Abolish the Rules Made of Stone?  
Contemporary International Law and the models to Internet Regulations

Gianpaolo Maria Ruotolo  
Department of Law, University of Foggia, Foggia, Italy  
gianpaolo.ruotolo@unifg.it

Abstract

The article frames different international law approaches to Internet regulation through the study of some specific aspects, the legal consequences of the qualification of the Internet as common heritage of mankind/global public good, and the domain name system (DNS) governance.

Keywords

internet – international law – informal law

1 The Legal Discipline of the Internet: a Non-Regulatory Approach and Some Autonomous Rules. The Requests for Comments (RFCs) Case

The difficulties of providing a complete and effective legal discipline for the Internet have been evident since its diffusion worldwide, in the early 1990s, when different approaches began to spread.¹ The first focused on the peculiarities of the phenomenon and proposed the inapplicability of traditional legal categories and, more generally, of law as a regulatory tool both for the Internet as an infrastructure and for human behaviours that take place there.² The reasons that would justify such an approach are many: the absence of physical

borders in cyberspace would prevent the identification of the (State) law applicable to a specific case and, for the same reason, the competent judge to settle disputes. Moreover, the Web would imply a constant risk of extraterritorial application of domestic law, with spill-over risks: subjecting the Internet to the domain of (State) law would entail the possibility of having many conflicting regulations for the same phenomenon. Therefore, this approach suggested the use of so-to-speak autonomous mechanisms of discipline, whose rules were produced by the Internet users themselves, and incorporated into a new genus of law, neither State nor international, called cyber-law.

In this regard, the example of netiquette was given. The same approach, in addition to conceiving the Internet as a “legal void”, a lawless space – in some ways similar to the high seas or to extra-atmospheric spaces, in which State sovereignty is absent, but not, as is well known, international law – affirmed that the only rules therein applicable were spontaneously generated by its users, in the same way as the lex mercatoria, the first case of “stateless global law”.

Such a reconstruction, even though raising some dogmatic issues (such as the one pertaining the same existence of a third genus of law in addition to international and domestic one) seized a general character of the Internet: its operating rules are often generated “from below”.

We may think to the Request For Comments (RFCs), containing mostly technical specifications, developed by experts and scholars on the basis of the practices that have proven to be most effective: these documents are “offered” to the Web community through the Internet Engineering Task Force (IETF, an international non-governmental organization that gathers technicians and

---

3 While the Internet is a network of connected computers, the world wide web, or Web for short, is what one sees when he's online. One may think of the Internet as roads, and of the Web as the things one may see on those roads, like houses and shops. Sometimes, indeed, the words are used as synonyms. On this one may see: <www.bbc.co.uk/newsround/47523993>.


5 One may mention the now abused “Declaration of independence of cyberspace” which, addressing the States, declared: “you are not welcome among us. You have no sovereignty where we gather. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Cyberspace does not lie within your borders”. See BARLOW, A Cyberspace Independence Declaration, San Francisco, 1996. The Declaration is published in its entirety at: <projects.eff.org/~barlow/Declaration-Final.html>.


researchers interested on an individual basis in the evolution of the Web). The documents thus elaborated obtain a different classification on the basis of their “success” in the community of the Web, which influences their regulatory scope. On this basis can be identified: a) the proposed standards, specifications that are sufficiently stable and that have met some success, but which are not yet considered mature enough to be definitively formalized; b) the draft standards, which have obtained at least two implementations that showed their effectiveness, and that for this reason the Internet Engineering Steering Group (IIEG, an IETF working group) considers sufficiently mature and c) the actual standards, with a significant number of applications.

The latter, in particular, certainly have both normative content and scope in the sense that, from a substantive point of view, they suggest to their recipients a certain behaviour. Some would say that they lack the requirement of legality, being unfit to produce effects regulated by law, and whose observance is left to the free choice of network operators. But one should bear in mind that the infringement of these rules excludes the possibility of using the resource that they govern and, therefore, all those who decide to use it, must respect them, or accept the exclusion (burden).

2 Overlaps between “Public”, Private International Law and “Code” as Tools of Regulation for the Internet

Another dogmatic approach, which today assumes a majority consistency, moves from the consideration that the Internet represents, albeit of a revolutionary scope, just a new media, considers it governable by law8 and stresses the need to harmonize, through international law, some concepts of general scope in order to build a common legal framework in which domestic legislators can move.9

This scholarship resizes also the fears of spill-over we mentioned, pointing out that they do not represent a specific issue of the Internet, but rather a phenomenon connected to each and every transnational situation, which would therefore be governable, depending on the cases, by “public” international law

---

or by conflict rules of common or conventional systems of private international law.

Indeed, in order to be truly effective and all-encompassing, a thorough legal regulation of the many aspects of the Internet must concurrently use both instruments of public international law and rules of private international law (be they uniform or common), while the former, in fact, impose limitations on the States in order to govern the Web as an infrastructure, the latter can identify the domestic Courts that have the power to settle a specific dispute and the applicable law. Forms of artificial intelligence could even automate the latter process, as was highlighted in a recent report by the European Parliament, which dedicates some interesting pages to the automation of private international law systems.

Moving on to a third way of reading the issue we are framing, it would even be pointless to speak of an ontologically governable or ungovernable nature of the Internet as such, since it would not have an unchangeable nature of its own, which would instead be contingently determined by the “code” that gives it shape, that is to say, by the set of hardware and, above all, software (the “code”, indeed) which regulates its use.

According to this vision, therefore, cyberspace would be governable through its informatics code, which, in turn, should be informed by international law, essentially aimed at deciding which values are to be taken as a reference parameter by the code itself.

And it is hardly necessary to highlight how, from a purely terminological point of view, “code” is a common expression for jurists and IT experts and refers, in both cases, to a sequence of instructions that must be applied...

---

11 “Artificial Intelligence: Issues Relating to the Interpretation and Application of International Law”; European Parliament Resolution of 20 January 2021 on artificial intelligence: issues relating to the interpretation and application of international law to the extent that the EU is concerned with regard to civilian and military uses and the authority of the state outside the scope of criminal justice (2020/2013 (IN1)), available online.
12 See LESSIG, Code - Version 2.0, Cambridge, 2006, p. xv, who argues that the Internet can be controlled by forces “in large part exercised by technologies […], backed by the rule of law (or at least what’s left of the rule of law). The challenge for our generation is to reconcile these two forces".
3 Digital Convergence

In addition to the difficulties illustrated so far, the identification of a discipline for the Web, both of domestic and international law, is made even more complex by the fact that information relating to the most disparate services and media passes through it. This ability to incorporate completely different contents and tools is referred to with the expression “digital convergence” (or even “technological convergence”), with which reference is made to the fusion, made possible only by digital technology, of a plurality of different tools, all capable of transmitting information.13

Each of these media, in its traditional form, is notoriously the subject of autonomous legal regulation – be it of international or domestic law – which differs from those envisaged for the others. And as long as the same media were separate from each other, their different regulation was not only justified, but even desirable, to take into account their peculiarities.14 Now, their fusion could imply the merging of their regulation, at least for some aspects: the scholarship that dealt with this issue suggested that, with digital convergence, regulatory differentiations should be maintained exclusively as regards the contents, but not for the medium that conveys them.15

Indeed, not even so delineated, the question appears to have a simple solution: whenever the Internet is used to offer services that are difficult to classify, in the doubt of which discipline to apply, which could provide for more or less strict rules, the various potentially competent domestic legal systems, and regulators, may select, on a case by case basis, the one that is the most restrictive of the prerogatives of individuals.

