VNĚJŠÍ VZTAHY ES/EU - PROSAZOVÁNÍ VLASTNÍCH ZÁJMŮ V KYBERPROSTORU

EXTERNAL RELATIONS OF THE ES/EU – THE ENFORCEMENT OF THEIR INTERESTS IN CYBERSPACE

DAVID SEHNÁLEK

Faculty of Law, Masaryk University

Abstract

This paper focuses on the possibility of state (or the EC) to enforce its interests in the cyberspace. The conclusion is that this possibility is limited by specific borderless nature of this virtual environment. However, states may use new means to create virtual borders and thus enforce their laws via technology.

Key words

cyberspace, technology, ubiquity, law enforcement

Abstrakt

Příspěvek se zabývá otázkou možnosti státu resp. ES prosazovat své zájmy v kyberprostoru. Závěr je, že tato možnosti je na jednu stranu snížena z důvodu specifických vlastností tohoto virtuálního světa. Státy však nejsou zcela bezbranné, protože technologie jim nabízí nové možnosti prosazování práva.

Klíčová slova

kyberprostor, technologie, ubikvita, prosazování práva

Introduction: real world vs. cyberspace

The natural existence of all human beings takes place in regular three-dimensional space and time. This space is usually internally divided by borders into smaller areas where states exercise their exclusive powers. In this paper, this place will be referred to as the "*real world*". Every state has the right to complete legislative, judicial, and executive control over the area of its territory (specific part of the *real world*), people. This power to control and regulate is called *jurisdiction* and it is a direct consequence of the sovereignty of every state.[1]

This paper is focused on law and its application and enforcement in *cyberspace*. Cyberspace is usually defined as a computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange.[2] This term was originally coined by science fiction novelist William Gibson in his story "Burning Chrome" and popularized by his 1984 novel Neuromancer where it was described *as a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.*[3] Cyberspace is usually associated only with the Internet. However, such an approach is mistakably simplistic. The Internet is only a medium, a material background which allows the cyberspace to exist.

Unique characteristics of cyberspace, cyberspace, state and law

Cyberspace has some qualities which make it unique and also very different from the real world. For example, cyberspace cannot be divided into particular lots as the real world by simply erecting borders. The space in cyberspace has more in common with the abstract, mathematical meanings of the term than the real world.[4] From the perspective of this paper this characteristic is important as it implies that the concept of territoriality is not applicable in cyberspace. However,

---

[1] see Cassese, Antonio: International law - 2. ed. - Oxford [u.a.] : Oxford Univ. Press, 2005. - LIII, 558 S. ISBN 0-19-925939-9 - ISBN 978-0-19-925939-7 page 49.
[2] see term cyberspace [cited on October 20, 2007] available at http://www.wordreference.com/definition/cyberspace
[3] see term cyberspace [cited on June 20, 2006] [cited on October 20, 2007] available at http://en.wikipedia.org/wiki/Cyberspace
[4] ibidem

there are some “like borders” or “quasi national areas”[5] in cyberspace but their functions are different. They cannot fulfill the function of delimitation of state's powers as the regular borders do. They exist for the simple reason that cyberspace also needs a system of addressing and localization to allow its users and computers to orientate in it. For this purpose a system of IP addresses and domain names (national and generic) has been created. However, none of them can be used in order to delimit state powers like the borders do with territory. For example, a top level domain name .cz does not necessarily mean that this is an abstract part of cyberspace where the Czech Republic exercises its exclusive rights and powers.

Another important characteristic of cyberspace is its ubiquitous and immediate character. It is not important where in the real world you are. Once you do something in cyberspace, your behavior has effects in the whole cyberspace and may have impact anywhere in the real world almost immediately.

These qualities of cyberspace have serious impact on the law and its application and enforcement. On one side, the state law is geographically determined. States have the power to wield authority over all individuals in their territory. The ubiquity of cyberspace makes it easy for potential violators to evade the authority of a certain state and easily break its laws from a territory which is not under the authority of this particular state.

To prevent such a situation, states may enact some legislation which will be binding upon their nationals abroad, as well as applying to other facts or conduct engaged in abroad and considered prejudicial to the state. States can as well pass legislation applicable to acts performed abroad by foreigners.[6] Nevertheless, they are some strict limits which have to be followed by every state. States have to respect the authority of other states. In other words, such *extraterritorial legislation* may not infringe upon the sovereignty of any other state. And what is important is the sovereignty of other states prevents the use of power to effectively enforce such legislation out of the territory of the state.

[5] for example geografical top level domain names
[6] see Cassese, Antonio: International law - 2. ed. - Oxford [u.a.] : Oxford Univ. Press, 2005. - LIII, 558 S. ISBN 0-19-925939-9 - ISBN 978-0-19-925939-7 page 49.

