. Concepts of a special cyberspace jurisdiction [Johnson/Post 1997, Reidenberg 1997] miss the central function of the territorial state as a entity assuring internal and external security but also extend the concept of space in a problematic way. The important criteria of "being away" from a space is not met if a person crosses the password border into cyberspace.

In cyberspace and Internet, states, international organisations, local government, transnational corporations, groups of the civil society, especially non-governmental international organisations, have to co-operate in a new form of multi-level governance. At the moment we are in a very interesting but painful process of readjusting principles of territorial sovereignty, conflict of laws and self-regulation for cyberspace (see for an overview [Grewlich 1999]).

Technical questions are solved in international law in the same way as in national or supranational law. The standard setting is left to standardisation bodies but maybe with a stronger role for the standardisation bodies like ITU, IETF and W3C.[6] Therefore, standardisation of the framework for code but also the implementation of the standards as code remains a very important task for the practical life of the Internet. As standardisation in IETF, the most relevant body for IPv6, is concerned, it seems to be blurred with code development. Regulatory constraints may not work properly. The standard IPv4 and its code has disregarded national borders. *Lessig* [Lessig 1999] phrased this fact properly: "Code as code!". *Lessig* also warned of the danger of a change of this code if civil society and states do not follow and developments very closely and use the regulatory power to interfere in case of undesired developments.

4 Implementation of Borders in Cyberspace

Recent developments in cyberspace regulation seem to attempt the creation of virtual borders within the existing IPv4 structure. The allocation of IPv4-address space originally was managed directly by the IANA. Later, blocks of the address space were allocated to the three registries RIPE-NCC, ARIN and APNIC to manage regional areas of the world. RFC 791[7]
(Sep. 1981) determines that the address space under of Internet Protocol version 4 (IPv4) is subdivided in three network classes[8] (A, B and C). Class A and B network numbers are a limited resource. Therefore, allocations of this space are restricted and class A network address blocks are mainly reserved for the IANA and determined organisations and networks (see RFC 1466 for these allocations)[9]. IPv4 addresses are allocated to networks and providers. Therefore, high-level routers can attribute an IPv4 address to a particular provider or network. Given the fact that the first choice will be a local provider Internet users can be localised to a certain degree. However, the circumvention of today's virtual borders is still possible depending on technical knowledge of anonymising and cost-factor (e.g. dial-up connection to the Internet via notebook or cellular phone to a foreign provider). It should be noted, that many IP addresses in today's Internet are assigned statically for some time in fixed connections environments (e.g., corporations, campuses, etc.). Even with the DHCP (Dynamic Host Configuration Protocol)[10], clients end up using the same address

for weeks to months. The same problem exists with always-on connections (e.g. cable modems, ISDN, DSL, etc.). Therefore, various suppliers[11]already offer methods and applications for the localization and identification of users. Other tracking devices like cookies also can help to identify the Internet user.

A good example of geographic tracking and its future risks is given with the French Yahoo! case [Lischka 2000]. On November 20, 2000, the *Tribunal de Grande Instance de Paris* has confirmed its decision of May 22, 2000 that Yahoo! has to block all French citizens from auctions of Nazi memorabilia at the US-Yahoo-auction-sites. Such auctions are allowed in the USA but illegal in France. The compliance with this judgement depends strongly on technical possibilities of geographic tracking. Expert witnesses stressed that blocking of users is possible but accuracy is limited to about 80% for France. Circumvention is quite easy by using an anonymizer[12]or techniques like tunnelling, or by signing up for AOL or other foreign providers. Therefore, besides Yahoo!'s willingness to comply loop-holes of compliance will remain. The Yahoo! case shows the very high interest of law-makers and courts in attribution of web-sites and users to a jurisdiction.

5 IPv6: Geographic Based Unicast Addresses

As the Internet has grown it became apparent that the existing version of IP - IPv4 - is inadequate to meet the need of IP addresses for networked devices [Stallings 2000]. Other reasons may be scaling problems, the routing information problem. Besides fulfilling the need for IP addresses and offering *Quality of Service*, IPv6 (or IPng [Internet Protocol next generation]) provides very interesting possibilities of geographic tracking. IPv6 addresses will have no classes. This function will be fulfilled by the subdivision of the address space based on prefixes similiar to IPv4. IPv6 defines three types of addresses. The unicast address is assigned to a single interface. The anycast address and multicast address are given to a group of interfaces. The difference lies in the fact that the anycast address allows addressing of the nearest interface with that address. Different from IPv4, the unicast address should be very stable for a particular user even if the provider or location is changed. Two prefixes are of special interest here: provider based unicast address and the geographic based unicast address. The provider based unicast address contains the entire functionality of IPv4's classes of addresses (A, B and C). The geographic unicast addresses should be able to show where the user is physically. Both prefixes have obvious advantages in routing. The geographic unicast addresses are not yet defined. The basis might be the ISO 3166-1 list but with a much higher granularity (e.g. regions or even mobil phone cells). No indications exist that the geographic unicast addresses may not be linked to jurisdictions. The cyberspace will be subdivided into jurisdictions. A nationalisation of cyberspace will be the result.