The element of convergence was, however, invoked by the International Telecommunications Union (ITU), on the occasion of the revision of the International Telecommunications Regulations (ITRs) of 2012, as a legitimate title for its competence to regulate the Internet as a whole.

It must also be remembered that the attribution of Internet governance competence to an intergovernmental international organization was opposed by many factors, including, in particular, the will of many States, especially

13 To concretely understand the scope of the convergence theory, think about how a smartphone is now able to make phone calls (with traditional or VoIP systems), play and transmit music and videos, read text files, take, send and view photos. One of the first theorists of this theory was Negroponte, Being Digital, London, 1995.


the industrialized ones, who fear the excessive importance of national governments, in particular those of an undemocratic nature.\textsuperscript{16}

4 The Awkwardness of a Unilateral State Regulation of the Internet. The Bilateral Relationship between the Internet and International Law

An analysis of the practice of the last few years highlights how the instruments of domestic law often proved unsuitable for effectively regulating the Internet by themselves.

One may think of how the restrictions on Internet access adopted by some countries in North Africa and the Middle East in no way prevented internal and foreign communications via the Web, in particular through social networks. Those, with other factors, made possible the revolutions of the so-called “green wave” at the beginning of 2011.\textsuperscript{17}

Even on the occasion of the revolution that led to the fall of the Mubarak regime in Egypt, the government tried to block contact between the insurgents by cutting off Web connections, but the blockage was circumvented. By the end of 2012, Iran imposed important restrictions on the Google search engine and its Gmail service: it seems that the blackout was prodromal to the much more complex, ambitious and illiberal operation of creating an autonomous domestic Iranian Net but, since the obscuration was implemented, from a technical point of view, by imparting to the Iranian servers which deal with resolving domain names into IP addresses\textsuperscript{18} the order to block this operation with reference to the unwanted addresses, this measure was circumvented by typing, as the destination to reach, the IP address of the site instead of its domain name or using a DNS server external to Iranian territory.

The technical element (the... “Code”) influenced the regulatory one.

On the inability of domestic legal systems to unilaterally regulate the issues that concern us, the 2003 United Nations (“UN”) World Summit on Information

\textsuperscript{16} Radu, Negotiating Internet Governance, Oxford, 2019, p. 109 ff.

\textsuperscript{17} The Report drawn up by the Special Rapporteur of the UN Human Rights Committee Frank La Rue “on the promotion and protection of the right to freedom of opinion and expression” (Doc. A/HRC/17/27) underlines the importance of the Internet for the development of these events in www.ohchr.org.

\textsuperscript{18} For a more detailed explanation of the way the domain name system works, please see infra Section 7 and Ruotolo, “Fragments of Fragments. The Domain Name System Regulation: ‘Global’ Law or Informalization of the International Legal Order?”, Computer Law & Security Review, 2017, p. 159 ff.
Society (“WSIS”) adopted a Declaration of Principles which recognizes the multilevel nature of Internet governance, which requires the involvement of a plurality of actors as States (for issues relating to aspects of public order) and international organizations (for the identification of uniform technical standards), economic operators, NGOs and the so-called civil society.19

This approach recalls some studies of global administrative law,20 which could provide us with further interpretations of the phenomenon, together with those elaborated in the context of the so-called informal international law, which we will also discuss later.

What is sure is that international legal order has been called to govern the Internet on a global basis, and to establish some general principles, so as to limit the domestic jurisdiction of the States.

Moreover, the relationship between international legal order and the Internet is bilateral: if on the one hand, in fact, the former is called to regulate the latter, on the other it has undergone some peculiar changes as a result of the dissemination of information by its operators (government officials, NGOs, scholars, lawyers) through the Internet itself.21

It must be said that this is not a completely new phenomenon.

Technological progress has always shaped legal systems, including the international one: one may think of the treaties concluded to regulate the behaviour of States in outer space,22 the use of geostationary orbit,23 civil aviation,24

22 One may consider, for instance, the Convention on International Liability for Damage Caused by Space Objects, 29 March 1972, entered into force 1 September 1972.
24 See the Convention on the International Civil Aviation Organization (ICAO), 7 December 1944, entered into force 4 April 1947.
nuclear energy,25 scientific research on the high seas,26 which all arose only when technological progress made them necessary.27

But while in these cases the “technical” peculiarities of the regulated objects influenced only their substantive content, in the case of the Internet, the influence extended not only to the content of the regulation of certain sectors, but even to some basic functions of the international legal order as a whole, in particular the procedures for the creation and application of its rules.28

What’s more, the qualification of the Internet as a global public good, we’ll see, is fairly consolidated in the literature, although with some methodological distinctions: while some Authors conceive the Internet as a “final” global public good, others see it as an “intermediate” one, instrumental for the pursuit of further goods.29 The two distinct approaches are also at the basis of the two different conceptions of the right of access to the Internet as instrumental for the protection of other fundamental rights (such as that of information, expression, development) or as an autonomous fundamental right.30

We already tried, in other papers, to frame the Internet as part of the common heritage of mankind; and indeed, for some, the two categories overlap.31

28 PERRIT, cit. supra note 21, p. 885 ff.
30 It is impossible for us to reconstruct the pertinent practice here, even only briefly. To limit to a recent element, we point out how the Indian Supreme Court, in a decision of 10 January 2020, made the fundamental right to access to the Internet derive from the rules relating to freedom of opinion and expression, establishing how, consequently, any restriction on the former must follow the same criteria and comply with the same conditions as those envisaged for the latter.
31 EGEDE, “Common Heritage of Mankind”, in Oxford Bibliografies, available online, declares the substantial coincidence between the category and the one of global public goods: the first, in fact, “represents the notion that certain global commons or elements regarded as beneficial to humanity as a whole should not be unilaterally exploited by individual states or their nationals, nor by corporations or other entities, but rather should be exploited under some sort of international arrangement or regime for the benefit of mankind as a whole”.

THE ITALIAN REVIEW OF INTERNATIONAL AND COMPARATIVE LAW 1 (2021) 246 – 275
Let’s make it clear that, in our opinion, the first expression may refer to the legal regime of applicable international law and the second one to the goods it applies to; we will develop these considerations later.

5 Pre-Existing Rules of International Law and the Interventionist Approach

Let us now try to understand whether there are pre-existing rules of international law which, in consideration of their object and their scope, can be applied to the Internet.

