Do We Need to Impose More Regulation Upon the World Wide Web? - A Metasystem Analysis

John P. van Gigch

vangeditor@aol.com

Abstract

Every day a new problem attributable to the World Wide Web's lack of formal structure and/or organization is made public. What arguably could be represented as one of its main strengths is rapidly turning out to be one of its most flagrant weaknesses.

The intent of this article is to show the need to establish a more formal organization than presently exists over the World Wide Web. (This article will use the terms the Internet and Cyberspace interchangeably.) It is proposed that this formal organization take the form of a metacontrol system-- to be explained-- and rely, at least in part, for this control to self-regulate. The so-called metasystem system would be responsible for preventing some of the unanticipated situations that take place in cyberspace and that, due to the web's lack of maturity, have not been encountered heretofore. Some activities, such as the denial-of-service (DoS) attacks, may well be illicit. Others, like the question of establishing a world-wide democratic board to administer the Internet's address system, are so new that there are no technical, legal or political precedents to ensure its design will succeed.

What is needed is a formal, over-arching control system, i.e. a "metasystem," to arbitrate over controversies, decide on the legality of new policies and, in general, act as a metalevel controller over the activities of the virtual community called Cyberspace. The World Wide Web Consortium has emerged as a possible candidate for this role.

This paper uses control theory to define both the problem and the proposed solution. Cyberspace lacks a metacontroller that can be used to resolve the many problems that arise when a new organizational configuration, such as the Internet, is created and when questions surface about the extent to which new activities interfere with individual or corporate freedoms.

Keywords: World Wide Web, as an organization; The meaning of virtual; Control; Disruptive activities; Hacker attacks & viruses, defense against; Metasystem control; Regulation; Imperatives of control.

Defining the Web as an Organization

Let us first make a list of the **agents** and **components** constituting the web.

- **Equipment**, such as satellites, computers, servers, switches, and other ancillary hardware and software used to create the web.
- **Web Sites**, of which to date there are millions.
- **Information**, in the form of data, messages, e-mail, records, files, reports that either circulate through the web or are stored in the storage devices of web members.
- **Individuals**, who, at any one time or another, are logged-in and interact in cyberspace. All individuals are "created equal," in the sense that nothing distinguishes "good guys" from "bad guys," hackers from non-hackers. **Individuals** represents anyone who has any connection to the web, either as a customer, an Internet Service Provider (ISP) operator, a member of a firm, or just a single participant without any formal affiliation.
- **Providers**, such as the Internet Service Providers (ISPs) who have gone through the legal formality to obtain a corporate identity. America-On-Line (AOL) is an example of a company that charges a fee for connecting individuals to the web and provides others with access to web resources.
- **Companies** that carry out activities on it and whose employees use the Internet to transact their company's business. Each company has a network of servers that are connected to the web through many portals.

The web is said to be a "**virtual organization**" as distinguished from the so-called "**traditional organization**." This leads to the question that needs to be answered at the outset.

Has the advent of cyberspace changed what is meant by the concept of **organization**?

The Traditional Organization

Until recently, **organizations** could be defined as congregations of individuals committed to the achievement of a common mission or goal. A traditional organization was defined in terms of a hierarchy of jobs and its incumbents who reported to each other. The top of the hierarchy was occupied by the individual with the most responsibility. Lower levels reported to higher levels and so on. Other conceptualizations of the organization exist. However, they mostly revolve around the way that its members are **physically** related to accomplish a definite goal.

Physical Space and Cyberspace.

The concept of Cyberspace is still evolving, but several configurations can already be perceived. Cyberspace can be viewed as:

a) a **community** of individuals (connected through a network of electronic connections),

b) a **network** of computers and other machines that communicate with each other, and

c) a **virtual organization**, a connotation discussed below.

The differentiation between physical space and cyberspace is subtle. **Physical space** refers to that aspect of reality visible to the naked eye. **Cyberspace** refers to an ethereal reality in which information in the form of communicated messages are transmitted and coexist. Cyberspace is "real"--it is not imaginary--but it does not exhibit physical reality. One cannot touch cyberspace, although the servers, switches and messages that make cyberspace possible do themselves exhibit a physical reality.

