Jovan Kurbalija

version 2
(22 October 2014)

There is a practical solution for global inviolability of the Internet root zone

Policy suggestions[1]

- The Internet root zone should be inviolable at any time, wherever it may be located.
- No state should have the jurisdiction to prescribe, adjudicate, or enforce policy over the Internet root zone.
- The Internet root zone may only be modified through existing procedures or new ones that might be introduced in September 2015.
- The inviolability of the Internet root zone should be based on customary law that recognises the consistent practice of no unilateral interference by the US authorities in the content of the Internet root zone.

What is the Internet root zone?

It is the highest level of the Internet 'address book' (domain name system). The root zone consists of thirteen root servers distributed around the world (ten in the USA and one each in Sweden, the Netherlands, and Japan). If one server crashes, the remaining twelve would continue to function. The robustness of the root zone is additionally strengthened by 200 anycast servers. At the core of the system is the root zone database which contains a list of all country domains (e.g. .uk, .it, .br) and generic domains (e.g. .com, .org).

Currently, the process of making changes in the root zone database involves the following steps: a) approval of the change by the US Department of Commerce; b) update of the root zone database at the master root server (first among the thirteen equal servers) which is operated by the Internet company VeriSign; c) propagation of the changed root zone database via root servers to the whole Internet.

The first step – approval by the US Department of Commerce – should be performed in a different way after 30 September 2015. By initiating the process of policy consultations, the US government requested that the post-September 2015 arrangement should be global and multistakeholder.

[1] The basis for this proposition was first outlined in the blog post: 'International inviolability for the root zone' (9 December 2013): http://www.diplomacy.edu/blog/international-inviolability-root-zone. The blog post triggered discussion within the legal and technical communities, which is reflected in this Policy Brief.

Context and controversies

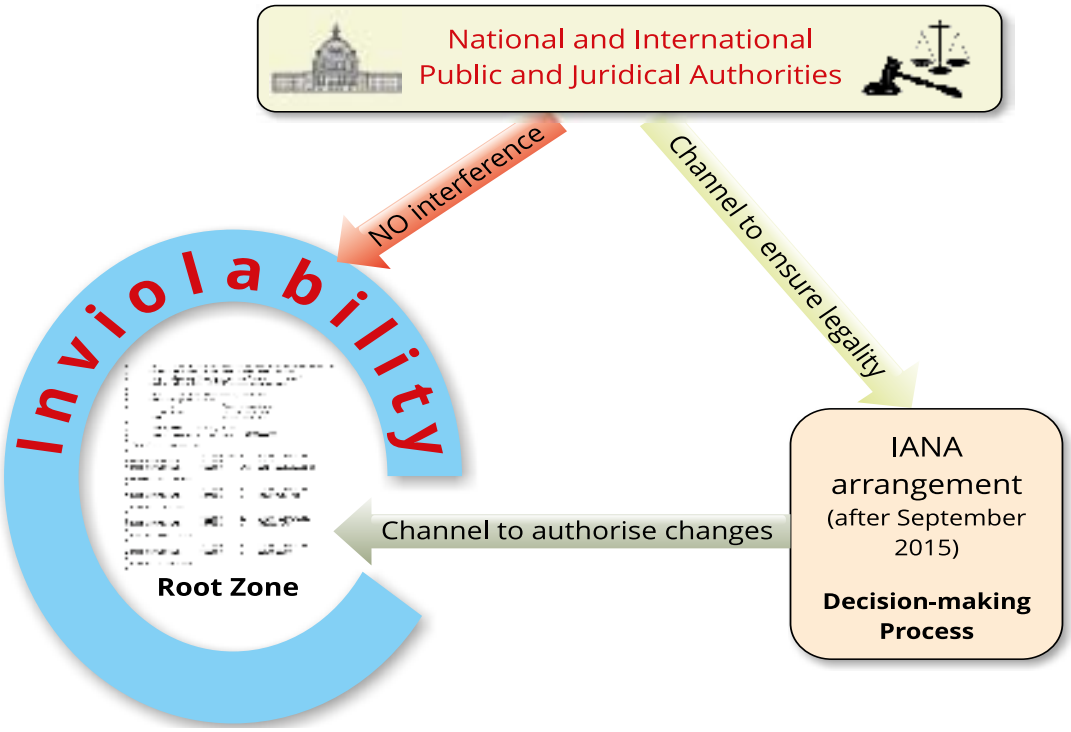
Control over the Internet root zone has been one of the most controversial issues in the Internet governance (IG) debate. As the core of the domain name system (Internet address book), it ensures the functional integrity of the Internet.

Since the first days of the World Summit on the Information Society (WSIS) back in 2002, the technical possibility of the USA 'removing' other countries from the Internet[2] – by deleting a country's top-level domain name (known as a ccTLD) from the root zone database – has led many states to criticise the USA's role in the supervision of the root zone and the Internet Corporation for Assigned Names and Numbers (ICANN).[3]

On both sides of the debate, the root zone issue has high symbolic relevance. On the US side, the Internet is considered an important part of the country's national creative history. In particular, the US Congress considers the country's historical role in the development of the Internet to be an important element of the future IG arrangement.