Besides evident routing improvements, privacy on the Internet will change dramatically. Jurisdictions, organisations and companies will be able to locate any user very easily. Monitoring and profiling of user activities will reach now unknown accuracy. It will be a new task for law-makers and courts to set limits for these kind of activities. As space is limited in this paper, we can address only some principles of constraints. The principle of privacy and data protection should be mentioned first. Users should be allowed to use dynamic unicast addresses or anonymizers. Strict constraints should be put on the generation and storage of user profiles. Non-discrimination of users will become a very important principle. Access to essential facilities and information will be endangered if available blocking possibilities could be arbitrarily used. The best example of the change of law enforcement will be the shift from content filtering to the blocking of groups of users, especially minors.

6 Present Implementation of IPv6 and the Role of ICANN

At the moment, the deployment of the IPv6 address system is still at a very early stage. The move from test installations to applications depends on interesting applications using the capabilities of IPv6 [Durand 2001]. Changes have to be carried out very carefully in order to keep the Internet in a stable condition.

ICANN [Schweighofer 2000] has the technical responsibility for the move from IPv4 to IPv6. Therefore, ICANN has created an ad hoc group to study and report on requirements for future numbering policies. The objective of the ad hoc group is to identify issues and problems of relevance to future policy in the area of addressing and numbering. (http://www.icann.org/committees/adhoc/index.htm). A draft concluding report has been published and posted by *T. Holmes* and *M. McFadden* (http://www.cix.org/adhocfinal.doc). The ad hoc group submitted the following proposal to the ICANN Board meeting in Melbourne in March 2001: *"... ICANN should continue to seek assurance, and regularly test, that the goals set for the Address Supporting Organisation when it was originally conceived, are fully met within the existing arrangement."* Summarising the report, the demand for a migration from IPv4 to IPv6 is not very strong for the time being given the still existing numbering resources of IPv4 and the high costs. A killer application cannot be seen for the moment.

In standard setting for IPv6, ICANN's ASO or PSO are not active at the moment. It is still the task of one member of the Supporting Organisation PSO, the Internet Engineering Task Force (IETF). In IETF, strong concerns exist on these problems of privacy (RFC 3041). ICANN should carefully analyse these discussions before the final IPv6 will be decided.

7 Conclusions

The existing border-less cyberspace is mainly the result of the open network architecture of IPv4. This structure does not obey principles of territorial jurisdiction of states. The Yahoo! case demonstrates needs of states and existing limits if IPv4. IPv6 offers extensive geographic tracking allowing a nationalisation of cyberspace. In the future, content filtering may be replaced by blocking of groups of users. As privacy and non-discrimination are endangered the final IPv6 should minimise negative effects but also jurisdictions should enhance the application of these principles of civil liberties in cyberspace.

References

BROWNLIE, I. (1998): Principles of Public International Law, Fifth Edition, Oxford University Press, Oxford

DURAND, A. (2001): Deploying IPv6, in: IEEE Internet Computing, pp. 79-81

ENGEL, CH. (1999): The Internet and the Nation State, Preprints of the Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter, Bonn, http://www.mpp-rdg.mpg.de/pdf_dat/engel1.pdf.

FIDLER, D. P. (1999): The Rule of Law in the Era of Globalization, in: JGLS, vol. 6, pp. 421-424.

GOLDSMITH, J. L. (1998): The Internet and the Abiding Significance of Territorial Sovereinty, Indiana JGLS, Vol 5, pp. 475-492

GREWLICH, K. W. (1999): Governance in "Cyberspace", Access and Public Interest in Global Communications, Kluwer Law International, The Hague.

ISCHII, K.; LUTTERBECK, B. (1998) ITR2 - Internet Governance als ein neuer politischer, rechtlicher und informatischer Grundbegriff, http://www.ig.cs.tu-berlin.de/s98/1332l506/vl02.html

JOHNSON, D. R./ POST, D. G. (1997): The Rise of Law on the Global Network, in: Kahin, B. and Nesson, Ch. (Ed), Borders in Cyberspace, Information Policy and the Global Information Infrastructure, The MIT Press, Cambridge, MA, pp. 3-47.