The Meaning of Virtual

One definition of "**virtual**" given by the Oxford dictionary (1976) is "for practical purposes." Labeling cyberspace as a virtual organization means that for practical purposes we can view it as an organization, but in actual fact, it is not. "Virtual" can also be used in the sense of "fictitious" i.e. the "virtual organization" does not exist in "the real sense," but exists "in lieu of the real thing." "Virtual" has also been used to denote an object or event that has the properties that are similar to the object or event it purports to replace. To state that cyberspace is a **virtual organization** denotes that the entity in question differs from the traditional embodiment of the organization. It is not a formal, actuarial legal entity. It is devoid of the usual trappings of a business organization, such as buildings, offices, and formal job descriptions.

The concept of "**virtual**" can be understood in another sense. Given that the traditional organization with a physical presence of bricks and mortar does not exist in its virtual connotation, cyberspace is a "construct" constituted of thin air and electrons flowing in outer space. In this latter meaning, cyberspace is supposed to fall outside the legal definition of an organization, business or legal entity. Some argue that this "ethereal" configuration does not present a centralized, unique formal entity that can be subjected to the usual constraints of formal corporations, such as taxes, regulations and other laws. It is devoid of hierarchies and common mission and/or goals.

Cyberspace is still in the process of conception and early formation. However, the series of disruptions, such as the denial-of- service (DoS) attacks that the Internet has suffered recently, as well as other situations (examples of which are described below), are very "**real**." They are not "**virtual**" at all. Disruptions of service like the ones caused by the recent I LOVE YOU virus were created by a **real** person and impacted thousands of **real** networks and web sites. To hide behind the virtual label is nothing short of naïve and misplaced.

There is little that is **virtual** (or ethereal) about the examples to be described below. Rather they point out the fact that the Internet is a new phenomenon whose reach and scope are not yet fully understood. In other words, the point is not to dwell on the differentiation between **virtual** and **real** (or physical). Rather, what is needed is to gauge the extent of the formalization and control that is needed to ensure that the organizations, --so-called virtual and otherwise -- that operate on the web, do so lawfully and cause no harm to others.

Examples of Lack of Metalevel Control

Below, we present examples of situations where the web's lack of maturity reveals a lack of formal organization and flaws existing organizations have in coping with emerging problems. These examples are only an infinitesimal sample of the type of problems that are presently arising and will be arising with more frequency in the future.

1. The Problem of Web Disruptions

The various forms of disruptions suffered by the web recently present an interesting question that differs in several respects from the problems encountered in the traditional organization. The most prominent disruption has taken the form of the "**denial-of-service**" (DoS) attacks during which several web sites were deluged by a cascade of messages, clogging the normal flow of communications between portals and their customers.

Assuredly, these attacks resemble the strikes and boycotts used to disrupt the activities of old mortar-and-brick industries. The difference is in magnitude. It will be difficult to convince the countless of businesses of this similarity after they suffered sixty-five billions dollars in damage when a so-called "innocent" student "confessed" to have used material from his dissertation to unleash the I LOVE YOU bug!

Meanwhile, new viruses are appearing daily. The Y2K Problem, while reported widely, did not cause the anticipated disruptions because a concerted effort, which proved to be very costly, was undertaken to circumvent it.

2. Privacy on the Internet

Another problem that merits attention is the invasion of privacy achieved without consumers' knowledge. This activity takes place when certain "dot-com" companies collect information about buying habits of consumers by installing a piece of software on the hard drive of unaware users. The companies not only invade privacy but, after collecting this information without permission, proceed to disseminate it to interested parties, such as employers and insurers. Internet companies involved in these activities swear that any control in the form of government regulations will stifle growth and progress. They also promise to abide to some form of self-regulation.