From a theoretical perspective, the approach according to which the study of international legal cases connected to the Internet can be conducted in the light of “traditional” rules, categories and concepts of international law has been critically defined “interventionist approach”, whenever it leads to an analogous application, to on-line cases, of rules of international law conceived to regulate “real” situations.

According to this criticism, the analogy would, in fact, be an unjustified consequence of the fact that, to make up for the absence of a specifically conceived regulation, the international lawyers are pushed, by a sort of legal horror vacui, to tackle the issues with their own instruments, in an attempt to intervene in the problems of the world, in order to manage them.32

Here we cannot develop a more in-depth analysis of this orientation and of the criticisms underlying it, but let us at least underline how it essentially concerns the way in which international lawyers conceive their profession and their function.33 By the way it does not seem to us to be applicable to all those cases in which there has been an explicit normative activity of international law.

---

33 “Short of conferral of any new express responsibilities, international lawyers have nowadays found themselves ostracized, their fate being reduced to either being the bored experts of overly discussed fields or the distant observers of phenomena deemed better addressed through non-legal regulatory tools”; D’Aspremont, cit. supra note 32. For a fascinating analysis of the function of international law in history and of the way of conceiving the profession of the international lawyer see Koskenniemi, The Gentle Civilizer of Nations. The Rise and Fall of International Law 1870–1960, Cambridge, 2001.
6 The Internet as Common Heritage of Mankind/Global Public Good

The aforementioned characteristics of the Internet lead us to search, for its international governance rules, first of all, among international law rules, which, over time, arose or were adopted, with the aim of regulating the States' use of resources that cannot be unilaterally appropriated and whose exploitation presupposes the possession of technological skills.

Those are, in most cases, related to goods that have been considered part of the common heritage of mankind and to which, therefore, is applicable that international law regime.\textsuperscript{34}

It is worth remembering how such norms have often been reported as an index of the transition from the so-called international law of coexistence between States to the so-called international law of cooperation, based on principles of equal “participation” in the life of the international community, but which would allow the differentiation of the obligations imposed on States on the basis of the “functions” they have assumed within a particular legal regime.\textsuperscript{35}

These two categories, however, have been more recently joined by the so-called international law of integration: according to a part of the doctrine, in fact, the contemporary international legal order is characterized as an integrated structure, organized in concentric circles, in which legal rules of a different nature merge, finding coordination and integration in a legal system that addresses a transnational and multi-stakeholder society.\textsuperscript{36}

\textsuperscript{34} With regard to the Internet, we had already made this qualification before; see Ruotolo, International Law. Profili di diritto internazionale pubblico della Rete, Bari, 2012. In the same sense, recently, see Segura Serrano, “The Cyberspace as Common Heritage of Mankind”, in Iovane et al. (eds.), The Protection of General Interests in Contemporary International Law. A Theoretical and Empirical Inquiry, Oxford, 2021, p. 189 ff.


\textsuperscript{36} One may think, for instance, to the differential treatment for developing countries. Among others, on this point, see Abi Saab, “Whither the International Community?”, European Journal of International Law, 1998, p. 248 ff.

\textsuperscript{37} Some scholars, to try to give meaning to legal processes that would not be adequately recognized by international law (as being connected to rules created by mechanisms that differ from the latter, which contemplates the centrality of the States) conceived the regulation of goods of relevance transnational as the product of the integration between different legal systems; the, indeed fragmented, “global law” (the law that regulates the use of goods of “global” relevance), the legal reflection of a multidimensional fragmentation of the global society as such. An attempt to bring global law to normative unity could be carried out by reconstructing the normative compatibility of the fragments that compose...
Let’s also recall that the notion of the common heritage of mankind, which is already traceable in the classical international law of the seventeenth century, was, as well known, updated in 1967 during the Third UN Conference on the Law of the Sea, and was therefore first included in the UN General Assembly resolution No. 2749 (XXV) of 17 December 1970 (according to which the area of the seabed and oceans and their subsoil, which lie beyond the limits of national jurisdictions, as well as their resources, are the common heritage of mankind and, therefore, their exploration and exploitation must be conducted for the benefit of all humanity) and then in Part XI of the UN Convention on the Law of the Sea (UNCLOS).38 A similar concept, even if not so clearly defined, had appeared in the Antarctic Treaty of 1959 and in an even earlier declaration of the General Assembly on the “legal principles governing the activities of States in the exploration and use of outer space”, adopted on 13 December 1963 as well as in the subsequent Treaty of 1967 relating to the activities of States in the exploration and use of space. Also the Treaty regulating the activities of States on the Moon and other celestial bodies of 1979, in Article 11, defined the Moon and its natural resources as common heritage of mankind.

Further applications are contained in the UNESCO Convention of 16 November 1972 on cultural and national heritage of exceptional value as well as in the Universal Declaration on the human genome adopted, again by UNESCO, on 11 November 1997, according to which it cannot be the object of appropriation by States or private individuals.39 The last declaration, in particular, confirms the versatility of the category, which can be used for the protection of very different assets, for both characteristics and functions.

By identifying the common distinctive features of all those rules, it can be seen that they entail the subjecting of protected goods to an international law regime aimed at limiting the freedom of exploitation of States essentially by imposing on them four distinct restrictions: a) a prohibition to extend their sovereignty to the assets that are common heritage and, in particular, the
prohibition of their unilateral appropriation; b) an obligation to try and make
the management of some goods object of an international regime of cooperation;
c) the prohibition of their use, even for general interests, such as damage
to the environment; d) the obligation to use such goods exclusively for peaceful
purposes and, therefore, the prohibition to carry out activities that are inconsis-
tent with international law, and in particular with the principles contained
in the UN Charter on the maintenance of international peace and security.

So, whenever a specific good is identified as part of the common heritage of
mankind, it goes at least under these four principles; this regime as a whole, is
now part of general international law, of which it would even represent a “basic
principle”, for some even of jus cogens.

In our opinion, the Internet possesses all the requisites to be the youngest
member of the family of goods subject to this regime: it, in fact, represents an
exhaustible resource (one may think of the issue of the IPv4 addresses, all already
assigned), not appropriable by a single State, and whose conservation is of com-
mon interest, as many declarations of States and international organizations have
already recorded. On the latter issue, already in 1999 the UN General Assembly
had the opportunity to note that “the dissemination and use of information tech-
nologies and means affect the interests of the entire international community and
that optimum effectiveness is enhanced by broad international cooperation”.