[2] 'Removal' was associated with the removal of a country domain name (e.g. '.it', '.ch') from the root zone database. It is not related to cutting off the Internet connection.

[3] The USA's supervision of the root zone database is often quoted as the source of US power over the Internet. The element of power is in forcing the other side to act in the way the holder of the power wants. The US supervision of the Internet root zone has not been, and cannot be, used in this way. First, due to a complex 'anycast' system which functionally distributes the root zone database around the globe, any unilateral decision by the USA would have a delayed, or more likely, no effect at all on the 'deleted' country. Second, any unilateral interference with the Internet root zone by the USA would trigger the fragmentation of the Internet into national and regional Internets, which would be particularly detrimental for US interests (Internet industry, English as the Internet *lingua franca,* etc.).



Most other countries argue that the Internet as a global infrastructure should not be under the jurisdiction of any single country. However, there is no consensus about what an alternative arrangement should entail (suggestions vary, from global multistakeholder to inter-governmental arrangements). Alternative proposals are often framed in a symbolic and value context as a matter of sovereign equality and fairness in international relations.

The USA has never used its custodial role in regard to the root zone for deleting a country from the Internet, even when there could have been a legal basis either under the US law related to sanctions[4] or in the UN Charter.[5] It was not used in any of the recent conflicts from the Balkan wars in the 1990s to the current conflicts in the Middle East.

However, the recent legal action against the Iranian domain (.ir) in the US courts highlighted the risk that ICANN, as a US-incorporated entity, could be legally forced by the court to make changes to the root zone under exceptional circumstances. Although unlikely to happen in the '.ir' case, the sheer possibility creates a weakness in the current arrangement.[6] Global inviolability of the root zone database from any state or judicial authority would address this problem.

Possible solutions

The following elements *de lege ferenda* could be used for developing global inviolability of the root zone:

- **customary law** based on the US practice of non-interference with the Internet root zone (*opinio juris* will need to be confirmed).[7]
- **diplomatic law** on inviolability applied to the Internet root zone.
- **a common heritage of mankind**[8] status of the root zone that will support inviolability

4 The US sanctions regime against Iran between 1992 and 2013 included banning the export of mobile telephones, laptop computers, and software applications such as antivirus programs. However, Internet access and the domain name were never part of the sanctions regime. The same applies to the US sanctions against Cuba that cover telecommunications, but have not affected Cuba's domain name (for telecommunication sanctions against Cuba see: http://www.treasury.gov/press-center/press-releases/Pages/tg273.aspx)

5 The UN Charter, in Article 41, specifies that sanctions may include 'complete or partial interruption of economic relations, and of rail, sea, air, postal, telegraphic, radio, and other means of communication,...'

6 For detailed argumentation on the court case 'Ben Haim *et al.* v Islamic Republic of Iran *et al.*', consult https://www.icann.org/en/system/files/files/ben-haim-motion-to-quash-writs-1-29jul14-en.pdf

7 One challenge could be that the root zone database contains both generic domain names (.com, .org) and country domain names (.it, .br). International customary law can apply to country domain names because it implies relations between countries (e.g. US non-interference with other countries), while this international aspect does not necessary apply to generic domain names.

8 While the root zone can have the status of common heritage of mankind, it is difficult to apply this status to the Internet as a whole due to the diversity of its elements (telecommunications, servers, content, etc.). For discussions on the Internet as a global commons see: Mueller M,

through exclusion of claims of sovereignty over the root zone and management 'by mankind as a whole'.[9]

Based on these elements, two solutions can be envisaged: 'software' and 'hardware' inviolability.

'Software' inviolability would protect the root zone database (computer file) wherever it is located. This approach would rely on a solution from diplomatic law which specifies that '[t]he archives and documents of the mission shall be inviolable at any time and wherever they may be' (article 24 of the Vienna Convention on Diplomatic Relations). Inviolability of the root zone could also benefit from the status of common heritage of mankind, as that would exclude the root zone from sovereignty claims by any state.[10]

'Hardware' inviolability would protect the server that contains the root zone database. Although 'software' inviolability is sufficient for protecting the root zone, the protection of a physical server would further strengthen its inviolability. This option opens the issue of where the root server would be located. It could be located on the UN premises, as they already enjoy legal inviolability from any national jurisdiction. If the main root server remains at the current location (Verisign), it would require changes in US national law in order to ensure inviolability of the root database from the actions of US courts.[11] If ICANN attains quasi-international legal status, with legal immunities the root server could be physically located at ICANN's premises.

Mathiason J and Klein H (2007) The Internet and Global Governance: Principles and Norms for a New Regime. *Global Governance* 13, p. 237. For an argument that 'critical Internet resources' should be considered common heritage of mankind see: Segura-Serrano A (2006) Internet Regulation: A Hard-Law Proposal. *Jean Monnet Working Paper* No. 1, p. 48.