It is interesting to note that Yahoo, one of the most successful portals on the web, is discussing the subject of Internet privacy with the Federal Trade Commission (Haney, 2000). The company stated that it is cooperating with an inquiry by the FTC into how Internet sites gather personal information. This cooperation is significant for several reasons. It indicates that the company is in favor of having an agency of the Federal Government act as a "**controller**" to work out industry guidelines that will regulate the way personal information obtained from web visitors is mined and shared among companies, without sometimes the knowledge of its owners (New York Times, 2000e).

Are these actions, on the part of one company, part of a trend that shows how e-commerce will grow and evolve, and, eventually, submit itself to the same forms of ***control and authority*** *as other more traditional forms of business?*

As this article is to appear, the US government has announced that the Federal Trade Commission has asked Congress for authority to impose tough consumer privacy safeguards (New York Times, 2000h). It will be interesting to follow these developments to determine whether the US government will be able to increase its control and oversight over the Internet or whether private enterprise's efforts to police itself i.e. to apply self-regulation will be sufficient to curb excesses.

3. Consumer Fraud

Recently eBay, one of the most successful web sites, had to cancel a sale and unlist one of its own sellers in the On-line Auction of an abstract painting presumably for fraudulently driving bidding higher by bidding on this own item. "According to the Federal Trade Commission's Internet marketing unit, Internet auctions remain the No. 1 source of consumer complaints related to their problems on-line and they vie with sweepstakes for the top source of fraud over all" (New York Times, 2000g & 2000k).

At present, Internet commerce is rife with outright forgeries, fake art, merchandise of questionable value and authenticity, as well as rife with other irregularities that mar a new medium with unprecedented commercial promise. The "bad apples" will spoil this promise, unless consumers are offered guarantees of the authenticity of what is offered for sale.

Many promoters vouch that a self-policing mechanism can ensure commerce without fraud. We believe that more formal control is needed.

4. Management of Internet Names

In March 2000, a group of appointees met in Egypt to invent a democratic charter for the Internet's first administrative body. It would be the successor of the Internet Corporation for Assigned Names and Numbers (ICANN) that has administered the domain-name system until now. It would be responsible to "produce a plan for turning the responsibility over to a fully elected successor board"(New York, March 13, 2000b).

The meetings of the board held to date have been met with open antagonism. At a meeting held in Cambridge, MA. "members were greeted by a hostile crowd of several hundred, some of whom saw ICANN as a part of secret conspiracy to advance big-business interests at the expense of the Internet's free-wheeling traditions" Another tug-of-war concerns "those wanting the board to move quickly to add new levels of competition in the registration of domain names, and those calling for more attention to getting the process right" (New York Times, 2000b). The magnitude of the enterprise is daunting when one realizes that ICANN is trying to reconcile the interests of millions, if not billions of web users across the world.

On a related case, a commission created by Congress to make recommendations on whether or not to tax e-commerce met several times but could not arrive at a consensus (New York Times, 2000d). Later, Congress voted to postpone any taxes on the Internet for five more years.

5. Commerce of Illicit Drugs

It has been reported that illicit drugs can be easily purchased on the web. The purchaser need only use a valid credit card. The locations of the web sites offering the drugs can be situated anywhere in the world. How can this illicit trade be controlled and prosecuted, let alone be traced?

6. Survival of Copyright Laws on the Internet

A) A Case Where Control Over Copyright Laws Was Enforced

Very recently it was reported that the American Motion Picture Association sued a Canadian Internet company over a dispute involving the redistribution of television programs without permission from the program owners. The company, incorporated in Canada, was within its legal rights, but the Motion Picture Association was able to shut it down by claiming that the company and its clients (many in the US) were circumventing simple barriers to non-Canadians, such as entering an area code. (New York Times, 2000c, McGeever, 2000).

The Internet company in question did not argue the legality of the action against it. Instead, it responded by inventing a so-called "enhanced geographic screening technology" that pinpointed "where the company's users are located geographically, thus barring anyone under the jurisdiction of US copyright restrictions from viewing protected programming outside Canada." US Internet users were barred from using the Internet across international borders. Critics object violently to this solution according to which right-holders place restricted centralized control on web content, much like the centralized control of cable television. In this case, content industries were successful in securing the legal means to enforce copyright laws (New York Times, 2000c).