JOHNSON, D./POST, D. (1996a): Law and Borders - The Rise of Law in Cyberspace, http://www.cli.org/X0025_LBFIN.html

JOHNSON, D./POST, D. (1996b): And How shall the Net be Governed? A Mediation on Relative Virtues of Decentralized, Emergent Law**,** http://www.cli.org/emdraft.html

KLEINWäCHTER, W. (2000): ICANN between technical mandate and political challenges, in: Telecommunications Policy, pp. 553-563.

LESSIG, L. (1999): Code and other laws of cyberspace, Basic Books, New York, NY.

LISCHKA, K. (2000) Zensur und Werbung, in Telepolis, magazin der netzkultur, online available under http://www.heise.de/tp/deutsch/inhalte/te/4349/1.html

LLOYD, I. (1997): Information Technology Law, Second Edition, Butterworths, London.

MATHEWS, J. T. (1997): Power Shift, in: Foreign Affairs, vol. 76, no. 1, pp. 50-66.

MENTHE, D. (1998) Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Technology Law Review Vol. 4 Iss 3, http://www.mttlr.org/volfour/menthe.html

PERRITT JR., H. H. (1998): The Internet as a Threat to Sovereignty: Thoughts on the Internet's Role in Strengthening National and Global Governance, in: GLSJ, Vol 5, http://www.law.indiana.edu/glsj/vol5/no2/4perrit.html.

REIDENBERG, J. R. (1997): Governing Networks and Rule-Making in Cyberspace, in: Kahin, B. and Nesson, Ch. (Ed), Borders in Cyberspace, Information Policy and the Global Information Infrastructure, The MIT Press, Cambridge, MA, pp. 84-105.

SCHWEIGHOFER, E. (2000): Wer reguliert das Internet, in: Medien und Recht, pp. 347-355

SLAUGHTER, A.-M. (1995): International Law in a World of Liberal States, in: EJIL, vol. 6, pp. 503-538.

SLAUGHTER, A.-M. (1997): The Real New World Order, in: Foreign Affairs, vol. 76, no. 5, pp. 183-197.

WRISTON, W. B. (1997): Bits, Bytes and Diplomacy, in: Foreign Affairs, vol. 76, no. 5, pp. 172-183.

---

[1] Cf. for a overview on Internet governance the Journal of Global Legal Studies (JGLS), online available under http://www.law.indiana.edu/glsj/, in particular volumes 5 and 6. The home page of the ICANN, http://www.icann.org/, is also very helpful. The specified hypertext links were last visited on March 12, 2001.

[2] Cf. for a critical view on the economical potential of the E-Commerce: The Economist, Feb. 26, 2000.

[3] Federal Networking Council, http://www.fnc.gov/Internet_res.htm

[4] The Transmission Control Protocol/Internet Protocol (TCP/IP) is the basic communication protocol of the Internet. Compared to the ISO/OSI 7-layer model TCP/IP can be described as a two-layer system: The higher layer, the Transmission Control Protocol, manages the assembling of the messages or files into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Even higher layer application protocols include the World Wide Web's Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), Telnet (Telnet) or the Simple Mail Transfer Protocol (SMTP) are often packaged together with TCP/IP as a "suite."

[5] UN COMMISSION ON GLOBAL GOVERNANCE (1995): Our Global Neighbourhood, http://www.cgg.ch/CHAP1.html

[6] For more information on these organisations see the homepages http://www.itu.int, http://www.ietf.org, and http://www.w3c.org. For the purpose of standardisation it does not matter if these bodies have its legal basis in international law or national law.

[7] All RFCs are online available at the site of the IETF, http://www.ietf.org/

[8] RFC 791 (Sep. 1981) Internet Protocol, DARPA Internet Program, Protocol Specification; p.7 ,, Addresses are fixed length of four octets (32 bits). An address begins with a network number, followed by local address (called the "rest" field). There are three formats or classes of Internet addresses: In class A, the high order bit is zero, the next 7 bits are the network, and the last 24 bits are the local address; in class B, the high order two bits are one-zero, the next 14 bits are the network and the last 16 bits are the local address; in class C, the high order three bits are one-one-zero, the next 21 bits are the network and the last 8 bits are the local address."

[9] A updated chart is available online under http://www.isi.edu/in-notes/iana/assignments/ipv4-address-space

[10] DHCP (Dynamic Host Configuration Protocol) offers network administrators to manage centrally and automate the assignment of Internet Protocol (IP) addresses.

[11] See e.g. the following sites of providers of geographic-tracking-software and evaluation programmes: http://www.infosplit.comhttp://www.bordercontrol.com, http://www.quova.com, http://www.digitalenvoy.com, http://www.netgeo.com , http://www.visualroute.com

[12] See f.e. http://www.anonymizer.com/