9 For more information see Wolfrum R (2008) *Common Heritage of Mankind. Max Plank Encyclopedia of Pubic International Law* (http://opil.ouplaw.com/home/EPIL).

10 The principle of common heritage of humankind is considered part of international customary law. It is also used to regulate the following areas in treaty law: the seabed (Part XI of the 1982 UN Convention on the Law of the Sea); outer space (Article 1 of the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Article 11(1) of the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies); and Antarctica (Paragraph 8 of the preamble of the 1991 Protocol on Environmental Protection to the Antarctic Treaty).

11 The other countries – Japan, the Netherlands, and Sweden – which host three of the thirteen root zone servers may grant special status to premises where these servers are located.

How to achieve root zone inviolability

The customary law on inviolability of the root zone – codifying the US practice of non-interference with the root zone[12] – could be formalised in one of the following ways:

- an Internet root convention;
- an advisory opinion of the International Court of Justice;
- a declaration of the UN General Assembly; or
- a unilateral declaration by the US government, which should be binding under international law.

Questions and answers

Here, you can find answers to questions and comments received over the last two weeks since the Policy Brief first published:

Will root zone inviolability require moving the root zone server from Verisign installations to some other physical location? This won't be necessary. The root zone should be inviolable wherever it is physically located.

Will any domain name be inviolable (e.g. killxxx.com)? No. Inviolability would apply only to top level domains. Specific domain names would be subject to the jurisdictions of where they are registered.

Would this arrangement require moving ICANN to a location outside of the United States? Not necessary. The status of ICANN is a separate issue from the status of the root zone.

Would this arrangement put ICANN beyond the reach of any law? No. ICANN would still have to observe laws like any other entity. Root zone inviolability provides specific protection only for the root zone.

Would inviolability make ICANN's accountability irrelevant? No. This is a separate issue. ICANN's accountability is discussed in the current IANA transition process.

How realistic is it to negotiate a root zone convention? The adoption of such a covention would

12 This practice particularly applies to non-interference with domain spaces of other countries without the consent of these countries.

be the most complicated scenario. The good news is that any of the suggested instruments (convention, declaration, advisory opinion, unilateral statement) would only codify the existing 'customary law' of non-interference by US authorities in the root zone. These instruments would not create a new law; they would codify the existing customary law.

How can you get customary law In 20 years when previously it has taken centuries? You are right if you point out the examples of the Law of the Sea and diplomatic law. These rules were crystallised by consistent practice over centuries before they were codified in the Vienna Convention on Diplomatic Relations (1961) and the Law of the Sea (1982). In the case of the root zone file, we have 20–30 years of consistent practice of non-intervention by the US authorities (governments and courts) in areas concerning the domains of other countries. What matters with customary law is consistent practice, not necessarily a prescribed passage of time. Obviously, practice happens over time. It could be posited that time and events occur faster nowadays than previously in human history. This shift towards the faster development of customary law in modern times was introduced with the process involving the North Sea Continental Shelf Cases of the International Court of Justice (1969).

How is 'root zone inviolability' linked to the current IANA transition process? These two issues can be treated separately. But they can also influence each other. Root zone inviolability could strengthen a post-2015 IANA arrangement.

Why do we need inviolability if the root zone is fully protected technically? Technical inviolability does not guarantee legal inviolability. Technical solutions do not shield institutions and individuals from court judgments.

Would root zone inviolability prevent the interference of those who have physical control over the root zone server? In principle, the law makes certain actions illegal, but cannot make them physically impossible to carry out. In the case of root zone inviolability, it is not realistic to think that interference might take place in violation of a law, when it never occurred while it was unregulated or 'legal'.

Does root zone inviolability require both a legal basis in customary law and a basis in the common heritage of mankind? No. Customary law recognising the US practice of non-interference is sufficient for root zone inviolability for country level domains (.uk, .tn, .fr). The situation is less clear with gTLDs (.com, .sport, .wine). The legal basis for the inviolability of gTLDs could be sought through the concept of common heritage of mankind.

Conclusion

At a minimum, the inviolability solution could put to rest the highly symbolic issue of the root zone, thus allowing the global community to focus more policy energy on other practical and relevant issues that will determine the future of the Internet.

We look forward to your comments – please e-mail them to jovank@diplomacy.edu

Diplo's policy briefs can be downloaded from http://www.diplomacy.edu/policybriefs

Disclaimer: The content of the policy brief represents the personal opinion of the author and should not be attributed to any organisation with which the author is affiliated.

Address: DiploFoundation, WMO Building
7bis, Avenue de la Paix, CH-1211 Geneva, Switzerland | tel: +41 22 907 3633

DiploFoundation, Anutruf, Ground Floor
Hriereb Street, Msida, MSD 1675, Malta | tel: +356 21 333 323