The recognized global importance of the Web, the aforementioned exist-
ence of a collective interest of the States in maintaining its full functionality,
and many acts adopted by international organizations, from which a consen-
sus emerges regarding the need to ensure that Internet governance rules are
shared by all interested parties, public and private led us to these conclusions.
It is no coincidence that the acts adopted more than ten years ago during the
twelfth UN Congress on Crime Prevention and Criminal Justice held in Brazil
from 12 to 19 April 2010 explicitly defined cyberspace “the fifth common space –
after land, sea, air, and outer space”.

\[\textit{The analysis of the customarization of the principle in question is carried out by Wolfrum,}
\]
\[\textit{“The Principle of Common Heritage of Mankind”, Zeitschrift für ausländisches öffentliches
\[\textit{In this sense see Salamanca Aguado, \textit{La Zona Internacional de los Fondos Marinos -
Patrimonio Común de la Humanidad}, Madrid, 2003, p. 298.}\]
and Science, 2007, p. 57 ff.}\]
\[\textit{Resolution a/res /53/70 of 4 January 1999, “Developments in the field of information and
telecommunications in the context of international security”. In the same sense, see also the
Statement of 15 December 2015 by the Maltese delegate to the UN on the occasion of the
World Summit on Information Society Review Process.}\]
\[\textit{See Doc. UN A/conf. 213/1E/7, 23 March 2010.}\]
From a methodological perspective, however, we need to clarify how as a result of the extension to the Internet of pre-existing international law obligations and a consequence of the application of the regime of the common heritage of mankind, one must always bear in mind an interpretative “readjustment” of the same obligations.

6.1 **A) The Prohibition of Unilateral Appropriation of the Internet by Single States**

The application to the Internet of the principle of non-appropriation, as is already the case for other common spaces such as the high seas or extra-atmospheric spaces, prohibits States from dealing with the Net – and even with those of its elements that are physically located in areas subject to their sovereignty – as if it were under their exclusive dominion and, therefore, to engage in behaviour that prevents, in whole or in part, other States from using it or, again, to limit their discretion regarding its use.

This leads us to conclude for the existence, at least, of a prohibition for all States to carry out any action or behaviour capable of endangering the existence of the Web as it is understood nowadays.

There’s to say, indeed, that some States are also engaging in behaviors that seem to be in conflict with the latter prohibition: we refer to the risks of fragmentation of the Internet (the phenomenon of the so-called “splinternet”) due to various factors of technological, commercial and political nature, and often dictated by the spread of nationalist tendencies that give great importance to national interests. One may think, for instance, to how China raised what has been called the “Great firewall” or to the fact that Russia in 2019 approved the “Internet Sovereignty Act” (Закон о «суверенном интернете») that mandate Internet surveillance and grants the Russian government powers to partition Russia from the rest of the Internet, also by creating national section of the Domain Name System.

6.2 **B) The International Obligation of Cooperation between States in the Governance of the Internet**

Secondly, the existence of an obligation of cooperation – of a procedural nature and which takes the triple form of an obligation to inform, consult and negotiate – requires States to create mechanisms, or use preexisting fora, to debate the problems connected to the use of the Internet and therefore, at least to try to reach a consensus regarding the measures of discipline and use of the common good.
6.3 **C) A Ban on Internet Pollution**

The prohibition of pollution, more than the aforementioned obligations, has to be adapted to the peculiarities of the Internet phenomenon.

Leaving aside any consideration of the fact that, as it was calculated, every second of consultation of the Web by a single user releases 0.2 grams of carbon dioxide into the atmosphere, and that therefore it is a source of real environmental pollution, let’s now switch our attention on the online behaviour inhibited by States by virtue of this prohibition.

To this end, we will briefly try to reconstruct how the same prohibition relates to “real” spaces, in order to proceed with its readjustment to the Internet.

The ban on “traditional” pollution of areas declared a common good extends to them the more general prohibition of pollution of areas subject to the sovereignty of other subjects of international law.\(^45\)

The latter, as known, is a corollary of the prohibition of interference and of the right of States to integrity, and is embodied in the “obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability.”\(^46\) The arbitration ruling given on 16 November 1957 in the dispute between France and Spain relating to Lake Lanoux also affirmed the existence of a “principle which prohibits the upstream State from altering the waters of a river in such a fashion as seriously to prejudice the downstream State”,\(^47\) and the Declaration of the UN Conference on the Human Environment adopted in Stockholm in 1972, at principle 21, recognizes that, in accordance with the UN Charter and the principles of international law, States have “the sovereign right to exploit their own resources pursuant to their own environmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction”, thereby and so reaffirms the existence of a prohibition of general international law to carry out, even within national borders, activities that damage the environment in other States or in areas not subject to the exclusive sovereignty of any State.\(^48\)

Even the UNCLOS, in Article 193, declares that the States hold a “sovereign right to exploit their natural resources pursuant to their environmental policies

---


\(^{48}\) The declaration can be found at: <https://legal.un.org/avl/pdf/ha/dunche/dunche_e.pdf>. See also Stevens, *International Courts and Environmental Protection*, Cambridge, 2009, p. 3 ff.
and in accordance with their duty to protect and preserve the marine environment" and, in Article 194(2), requires them to adopt “all measures necessary to ensure that activities under their jurisdiction or control are so conducted as not to cause damage by pollution to other States and their environment, and that pollution arising from incidents or activities under their jurisdiction or control does not spread beyond the areas where they exercise sovereign rights in accordance with this Convention”. The Convention, on this point, may be codifying general international law.

Finally, let us recall that Principle No. 2 of the 1992 Rio Declaration on Development and Environment underlines that “States have, in accordance with the Charter of the UN and the principles of international law, the sovereign right to exploit their own resources pursuant to their own environmental and developmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national sovereignty”.

Even the International Court of Justice (ICJ), in its Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons of 8 July 1996 recognized that “the environment is under daily threat and that the use of nuclear weapons could constitute a catastrophe for the environment. The Court also recognizes that the environment is not an abstraction but represents the living space, the quality of life and the very health of human beings, including generations unborn. The existence of the general obligation of States to ensure that activities within their jurisdiction and control respect the environment of other States or of areas beyond national control is now part of the corpus of international law relating to the environment”.49

We now have to try and adapt these concepts to the virtual environment of the Internet: so, if environmental pollution is an alteration by means of pathogenic factors of human origin, in the case of the Internet we could refer to “virtual pollution” of the IT environment made by means of malicious software. In our opinion, indeed, the ban should be read not only as relating to the direct dissemination by States of such instruments, but also as an obligation imposed on them, to put in place preventive and repressive measures to prevent such tools from being massively disseminated by private individuals.

It should be clarified that the prohibition does not seem to have such content and scope as to prohibit any State behaviour that involves the design and/or dissemination of any malicious computer tool, but only, and more limitedly,

those with a level of offensiveness capable to block the functioning of the Internet as a whole, or at least one of its main functions and/or branches (one may think, to the blocking of the domain name system, DNS).\textsuperscript{50}

6.4  \textit{D) The Obligation of a Peaceful Use: Cyber Warfare and the Legitimacy of Reactions}

We can now investigate the obligation imposed on States to use the Internet exclusively for peaceful purposes, which (also) derives from the qualification of the same as a common good (as well as, obviously, from the generalized prohibition of the threat and the use of force).

This presupposes the possibility of framing certain informatics tools as weapons, to perform the so-called cyber-war, and implies also the need to frame the range of possible legitimate State reactions.\textsuperscript{51}

We must first of all clarify that with the first expression (cyber-war or cyber-warfare) reference is made to the use by a State of computer tools with the intention of harming other subjects of international law, with an analogous approach to that of traditional (kinetic) warfare, but without necessarily aiming at their \textit{debellatio}.