B) Cases Where Copyright Holders' Rights Are Being Eroded

Three camps in the tug-of-war over copyrights have emerged.

- The first camp is comprised of organizations that seek to protect intellectual property on the Internet. These organizations try to defend copyright laws by attempting to amend digital copyright laws and hold the Napster-like service providers (see below) "accountable for copyright violations while maintaining protections from liability for service providers that are innocent bystanders to digital piracy" (New York Times, 2000f).

- The second camp is represented by operators of online services, such as Napster, Freenet and Gnutella, who make it possible "to find and acquire files without reference to a central database and thus provide no single target for aggrieved copyright holders. If Napster-like service operators prevail, it will be impossible to control the traffic in any kind of digital information." Cyberspace might become "a world in which copyright laws and rights will be invalid and in which all information--be it music, video, text or software--will be freely shared." It is interesting to note that "Napster-like service operators provide files and freely bypass ISP's depriving the latter of sources of revenue." (New York Times, 2000f & 2000i).

  Napster-like services consist solely of software operators and programmers without corporate identities. Therefore, they cannot be sued or prosecuted. Indeed they represent a good example of a "virtual" community. (See above.) Under the new scheme implemented by Napster-like operators, electronic journals, such as the one presenting the present article, will not be in a position to protect any of its editors and authors from copyright infringement.

  Is this what the public wants--a world that does not protect and reward authors and artists for their creativity? The latter will have to think hard before relinquishing such important and prized right.

- Recently, a third camp emerged when a Hollywood mogul who bought an interest in a Napster-like service offered to pay authors and artists for their works in an alternative way, thus placating their claim of copyright infringement. (New York Times, 2000j)

It is too early to tell which of the three camps will prevail. One point appears certain: due to cyberspace's fluid nature, it will be increasing difficult to impose upon it traditional forms of control--a topic to which we now turn.

Control

The traditional formal organization functions with many levels of **control**, including fiduciary, legal and/or regulatory. The levels of **control** may be internal or external. As an example, an accounting system acts as an internal **control** system to keep track of assets and liabilities, flow of funds, profits and losses and so on. The Internal Revenue Service is responsible for **controlling** the timely payment of taxes and liabilities of individuals and corporations throughout the land.

Social norms **control** and curb the urge of individuals to act independently, without regard for other individuals and the rest of society.

A system of laws, written or unwritten, also serves to provide society with norms and constraints to ensure order and equity among its members.

The Control System

In the formal sense, a simple control system is made up of:

a) **a controller**,

b) **a controlled system**, and,

c) **the environment**--a system that falls outside the control system's purview.

An additional component to the simple control system can be conceived in the form of:

d) **a metacontroller**--a system that controls the controller at the metalevel i.e. a level "above" that of the controller.

The differentiation between **controller** and **metacontroller** can be understood in various ways. It can mean:

- **a difference in the physical position** from which the control is exercised. The metacontroller is "physically" above or beyond the controller, e.g. at the plant, in a remote location, as opposed to the company's headquarters.

- **a difference in the level of responsibility**, where the metacontroller holds the responsibility for the controller's results, plus has additional responsibilities of its own, due to its metalevel position.

- **a difference in the level of logic**, where by **logic** we mean a difference in the perspective or point of view from which control is exercised. An example of differences in the level of logic may be exemplified by the difference in the type and form of control exercised by a foreman over his workers or the difference between the control exercised by a sales manager over his/her sales representatives. The superior-subordinate relationship shows many of the differences that can be attributed to differences in levels of logic.

- **a difference in the way the problem** at hand is **conceptualized** and/or the kind of solution that is proposed.

That problems exhibit logic levels has been explained in greater detail elsewhere. See van Gigch (1991) & (2000).

