Defining Cyberspace in the Context of the Law

Peter R. Stephenson
University of Leicester School of Law

Abstract

In "Defining a Cyber Jurisprudence" the author provides several definitions required for a clear understanding of cyber law[1]. These definitions are based, largely, upon a definition of cyber science (Definition 1). However, this, and subsequent definitions depend upon a primary, or axiomatic definition of cyberspace. That paper provides no such definition.

The purpose of this paper is to set out an axiomatic definition of cyberspace that can be used to support the definitions in [1] and future definitions in a legal context. However, this is not intended to be a detailed treatise on the technical aspects of cyberspace and its various components such as private networks, the Internet, Clearnet and Darknet. Rather, it applies accepted technical definitions such that a framework for discourse regarding law in cyberspace is logical.

Keywords— law, cyberspace, cyber science, cyber law, cybercrime, Internet law

I. Introduction

In [1] the author develops five definitions that are fundamental to a discourse on cyber jurisprudence:

- Definition 1 – Cyber science
- Definition 2 – Cyber law
- Definition 3 – Cyber crime
- Definition 4 – Cyber tort
- Definition 5 – Cyber jurisprudence

In each of these definitions an axiom that defines the concept of cyberspace is implied.

However, such an axiom has not been provided and definitions on the Internet are numerous and varied. The Oxford Living Dictionaries[2] has a good starting point, however:

> *The notional environment in which communication over computer networks occurs.*

Black's online law dictionary[3] offers a much more convoluted definition, this time with a legal twist:

> *The realm where computer communications and simulations are used on the internet. It is like the human psyche translated to the internet. The objects are not physical and made up of data manipulation.*

Using this as a starting point, we examine other, broader, definitions and apply legal principles to arrive at a definition which defines cyberspace clearly, concisely and unambiguously.

We begin with a survey of applicable definitions that we can use as starting points. This survey is not intended to – nor can it be, practically – exhaustive. It is, however, representative of current thinking.

We then distil these representative definitions into a single, albeit somewhat technical, definition. Give that definition, we apply applicable legal principles that result in a definition that addresses cyberspace from a perspective that does not preclude jurisprudential interpretation.

[1] Peter R. Stephenson, 'Defining a Cyber Jurisprudence' (Conference on Digital Forensics, Security and Law, Daytona Beach, 16 May 2017)

[2] 'Definition of cyberspace in English' (*Oxford Living Dictionaries*) <https://en.oxforddictionaries.com/definition/us/cyberspace> accessed 7 July 2017

[3] 'What is Cyberspace?' (*Black's Law Dictionary Free Online Legal Dictionary 2nd Ed*) <http://thelawdictionary.org/cyberspace/> accessed 7 July 2017

II. Survey of Definitions of Cyberspace

There is a tendency in law circles to characterize cyberspace with the Internet. For example, Duhaime's Law Dictionary[4] defines cyberspace as:

> *Synonymous with Internet; a decentralized but interconnected body of data and self-maintained telecommunications network.*

The NATO Cooperative Cyber Defense Centre of Excellence provides 23 separate definitions, each representative of a particular nation where that definition prevails[5].

Here, too, confusion and ambiguity reign [5].

UK:

> *An informal word first thought to have been used by novelist William Gibson to refer to the total data on all computers on all the networks in the world. The word has passed into common use as a way of referring to any large collection of network-accessible computer-based data.*

Turkey:

> *The environment which consists of information systems that span across the world including the networks that interconnect these systems.*

The Netherlands:

> *For the purposes of this strategy, "cyberspace" is understood to cover entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases, relates in some way to the data (source code, information, etc.) present in this domain.*

Latvia:

> *Cyber space is an interactive environment that includes users, networks, computing technology, software, processes, information in transit or storage, applications, services, and systems that can be connected directly or indirectly to the Internet, telecommunications and computer networks. Cyber space has no physical borders.*

International Organization for Standardization:

> *The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.*

United States:

> *The notional environment in which communication over computer networks occurs*

These, and other, national definitions have a few concepts in common:

- Communication
- Networks
- Users
- Information technology
- Lack of physical form
- Global
- No borders

[4] 'Cyberspace Definition' (*Duhaime's Law Dictionary*) <http://www.duhaime.org/LegalDictionary/C/Cyberspace.aspx> accessed 7 July 2017

[5] 'Terms and Definition - Cyber Space' (*The NATO Cooperative Cyber Defence Centre of Excellence*) <https://ccdcoe.org/cyber-definitions.html> accessed 7 July 2017

Hardy, in a 1994 paper gives a perspective from that time period[6]:

> *Much commentary in the popular and legal press these days raises legal questions relating to electronic communications over computer networks. Popularly, the world of such communications is often called "cyberspace," a term that this article will also use as a convenient shorthand.*

Unfortunately, the notion of a "convenient shorthand" still prevails. It is, perhaps, notable, however, that some core concepts still are included in this 23-year-old definition:

- Communication
- Networks

Ma, et al, introduce an important concept: the online community aspect of cyberspace[7]. This online community is analogous with physical communities such as cities, states and nations. In these cases, as in cyberspace, there is some unifying factor that may or may not be offset by the similarities and differences of the members of the community.

In a thesis addressing information dominance[8] reference is made to the convergence of soft and hard power. Hard power comprises cyber events – those events that require cyberspace. Soft power comprises pure information and thought.

The hard power end is referred to as the cyber end of a continuum that stretches to the realm of information called the noosphere. The convergence is the infosphere. It is the infosphere – the convergence of pure cyber with pure information – that describes, but does not necessarily define, cyberspace.

III. General Framework

Table 1 summarizes the most prevalent terms used by descriptions or definitions of cyberspace.

network	11
Global	7
communication	5
information	5
infrastructure	4
technology	4
people	3
complex	2
users	2

Table 1 - Prevalence of descriptive terms in definitions of cyberspace

If we use these as our starting point we get something akin to:

> *Cyberspace is a complex global communication network, based upon a technological infrastructure where people can exchange information easily and quickly.*

This captures the technical essence of cyberspace but it leaves some important questions unanswered. For example, if cyberspace is a contiguous global network, what are the jurisdictional and choice of law ramifications?

Where does cyberspace begin and end? [1] gives us several definitions, most of which reference cyber science which, in turn, assumes that we know the answer to this. Knowing where cyberspace begins and ends is critical. Today it is not uncommon for the courts to view an action that has begun in the physical space and moved to cyberspace as being a cyber event. Referring back to definition 1:

> *Cyber science is the study of phenomena caused or generated within the cyber space, which may or may not interact with phenomena caused or generated within the physical space.*

We see that it is imperative that we know where the demarcation is between physical and cyber space.

[6] I. Trotter Hardy, *The Proper Legal Regime for 'Cyberspace'* (William & Mary Law School Scholarship Repository 1994)

[7] J. Ma and others, *Perspectives on Cyber Science and Technology for Cyberization and Cyber-Enabled Worlds* (2016)

[8] Peter R. Stephenson, 'Information Dominance as an Affirmative Countermeasure against International Terrorism' (MA, Norwich University 2007)

IV. Analysis and Definition Development

We begin with the rough statement from Section III:

> *A complex global communication network, based upon a technological infrastructure where people are able to exchange information easily and quickly.*

Digging a bit deeper, and addressing the aspect of community, we can begin to think of cyberspace as a community with citizens ("netizens"?) and a finite boundary. That boundary is, at first, a bit fuzzy since it subsumes the physical boundaries of all of the nations of the globe.

There are a couple of other definitions that we should note, beginning with the first definition by Gibson[9]:

> *[Cyberspace is] a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematic 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. Like city lights, receding.*

Back in 2008, then Deputy Defense Secretary Gordon England in an official use only memo[10] defined cyberspace as:

> *… a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.*

There are elements of these definitions that lend themselves to legal use. If we consider a few of the primary jurisprudential aspects of the law we get some guidance. For example, in the paper cited in footnote 1 we see some specific definitions whose elements we should consider from the perspective of consistency. In other words, nothing in our definition may preclude the application of these elements. Definitions 1 – 5 below are from the paper cited in footnote 1.