The traditional definition of war in international law, which, as is well known, conceives it as “a contention between two or more States, through

\footnotesize{
\begin{itemize}
\item \textsuperscript{50} In February 2012, the hacker organization known as “Anonymous” declared that, in order to prevent all financial transactions online, it would have put in place a “global blackout” of the Web, even if only temporary, by means of a concurrent attack to all 13 root servers, as a retaliatory reaction to the global economic crisis; however, either the attack did not take place or the security devices of the DNS system resisted very well, since there were no significant interruptions to the DNS itself.
\end{itemize}
}
their armed forces, for the purposes of overpowering each other and imposing such conditions of peace as the victor pleases\textsuperscript{52} and, therefore, implies the intention of every belligerent to annihilate the adversary. This would exclude from the same category every conflict with more limited objectives, as would happen most of the time in the case of a cyber-war.

More up-to-date definitions, indeed, seem to include armed conflicts with less “ambitious” objectives in the concept: one may think of the one developed by the International Criminal Tribunal for the former Yugoslavia in the \textit{Tadić} case, according to which every “armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State”.\textsuperscript{53}

But a cyber-war and a kinetic one also differ in further elements, mostly linked to the difficulty of identifying, in the former case, the attacking State,\textsuperscript{54} as well as to the limitation of the side effects of such attacks and, consequently, to respect certain rules of \textit{jus in bello}.

So, we will now try to understand whether such activities, if attributable to States, are forms of threat or of use of force, prohibited by contemporary international law.

As is known, the majority interpretation of Article 2(4) of the Charter of the UN, as well as of the corresponding rule of general international law, considers that the prohibition of the threat and use of force provided therein relates \textit{exclusively} to \textit{military} force.\textsuperscript{55}

The prohibition underwent an evolutionary interpretation that includes behaviours such as those we are dealing with, or at least some of them: the ICJ, in the well-known case of \textit{Military and paramilitary activities in Nicaragua}, has included in the prohibition of the threat and use of force (but, as is well known, \textit{not} in the one of armed attack) also activities that are not \textit{directly} attributable to the use of \textit{military} force in the \textit{strict} sense, such as training and

---

\textsuperscript{52} \textit{Oppenheim, International Law}, Roxburgh, 1920, p. 67.
\textsuperscript{53} International Criminal Tribunal for Former Yugoslavia (ICTY) Case No. IT-94-1-AR72, para. 70.
the mere supply of weapons to irregular militias operating on the territory of another State.\textsuperscript{56}

Again, in the 1996 opinion relating to the \textit{Legitimacy of the use of force}, the ICJ also clarified that the UN Charter system does not contain any \textit{mandatory} listing of the concept of “weapon”: on this basis some scholars, in order to update the international legal order to technological evolutions and to meet the need to fight new instruments of threat to international peace and security, have put forward the hypothesis of considering \textit{at least some} cyber-tools as weapons and, consequently, to prohibit them, focusing not on the tool itself.\textsuperscript{57}

Not each and every cyber-attack carried out by one State against another, therefore, is prohibited by the rules on the use of force: the discriminating criterion should be found in the effects it produces, which, have to be comparable to those of a kinetic armed attack and should cause the destruction of property and the loss of human lives.\textsuperscript{58}

Moreover, as the Declaration relating to the principles of international law concerning friendly relations prohibits States from applying economic, political or any other kind of measures or encouraging their use, in order to force another State to subordinate the exercise of its sovereign rights and to obtain benefits of any kind from it,\textsuperscript{59} even cyber-attacks that do not lead to the destruction of property and to the loss of human lives, could be considered prohibited, this time by the principle of non-interference, whether they should be a threat of the use of force.

On the possibility of an armed self-defense reaction from a cyber attack, one should remember that the international legal order distinguishes \textit{minoris generis} violations of the prohibition of the use of force from armed attacks,\textsuperscript{60} and allows only in the latter case, as clarified by the ICJ in the \textit{Nicaragua v. United

\begin{itemize}
\item \textsuperscript{58} On this requirement see BROWNLE, \textit{International Law and the Use of Force by States}, Oxford, 1963, p. 362 ff.
\item \textsuperscript{59} Declaration concerning the principles of international law concerning friendly relations between States, emphasis added, UN General Assembly Resolution No. 2625 of 24 October 1970, Doc. A/RES/2625 (XXV), inwww.un.org.
\end{itemize}

\textit{THE ITALIAN REVIEW OF INTERNATIONAL AND COMPARATIVE LAW 1 (2021) 246–275}

Downloaded from Brill.com04/03/2022 10:45:59AM via free access
States case, an armed reaction in self-defense. Attention, then, must be shifted to the means that can be legitimately used by the State that reacts to a cyber-attack, and, in particular, whether they can take exclusively the same form.

A criterion that can provide aid could be identified in the principle of proportionality or, at least, of not excessive disproportionality of the response, that could lead to conceive as legitimate every armed reaction of the State that has suffered a large-scale cyber-attack which has produced damages comparable to those of a conventional military attack, and that does not infringe jus cogens and international humanitarian law.61

In this sense, some elements of the practice should be mentioned: the 2011 report on cybersecurity transmitted by the Pentagon to the US Congress explicitly declares that the United States will consider legitimate to react with the use of military force against particularly virulent cyber-attacks: “when warranted, we will respond to hostile attacks in cyberspace as we would to any other threat to our country (...) We reserve the right to use all necessary means – diplomatic, informational, military and economic – to defend our nation, our allies, our partners and our interests”. According to this report, all the “significant cyber attacks directed against the US economy, government or military” fall into the category that legitimizes the use of force, and the reaction could involve both the use of electronic means and conventional military options.

And the subsequent US practice moved in the same direction: the various National Defense Authorization Acts (NDAA)62 that have followed over the years, contain many provisions that impact on the US cyber-defence.63

Likewise, interesting is the practice that developed after the cyber-attacks that the Estonian Government, banks and companies suffered in 2007, which originated from Russian IP addresses. On that occasion, the North Atlantic Treaty Organization (NATO), even not defining cyber-attacks as a clear military

---


62 It is the name of a series of federal laws in the United States that specify the annual budget and expenses of the Department of Defense. The first NDAA was approved in 1961.

63 A list of these provisions has been compiled in an Excel file downloadable at: <https://thirdway.imgix.net>. In this regard, see Garcia, “The Militarization of Cyberspace: Cyber-Related Provisions in the National Defense Authorization Act” in ThirdWay, 30 March 2021, available online, which highlights how “across 13 categories, three of the top four were aimed at the Department of Defense’s (DoD) core cyber missions, such as changing organizational processes and structures, protecting DoD assets, and engaging with foreign partners while deterring nation-state adversaries”.