The abovementioned implies that cyberspace has some characteristic attributes which necessitates changing or at least modifying the rules designed and developed for the real world to be fully and effectively applicable in this new virtual reality. These traditional rules were developed throughout ages and they more or less comply with the needs of our real world but they might seem rather problematic if applied in cyberspace. The main problem in respect to law is that the global character of cyberspace causes that any act done in cyberspace may possibly impact other individuals or even states anywhere in the real world. Since states enforce their laws and are limited to their territory only, they cannot effectively prevent others from infringing. It is so easy to move to a state with liberal regulation and conduct a business or other activities in cyberspace from this state. The source of the activity is located in the real world outside of the power of the first state but its protected general interests (e.g. protection of consumers, personal data protection) might be breached.

It may seem that states are absolutely unable to effectively regulate legal relations in the cyberspace. Some cyber-utopian authors therefore tried to proclaim that cyberspace is an inherently unregulatable space.[7] This is, however and fortunately not the truth. There is no doubt that the cyberspace is a space where law is present and that the state can regulate it.[8] It is the technology and the "architecture" of the cyberspace which affects its nature. The architecture is determined by software code, which is malleable and operates through technology itself. As it was said already, states may therefore encounter enforcement difficulties while trying to limit or prevent some malicious behavior in cyberspace. It might be difficult for the state and its institutions (e.g. police) to track down online perpetrators — particularly those who disguise their identities. There is also the possibility that the offender is from a different jurisdiction, rendering him away from the regulatory reach of the enforcing government[9] as the extraterritorial enforcement of law is not always possible and/or effective.

[7] viz barlow deklarace nezávislosti internetu

[8] pro víc informací viz. "The regulation of cyberspace and the loss of national sovereignty" Noel Cox Auckland University of Technology, Auckland, New Zealand, Information and Communications Technology Law, Vol. 11, 2002

[9] Cyberspace And The State Action Debate: The Cultural Value Of
Applying Constitutional Norms To "Private" Regulation by Paul Schiff Berman, University of Colorado Law Review, Vol. 71, No. 4, May 2000

It may seem that the technology is the main source of problem with the cyberspace and sovereignty of states. It is the technology which makes cyberspace global and ubiquitous. States may seem unable to control cyberspace and unable to enforce their laws. It may seem that cyberspace exist independently in states. The truth is however different and none of this is the truth. It was the state (USA) which has initiated the "birth" and existence of Internet (which is as it was said already, the most important medium allowing cyberspace to exist). The predecessor of the Internet, the network called ARPANET was developed by the United States Department of Defense Advanced Research Projects Agency. The reason was to create a network resistant to losses of part of connections between linked computers which would provide military with reliable mean of communication. The other reason was to enable dislocated scientists to share powerful computers.[10] It was therefore state who originally designed the cyberspace through the technology and who used the technology to create it.

The technology is the key instrument for the state which may enable them to regain lost positions in cyberspace. States may not be capable of enforcing their laws directly against individuals who are outside of such state's personal and territorial jurisdiction. However, such state may use its powers to change the technological background of the cyberspace. Using technology, state can raise new "electronic" borders to enforce its interests and law. In fact, it is not that complicated to develop them and implement them. There are already states (usually those one who do not respect human rights in their "western" conception). As an example of such border I would like to mention the *Golden Shield Project* by China (also known as the Great Firewall of China). This system was started in 1998 and blocks content by preventing IP addresses from being routed through and consists of standard firewall and proxy servers at the Internet gateways. The system also selectively engages in DNS poisoning when particular sites are requested.[11] Another similar system was developed by Saudi Arabia. According to the information published by Reporters Without Borders Saudi Arabia has created one of the world's biggest Internet filtering system which is blocking access to nearly 400,000 webpages, with the aim of "protecting citizens from offensive content and content the violates the principles of Islam and the social norms."[12]

---

[10] see term Arpanet [cited on October 20, 2007] available at http://en.wikipedia.org/wiki/ARPANET
[11] see term Golden Shield Project [cited on October 20, 2007] available at http://en.wikipedia.org/wiki/Internet_censorship_in_the_People's_Republic_of_China
[12] [cited on October 20, 2007] available at http://www.rsf.org/article.php3?id_article=10766

Above mentioned examples clearly demonstrates that it is possible for a state to defend and enforce its laws and interests. Some commonly used passive methods for censoring content (and raising virtual borders) are:

- **IP blocking** - denying access to a certain IP address. This makes inaccessible also all websites hosted on the same server;
- **DNS filtering and redirection** - domain names are not resolved or the system returns incorrect IP addresses.
- **URL filte**ring - Scan the requested Uniform Resource Locator (URL) string for target keywords regardless of the domain name specified in the URL. This affects the HTTP protocol.
- **Packet filtering** – which may terminate TCP packet transmissions if a certain number of controversial keywords are detected.
- **Web feed blocking** - incoming URLs starting with the words "rss", "feed", or "blog" are blocked.[13]

I have marked the above mentioned methods as passive ones. There are also some other technological means which may allow states to enforce their interests and are of a different nature. Instead of filtering or blocking the communication in the cyberspace, states may as well use “pirate methods” in order to enforce their interests. As an example of such active electronic tool may serve the so called **denial-of-service attack** (**DoS attack**) which, if successful can make the target computer resource unavailable to its intended users.[14] However, using DoS attack a state may easily infringe some other state’s sovereignty. The disadvantage of such a tool is that not only targeted website but also other websites located on a same computer may become unavailable. In my opinion, any “active” tool is against non-interference principle and thus against the international law.[15]

---

[13] this data were taken and simplified from http://en.wikipedia.org/wiki/Internet_censorship_in_the_People's_Republic_of_China. For more information on Great firewall of China and methods of censorships in cyberspace see also Empirical Analysis of Internet Filtering in China, Jonathan Zittrain and Benjamin Edelman, Berkman Center for Internet & Society, Harvard Law Schoul, [cited on October 20, 2007] available at http://cyber.law.harvard.edu/filtering/china/

[14] see term Denial-of-service_attack [cited on October 20, 2007] available at http://en.wikipedia.org/wiki/Denial-of-service_attack

[15] see Pikna Bohumil: Mezinárodní terorismus a bezpečnost Evropské unie - právní náhled. Linde Praha 2006, **ISBN:** 80-7201-615-6, p. 42

EC, EU and the enforcement of their interests in the cyberspace

Not only states but international organizations may try to use any of the above-mentioned methods to protect and enforce their interests and law. This might be the truth in matters which fall under the scope of the European Communities as well. On the other side, I do not think that there is at this moment any reason, justification and effective legal instrument which would allow to adopt any of above mentioned measures in the area which fall within the scope of the second pillar of the EU (Common and Foreign Security Policy) or within the third pillar (Police and Judicial Co-operation in Criminal Matters). More probable is that the EU will regulate the cyberspace using traditional legislative measures with norm of conduct. For example in the third pillar of the European Union a general measure was already adopted which has an impact in cyberspace - the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between member states which allows arresting and surrendering to another Member state a person who has committed a computer-related crime.

As the trade is often realized in cyberspace and regulation of external trade falls within the scope of exclusive competences of the European Community, the legal regulation of cyberspace is more likely to happen in the area of external trade regulation. It is important to note, that in such case the EC is bound by its obligations which it has in international (economic) law. Member states have to respect these obligations as well (even an action which aim is to secure some political or security interests in cyberspace can hinder the international trade).

The problem is that any measure adopted by EC must be in accordance with EC's obligation arising from the General agreement on trade in services and/or General agreement on tariffs and trade. To the best of my knowledge, such a situation has never happened yet, but there is already an analogous case where such problem occurred. In case No. WT/DS285 United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services the United States outlawed non-licensed on-line gambling operated from Antigua. In its request for establishment or a panel at WTO Antigua and Barbuda claimed that the total prohibition of gambling and betting services offered from outside the United States might conflict with the United States'

obligations under GATS and its Schedule of Specific Commitments annexed to the GATS.[16] This example clearly shows that international economic law can seriously impact the states' or EC's ability to enforce its laws in cyberspace.[17]

Conclusion

As we can see, states are not as defend less in cyberspace as it may seem. On the one side the possibility to enforce their laws might be limited by the territorial character of the law. On the other side, states may use their powers to erect virtual borders in cyberspace using the technology. Thus, the technology can help them to protect their interests and laws. However, using technological means to enforce their interests, no state is allowed to infringe other state sovereignty. States are also bound be their obligations arising from their membership in international organizations (WTO in particular). From the view point of the EC and future legislation concerning the cyberspace, these limitations must be taken into the account as well.

Contact details:

JUDr. David Sehnálek, Ph.D., e-mail: david.sehnalek@gmail.com

[16] Request for the Establishment of a Panel by Antigua and Barbuda WT/DS285/2 http://www.wto.org/English/tratop_e/dispu_e/285r_d_e.pdf

[17] see Reidenberg, J.R. Technology and Internet Jurisdiction. University of Pennsylvania LAW REVIEW, Vol. 153, No. 6