- DEFINITION 1 – Cyber Science

Cyber science is the study of phenomena caused or generated within the cyber space, which may or may not interact with phenomena caused or generated within the physical space.

- DEFINITION 2 – Cyber Law

Cyber law is the set of obligations and duties applied to events related directly to cyber science.

- DEFINITION 3 – Cyber Crime

A cybercrime is crime or misdemeanor occurring in the space defined by cyber science and comprising an act committed or omitted, in violation of public law either forbidding or commanding it.

- DEFINITION 4 – Cyber Tort

A cyber tort is a breach of duties fixed and imposed upon the parties by the law itself in the space defined by cyber science without regard to their consent to assume them, or their efforts to evade them that causes harm.

- DEFINITION 5 – Cyber Jurisprudence

Cyber jurisprudence is the legal study that concentrates on the logical structure, the meanings and uses of its concepts, and the formal terms and modes of operation of cyber law.

Those elements are:

[9] William Gibson, *Neuromancer* (Ace Books 1984)

[10] Gordon England, (Deputy Secretary of Defense 2008)

- obligations and duties
- an act committed or omitted, in violation of public law either forbidding or commanding it
- duties fixed and imposed upon the parties by the law itself
- logical structure, the meanings and uses of its [legal study] concepts, and the formal terms and modes of operation
- phenomena caused or generated

Now, we add some elements of some of the 28 recognized definitions of cyberspace[11]:

- information infrastructure[12].
- metaphor for the non-physical terrain created by computer systems (Google)
- The notional environment within which electronic communication occurs [5]
- The information space consisting of the sum total of all computer networks [13]

Next, we add some elements from the definitions in section III:

- network
- Global
- communication
- information infrastructure
- technology
- people
- complex

Finally, we look to the law and the ways that it has handled the concept of cyberspace in the past. An excellent characterization is found in Barrett v. Rosenthal. 114 Cal.App.4th 1379, 9 Cal.Rptr.3d 142:

> *Moreover, the Internet is not a separate physical place, like a hallway in an apartment building, but "a decentralized, global medium of communications—or 'cyberspace'—that links people, institutions, corporations and governments around the world.*

In Reno v. Am. Civil Liberties Union, 521 U.S. 844, 117 S. Ct. 2329, 138 L. Ed. 2d 874 (1997), the United States Supreme Court characterized cyberspace as a collection of on-line tools:

> *... as presently constituted, those most relevant to this case are electronic mail (e-mail), automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.*

This approach is typical of the way the courts handle cyberspace issues. Much of the time the courts apply the same principles as they would apply in physical space to issues in cyberspace. Jaynes v. Commonwealth of Virginia, 276 Va. 443, Supreme Court of Virginia, September 12, 2008:

> *Conduct which is not prohibited in the physical world should not be subject to prosecution merely because it occurs in the virtual world of the Internet and cyberspace.*

We find a similar approach in 168 Cal.App.4th 414 (2008):

> *[W]e shall conclude that territorial jurisdiction to prosecute lies under the traditionally applicable legal principles, and it makes no difference that the*

[11] Daniel T. Kuehl, 'Part I. Foundation and Overview' in Stuart H. Starr Franklin D. Kramer, Larry K. Wentz (ed), *Cyberpower and National Security* (Center for Technology & National Security Policy 2009)

[12] Edward Waltz, *Information Warfare Principles and Operations* (Artech House Publishers 1998)

[13] Dorothy E. Denning, *Information Warfare and Security* (Addison-Wesley Professional 1999)

charged conduct took place in cyberspace rather than real space.

The point here is that courts often equate the cyber space with the physical space, through a lack of understanding it would seem, and a useful definition of cyberspace should accommodate *stare decisis* wherever practical.

Also, because we are not arguing jurisdiction at this point, we must ensure that our definition is sufficiently broad to accommodate that debate when it comes.