THE ITALIAN REVIEW OF INTERNATIONAL AND COMPARATIVE LAW I (2021) 246 – 275
action, did not deny the possibility of a military reaction, and limited only to excluding the **automatic** application of the provisions on collective self-defence contained in the NATO Treaty to these attacks. It is probable, however, that in this case the “soft” reaction was suggested to NATO by the type of attacks suffered by the Estonian sites, which in no way endangered human lives or assets located in the territory of the attacked State (there’s also to say, indeed, that sometimes hospitals had to stop their treatments for some hours).

What we are dealing with, however, represents a still very fluid branch of the international legal order, in which the behaviour of States is not uniquely oriented and where positions that could also be read as expressions of unilateralism cannot be ignored, also in consideration of the fact that it is almost inevitable that the practice, in this matter, emanates mostly from developed countries.

However, it must also be said that, at the time of writing, there is no news of armed reactions, through conventional tools, against cyber-attacks, probably because none of the latter has ever exceeded the threshold that we have identified as necessary to legitimize a kinetic reaction.

### 6.5  **E) Cyber Terrorism**

Even more complex, then, is to reach a univocal definition of cyber-terrorism.

The literature that has dealt with the issue, in the absence of a generally accepted definition of the same “traditional” phenomenon, has often considered cyber-terrorism as the commission of ordinary computer crimes with the specific intention of instilling fear in a target population.64

The analysis of the practice indicates two definitions of cyber terrorism worthy of particular attention, one emanating from the US Federal Bureau of Investigation (FBI), the other drawn up by NATO.

For the FBI, among the first State bodies to deal with the issue, it would be cyber terrorism any “premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents”.65

---


65 The definition is contained in a brief prepared in 1997 for the FBI Laboratory by special agent M. Pollitt and then published under the title of “Cyberterrorism – Fact or Fancy?”, available at: <www.scribd.com>.
According to this interpretation, therefore, to be a terrorist-type cyber-attack, it is necessary, in addition to the political matrix, that the same 1) is carried out by sub-national groups or clandestine agents (and not, therefore and obviously, by a State regular army), 2) takes place against computer systems, computer programs and data, and 3) produces damage against non-military targets.

NATO’s opinion appears to be partially different: according to its definition, cyber-terrorism is every “cyber-attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society with an ideological goal”. Therefore, all computer attacks for an ideological objective, carried out 1) using or exploiting computer or communication networks, and 2) with the aim of causing destruction or interruption of operations of a sufficiently large size to generate fear or intimidate the target society, fall within the category.

The two definitions, which have in common the psychological element of the political/ideological intent of the action, differ, from a substantive point of view, in that: while in the US perspective, IT structures must be the target of the attack, for the Atlantic Alliance only an attack launched by computers and telecommunications networks would be ascribable to cyber terrorism. Moreover, while the FBI definition takes a position on the subjective profiles of the behaviour, and only includes the operations carried out by independent, or “sponsored” by States (the “sub-national groups” of the text), individuals or groups, thus leaving out the so-called State terrorism, the elaboration of NATO, on this point, remains less defined.

In the absence of significant practice specifically related to cyber-terrorism, to attempt a general definition, it is possible to start from the practice relating to traditional terrorism: in the latter context, in particular, the practice of recent years has witnessed developments which, despite the continuing absence of a generally shared definition, includes terrorism in any activity attributable to individuals or groups of individuals not accountable to any State (in the sense that they do not act on its behalf or with its protection) who engage in acts of indiscriminate violence directed against both civilian and military/governmental targets.

66 The definition is reported by an Alliance official, Everard, in his NATO and cyberterrorism paper, in the official paper “Responses to cyber terrorism edited by NATO’s Center of Excellence Defense Against Terrorism” published in Ankara in 2007.

To fall into the category it is also necessary that the behaviour is also characterized by the psychological element of the destabilization of the world order as understood by the generality of States.

Therefore, both State terrorism, which must be traced back to the violation of other, more general, obligations of international law and in particular of the generalized prohibition of the use of force, and, for substantially similar reasons, the one sponsored by States are excluded from such a definition.68

On this basis, we can affirm that a definition of cyber terrorism as emerged from recent practice and that is substantially compatible with the one of “classic” terrorism could draw its objective element from the text adopted within NATO. This could allow us to include all harmful activities carried out using IT tools, regardless of their target and would have the advantage of unifying cyber terrorism and cyber war in a single category of behaviours, which would therefore be distinguished on the basis of the nature of the aggressor (organization of individuals in the first case, of the State in the second one).

7 The Governance of the Domain Name System and of ICANN as an Indication of a Tendency Towards the Informalization of the International Legal Order

Since the dawn of the Internet, the management of the Domain Name System (DNS), which allows users to identify websites by typing names that are easy to memorize (domain names, in fact) instead of their respective numerical network addresses (IP addresses), and therefore represents the indispensable “directory” of the Web, fundamental for its functioning and its very existence, had always been unilaterally carried out by the US.69

It must also be said that the US government had originally conceived its role as temporary: the Statement of Policy on the Management of Internet Names

---

68 Draetta, “The Internet and Terrorist Activities”, in Bianchi (ed.), cit. supra note 64, p. 453 ff.: “it seems that the notion of cyber terrorism is insufficiently defined and addressed in the international conventional law, with the exception of the regional integration at the EU level, where such a notion seems to be emerging with sufficiently precise contours. As to terrorist acts carried out through the internet, international legal instruments dealing with cybercrimes do not yet contain specific provisions for terrorism, as they do for child pornography, infringement of intellectual rights, racism and xenophobia. There is here a definite need for improvement”, p. 464.

69 There’s to say that the US Department of Commerce had a supervisory role on “global” policies and procedures. However, other policies and procedures – e.g. those governing the so-called country code Top-Level Domains (ccTLDs) – were and are in the hands of the ccTLD manager to which the ccTLD was “delegated”.

---
and Addresses adopted on 10 June 1998 by the US Department of Commerce contains a commitment to a transition that would allow the private sector to have a dominant role in the management of the DNS. Many declarations issued over time by the US have repeatedly recognized their intention to preserve security and stability of the DNS and, consequently, the commitment to avoid measures that could have negative effects on its efficiency.

Although the practice had not registered many formal protests from other States to the legitimacy of the exclusive authority of the US government over the DNS (and this even though the servers on which the related data are stored are scattered over the entire surface of the planet, and therefore also outside the US national territory) in 2003, the UN WSIS, convened by the General Assembly by its resolution 56/183 of 21 December 2001, discussed and studied the mechanisms for guaranteeing a wider international involvement in Internet governance, and in particular in the management of the DNS.

The study was conducted by the Working Group on Internet Governance (WGIG), a multistakeholder institution, whose task, assigned by the WSIS, was precisely “to investigate and make proposals for action, as appropriate, on the governance of the Internet”.

The work of the WGIG ended with a report that recognized that no government should play a prominent role in Internet governance and pushed for greater internationalization, even proposing the establishment of a new “global” consultative body, the Internet Governance Forum (IGF), which is today assigned the task of discussing public policies related to the key elements of Internet governance in order to promote its sustainability and to keep the debate open between all bodies who deal with it.

70 Available at: <www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses>. As can be seen from the quoted text, the original intention was, therefore, to hand over the governance of the DNS system to the “private” sector. We will see later if this is about to happen and in what form.


72 The only noteworthy exception was that emanating from the Brazilian government, we reconstructed in Ruotolo, cit. supra note 34.

73 A root server map can be found at: <public-root.com/root-server-locations.htm>.


75 We use the expression to refer to groups whose composition contemplates the participation of representatives of States and international organizations, alongside with non-governmental organizations (NGOs) and private individuals.

76 On 13 December 2015 the UN General Assembly approved a document on the overall review of the implementation of the outcomes of the World Summit on the Information Society which, among other things, extended for 10 years the mandate of the IGF; Doc. A/70/L.33, available at: <unbisnet.un.org>.
Furthermore, it promotes *ex ante* and evaluates *ex post*, on an ongoing basis, the implementation by States of the Principles adopted during the WSIS and addresses the issues related to the critical resources of the Internet.\(^7\)

The WSIS also proposed four distinct possible regulatory models for the Web, two of which involved the creation of UN-related bodies; according to three of the four proposed models, the Internet Corporation for Assigned Names and Numbers (ICANN),\(^7\) a US private non-profit organization established in 1998 by California State regulations which manages the functioning mechanisms of the Web, should have been supplanted by an intergovernmental body, or should have been accountable to it.

The conclusions of this report should have been the starting point of the second phase of the Summit, held in Tunis in 2005, where, however, there was a blockage of the negotiations on the internationalization of the governance of the Web, when the US delegates, as requested by Congress, strongly opposed to the transferring of the administration of the DNS to any international body.

From 2010, the issue of the role of States in the global governance of the Internet returned to the attention of the international community, since many countries, including the US and the European Union, pushed for an increase in their role within ICANN while others, such as Brazil, South Africa and India were trying to revive the proposals for the establishment of an international regulatory body within the UN system, capable of absorbing the already existing bodies (ICANN *in primis*). A third group of States, including Russia and China, pushed for an international *consensus* on the basis of which to adopt an International Code of Conduct for Information Security within the UN, in

\(^7\) To date, the **IGF** met fifteen times: from 30 October to 2 November 2006 in Athens in Greece, from 12 to 15 November 2007 in Rio de Janeiro in Brazil, from 3 to 6 December 2008 in Hyderabad in India, from 15 to November 18, 2009 in Sharm El Sheik in Egypt, from 14 to 17 September 2010 in Vilnius in Lithuania, from 27 to 30 September 2011 in Nairobi in Kenya, from 6 to 9 November 2012 in Baku in Azerbaijan, from 22 to 25 October 2013 in Bali in Indonesia, from 2 to 5 September 2014 in Istanbul in Turkey, from 10 to 13 November 2015 in Brazil, from 6 to 9 December 2016 in Jalisco in Mexico, from 18 to 21 December 2017 in Geneva in Switzerland, from 12 to 14 November 2018 in Paris, at UNESCO, from 25 to 29 November 2019 in Berlin. The 2020 edition, due to the COVID-19 pandemic, was held online. For a reconstruction of the activity of international organizations in the field of Internet governance, also for further bibliographical indications, we would like to refer to Ruotolo, "Internet (diritto internazionale)", Enciclopedia del diritto, Milano, p. 545 ff.

the form of a General Assembly resolution.\textsuperscript{79} A revised version of this Code, proposed to the General Assembly in January 2015, reiterates that “all States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet”.\textsuperscript{80}

In 2013 the main organizations responsible for the technical management of the Internet – ICANN, IETF, Internet Society (ISoc)\textsuperscript{81} – gathered in Montevideo and adopted the Statement on the Future of Internet Cooperation, which called for an acceleration of the globalization of the functions of ICANN and IANA (Internet Assigned Numbers Authority, the section of ICANN, which actually manages the DNS) towards a model in which all interested parties, including Governments, would participate on an equal footing.\textsuperscript{82}

Despite all these attempts, until 2016 (when the transfer process in favour of ICANN was finally perfected) the US continued to manage the DNS system:\textsuperscript{83} this raised, from an international law perspective, issues relating to the legitimization of that power, since, as we said, the servers on which the same power is exercised are (also) located outside the US.

Essentially, two distinct reconstructive models have been proposed to identify the legal title of the exercise of that power: the first uses “traditional” elements of international law, the second, instead, refers to models borrowed from global administrative law.\textsuperscript{84}

\textsuperscript{79} Doc. A/66/359.
\textsuperscript{80} General Assembly, 9 January 2015, letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, 13 January 2015, p. 5, available at: <regmedia.co.uk/2015/02/04/un-internet-security-13jan15.pdf>.
\textsuperscript{81} Internet Society (ISoc) is an international non-governmental organization – founded in 1992 by Vinton Cerf, Robert Kahn, Jon Postel and other pioneers of the Net – dedicated to fostering the free, fair, universal and stable development of the Internet and to promote its beneficial uses for all humanity.
\textsuperscript{82} The Statement is available at: <www.icann.org/news/announcement-2013-10-07-en>.
\textsuperscript{84} As is well known, global administrative law is a reconstructive model resulting from the doctrinal elaboration of a group of American scholars at the beginning of this century. See BOISSON DE CHAZOURNES, \textit{cit. supra} note 20; CHESTERMAN, “Globalization and Public Law: a Global Administrative Law?”, in FARRALL and RUBENSTEIN (eds.), \textit{Sanctions, Accountability and Governance in a Globalized World}, Cambridge, 2009, p. 75 ff.; D’ALBERTI,
Following the first model, the said power, explicating itself on objects located in geographic areas that are outside the US territory, had to be read as a form of extraterritorial exercise of coercive power or government, which finds a territorial limit in the customary principle of non-interference, a principle which can be legitimately waived only by specific customary or treaty provisions (and in this case the relative rules would have permissive content) or authorizations (be they explicit or implicit) of the territorial sovereign, that is to say, in the DNS case, by the States on whose territory the servers are located.

In the impossibility of identifying international law rules, be they customary or treaty, which would give the US the legitimacy to carry out, outside its territory, actions that have the effect of modifying the DNS root file, as well as in the impossibility of tracing back explicit declarations of authorization for such changes by the States in whose territory DNS servers are located, such actions could find their legitimacy in the silent compliance with this activity. As regards the methods of exercising this power, the US Federal Government – recognizing the existence of a qualified interest of other States to ensure the stability and security of the DNS system – always collaborated with them to

---


86 The principle, whose discussion is impossible here, is peacefully recognized as part of general international law and is generally conceived as “a corollary of every State’s right to sovereignty, territorial integrity and political independence”; OPPENHEIM, cit. supra note 52, p. 428. The Declaration of the UN General Assembly on Friendly Relations between States (Res. 2625 (XXV), 1970) contains an entire section on the principle in question “concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter”; the same General Assembly, moreover, had previously adopted a Declaration “on the Inadmissibility of Intervention and Interference in the Domestic Affairs of States” (Res. 2131 (XX) 1965).
preserve this fundamental need, explicitly admitting the existence of a common interest in the permanence of the functionality of the Web, as an asset of “global” importance.