We find, therefore, that we must put the emphasis on the technology infrastructure as the servant of people (users). It may neither depend upon nor may it preclude sovereignty. Sovereignty is defined by Viridiana Maldonado[14]:

> *Sovereignty is understood in jurisprudence as the full right and power of a governing body to govern itself without any interference from outside sources or bodies.*

This leads us to a working definition of cyberspace that we can use in a legal context.

> *Definition of Cyberspace*
>
> *Cyberspace is a complex global information infrastructure that facilitates communication between technology such as computers, networks and other digital systems, both independently and on behalf of people using it. Cyberspace is distinct from physical space and the constraints imposed by it such as geographic boundaries.*

This implies that a physical space with a geographic boundary – a state or nation, for example, could have a "cyberspace" associated with it in much the same way as it has an "airspace". Certainly, this could become important in debates about jurisdictions in cyberspace as well as choice of laws.

Finally, if we accept the cyberspace/airspace analogy, where does a geographic territory's cyberspace extend? Is it from the starting or ending point of an activity?

These questions will impact – and be impacted by – choice of law debates and there is some current opinion that attempts to simplify the question. For example, Ragonese v. Rosenfeld, et al. Ragonese v. Gaston Rosenfeld, Traveltronics Inc., Aerolineas Argentinas, Mario Zatocki and Zamar Viajes Inc. 318 N.J.Super. 63, Superior Court of New Jersey, July 20, 1998:

> *Generally, the debate over jurisdiction in cyberspace has revolved around two issues: passive web sites versus interactive web sites, and whether a defendant's Internet-related contacts with the forum combined with other non-Internet related contacts are sufficient to establish a persistent course of conduct.*

This is beyond the scope of this paper except to show that our definition is not in conflict with jurisdictional positions such as we see in Ragonese v. Rosenfeld, et al.

V. Bibliography

'Cyberspace Definition' (*Duhaime's Law Dictionary*) <http://www.duhaime.org/LegalDictionary/C/Cyberspace.aspx> accessed 7 July 2017

'Definition of cyberspace in English' (*Oxford Living Dictionaries*) <https://en.oxforddictionaries.com/definition/us/cyberspace> accessed 7 July 2017

'Terms and Definition - Cyber Space' (*The NATO Cooperative Cyber Defence Centre of Excellence*) <https://ccdcoe.org/cyber-definitions.html> accessed 7 July 2017

'What is Cyberspace?' (*Black's Law Dictionary Free Online Legal Dictionary 2nd Ed*) <http://thelawdictionary.org/cyberspace/> accessed 7 July 2017

Denning DE, *Information Warfare and Security* (Addison-Wesley Professional 1999)

England G, (Deputy Secretary of Defense 2008)

Gibson W, *Neuromancer* (Ace Books 1984)

[14] Viridiana Maldonado, 'What is sovereignty and why is it an essential element of a state?' (*Quora*, 9 Dec 2015) <https://www.quora.com/What-is-sovereignty-and-why-is-it-an-essential-element-of-a-state> accessed 9 July 2017

Hardy IT, *The Proper Legal Regime for 'Cyberspace'* (William & Mary Law School Scholarship Repository 1994)
Kuehl DT, 'Part I. Foundation and Overview' in Franklin D. Kramer SHS, Larry K. Wentz (ed), *Cyberpower and National Security* (Center for Technology & National Security Policy 2009)
Ma J and others, *Perspectives on Cyber Science and Technology for Cyberization and Cyber-Enabled Worlds* (2016)
Maldonado V, 'What is sovereignty and why is it an essential element of a state?' (*Quora*, 9 Dec 2015) <https://www.quora.com/What-is-sovereignty-and-why-is-it-an-essential-element-of-a-state> accessed 9 July 2017
Stephenson PR, 'Information Dominance as an Affirmative Countermeasure against International Terrorism' (MA, Norwich University 2007)
——, 'Defining a Cyber Jurisprudence' (Conference on Digital Forensics, Security and Law, Daytona Beach, 16 May 2017)
Waltz E, *Information Warfare Principles and Operations* (Artech House Publishers 1998)