In short, the State that exercised the exclusive power of governance of the DNS system, at the same time, recognized the existence of a global need to ensure its functioning, and that the same need was somehow attributable to fundamental interests of the international community as a whole.

Also the second model starts with the consideration of the existence of a common and basic interest of the States to ensure the Internet’s functionality, but reads the exercise of the US power of governance as one of the forms in which global administrative law expresses. So, reference was made to the exercise of administrative powers by domestic administrations at a level that involves not only the legal order and the interests of their State of origin, but also legal systems and, again, interests of different States, in order to pursue common objectives. This leads to the emergence of forms of “administrative” law of transnational relevance (to be understood as the legal discipline of public administrations and their relations with individuals), in all those cases in which the objective to be achieved needs a “mixed” mechanism, in which a more strictly administrative regulation is grafted onto a system of basic rules provided for by international law.

In particular, the DNS case could be read as a “distributed administration”, put in place by a specific State (the US) entitled to perform functions of “global” importance, by virtue of a common, recognized interest.


88 The fundamental interests of the international community, and the ways to guarantee their protection, is a topic on which internationalist scholarship has largely concentrated, starting from theoretical premises that are often very different from each other and with multiple and differentiated outcomes. For some different perspectives see. GAJA, “The Protection of General Interests in the International Community”, rcadi, Vol. 364; IOVANE, La tutela dei valori fondamentali nel diritto internazionale, Napoli, 2000; PICONE, Comunità internazionale e obblighi “erga omnes” – Studi critici di diritto internazionale, Napoli, 2013; VILLALPANDO, “The Legal Dimension of the International Community: How Community Interests Are Protected in International Law”, European Journal of International Law, 2010, p. 387 ff.

ICANN itself was seen as a sort of paradigm of another form of global administration, the “hybrid intergovernmental-private administration”, as it was established as a purely non-governmental body but, over time, it involved representatives of national governments and international organizations, within the Governmental Advisory Committee. In that context, State actors – who are bound both by domestic and international law – operate alongside private actors, who are not, at least directly, subject to international law constraints, and can become bearers of competing interests.

The recognition of the existence of a common interest of the States in the continuing functionality of the Web, represents one of the conditions that led the US administration to complete the procedure for the transfer of the DNS system governance to the so-called “global community”.

This expression is generally used to refer to the constellation of all entities that carry out activities of international relevance, even though not subjects of international law, and which therefore includes, alongside States and international governmental organizations, also non-governmental organizations, multinational companies, and individuals.

In order to regulate their relations, all these bodies increasingly use, alongside rules belonging to the classic sources of international law, also regulatory instruments, organizational structures and “atypical” decision-making procedures, characterized, in particular, by a high degree of informality.

These structures aim to put in place different forms of cross-border cooperation between public authorities in contexts that differ from an international organization (through, therefore, processes of informal nature), between actors that differ from those that traditionally manage international relations (between subjects, therefore, which only partially fall within those formally classified as subjects of international law).

---

90 Kingsbury, Krisch and Stewart, “The Emergence of Global Administrative Law”, Law & Contemporary Problems, 2005, p. 2 ff., which, in addition to the example of ICANN also cite the “Codex Alimentarius Commission, which adopts standards on food safety through a decisional process that now includes significant participation by non-governmental actors as well as by government representatives, and produces standards that gain a quasi-mandatory effect via the SPS Agreement under WTO law”.

91 The expression is expressly used in the NTIA press release we have cited above.

92 Iriye, Global Community: The Role of International Organizations in the Making of the Contemporary World, Oakland, 2004, p. 209 ff. includes “all organizations—the State, business enterprises, international organizations, and nongovernmental associations” which, collectively form what Kofi Annan, former Secretary general of the UN, called a "strategic partnership".
The same structures are based, use and produce rules different from international treaties or other sources of international law (and equally informal, therefore, is their “regulatory output”).

Even the nomenclature used to define these instruments, which does everything to avoid the more traditional expressions of “treaty”, “agreement”, “international organization” and the like, is an important index of this informalization.

To give some examples, in addition to ICANN, we can cite, among others, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, the International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use, the Kimberley Process Certification Scheme, the Proliferation Security Initiative, the International Competition Network, the Financial Stability Board, and the Basel Committee on Banking Supervision.

In this regard, the doctrine has spoken of informal international lawmaking. The reasons for the emergence of such a model in practice are manifold, but all originate from the increasingly frequent existence of relationships and interests that transcend both State borders and States as centres of interests.

For this reason, they are not effectively manageable by the traditional operators of international law alone, through formal processes, and through the rules developed in such procedures, which involve mostly the expression of State consent.

Moreover, as has been effectively stated, the legal discipline of new technologies is often made particularly complex, and difficult to pursue through traditional instruments, due to the fact that they transform too quickly to be easily regulated.

It must also be clarified that the phenomenon is not even superimposable to the well-known and in any case composite category of soft law, and this for two reasons: the latter, first of all, collects rules produced by traditional subjects of international legal order, through “classic” processes, and secondly and


96 BROWNSWORD and YEUNG, “Regulating Technologies: Tools, Targets and Thematics”, in BROWNSWORD and YEUNG (eds.), cit. supra note 95, p. 5.
above all, because the “informal” rules we speak of have very little of soft, in the sense of vague, non-binding, not shared, since failure to comply with them implies the deprivation of the possibility of using the resource they govern.

In the latter sense, the sources relating to Internet governance seem paradigmatic: think of the ineluctable need to comply with the RFCs we talked about, or the rules envisaged for the DNS system.

But we need to clarify that, even with reference to the “informal” structures, State consent still plays a decisive role: but, in such cases, it is expressed in a peculiar manner and contexts.

In short, the surfacing “novelties” we studied concern the emergence of unprecedented procedural rules and do not imply the overcoming of the post-Westphalian structure of international law and legal order.

As has been well said, indeed, “global” law neither replaces international law (and so it does not abolish its “rules made of stone”, to answer the question in our title…) nor embodies an exclusive legal order of its kind:97 the State still remains at the centre of the system (one may think, for example, to the role that the US consensus played in the transition to the new governance of the DNS system) and continues to hold the monopoly of force (think of cyber warfare…).

The system is not (at least not yet) characterized by the emergence of new subjects, but, more simply, of new regulatory procedures.

In short, the discipline of international law of the Internet seems to be built through the competition of regulatory models (the Internet regulations we mentioned in our title) of traditional international law, such as the regime of the common heritage of mankind, in particular as for the limitations imposed on States, and informal regulatory models, which instead are applied to broaden the number of subjects participating in the governance of the Internet.

The latter, to which it has to be added the birth, lastly, of the Facebook Oversight Board, the body for controlling the legitimacy of the information published or censored by the social network, joining a broader trend, contribute to the consolidation of the “informalization” of the contemporary international legal order.