Metalevel Control in the Traditional Organization

Metalevel control refers to a form of control exercised by the **metacontroller**. The traditional organization can be conceived as a giant control system with many control levels. As we climb the organizational hierarchy, a **lower** organizational level is controlled from above by a **higher** organization level that embodies the **metacontroller**.

Each **controller** has its own **metacontroller**. An organization, taken as a single system, is also subject to metacontrols from outside the organization. In this sense supra-organizations, governmental, regulatory or otherwise, act as metacontrollers over any and all organizations.

Metalevel Control of the Virtual Organization

The following questions need to be answered:

- **Can** cyberspace and/or the Internet be subjected to a metacontroller?

- **Should** cyberspace and/or the Internet be subjected to any control at all?

Control of Cyberspace

The architects of cyberspace, whomever they may be, argue that it should be left alone, free to evolve without the usual constraints and/or intrusions from government or other supra-organizations, such as Congress or judicial powers.

To many, the fact that cyberspace and the Internet are "virtual" entities means that they cannot or should not be treated as traditional organizations.

The distinction is rather flimsy. As described above, the differentiation between what is virtual and what is not is ambiguous. We argue that, while cyberspace and the Internet do not physically exhibit the usual attributes of traditional organizations, they are still very "real," and not "virtual" at all.

They are built by real people that have a physical presence and its products and results are visible for all to see. In particular, the denial-of-service (DoS) attacks are not "virtual". They disrupt and interrupt actual legitimate businesses and threaten valuable data centers.

Some of the arguments for or against imposing metacontrol follow:

- **Chance events**

Denial-of-service (DoS) attacks cannot hide behind the argument of irreality or virtualness. These disruptions cause very real hardships, change the course of normal business and are not mere accidents due to chance or the act of a Providence.

- **Constructive Intent**

Some circles have argued that DoS attacks are not acts of vandalism. They are said to be "constructive," in that they reveal flaws in a company's security system and that they are organized by companies who pay hackers to test their own systems' robustness. It has also been said that DoS incidents and nasty viruses are no different than labor strikes or unruly (but lawful) manifestations by a few young "computer nerds" who operate at the margin, who are doing it for fun and who, in actual fact, are providing a necessary service to the industry, by obliging companies to invent new ways to repel these kinds of attacks.

- **Creativity and Entrepreneurship**

Another argument against imposing metacontrol is that cyberspace and the Internet should be devoid of metacontrol in the name of creativity, innovation and entrepreneurship. Complete freedom is said to foster innovation and to encourage new discoveries.

- **Freedom of Speech**

Some cyberspace participants have used the argument that DoS attacks and viruses are no different from activities akin to pornography or web sites showing adult material. Hence, they are protected by the First Amendment to the Constitution and should be allowed to function in the name of freedom of expression.

Government Jurisdiction

When disruptions of commerce occur, the government and its agencies feel the need to intervene. Internet commerce is new and legislators and law enforcement officials are not certain, a) how to act to stop disruptions on the web, and b) whether certain disruptions fall under their direct jurisdiction.

On the other hand, legislators feel that the role of government should be limited to creating measures to prevent the disruptions. They feel it is up to private enterprise to take adequate measures to secure their web sites from interruptions.

The issue of jurisdiction becomes more complicated when governments, in particular in Europe, are proposing to impose taxes on Internet transactions. Taxes may not be in the realm of DoS attacks, but they point to the fact that the issues of "who is in control" and to "what extent control" can be imposed on the web, either nationally or even internationally, are becoming serious issues that involve many parties and levels of government.

President Clinton sounded the right cord when he stated, "the Federal Government ought to get in involved in protecting the privacy of financial information and medical records on the Internet." But he called "on the industry to police itself in other areas that are better left to self-regulation" (New York Times, 2000a).

The industry was in accord that cooperation between government and industry were only justified on issues pertaining to privacy and security. The example given above of Yahoo cooperating with the FTC on the subject of Internet privacy is a budding example of self-regulation and control in cyberspace. In spite of Yahoo's attempt to apply self-regulation, the FTC felt compelled to push for new legislation (New York Times, 2000h).

Argument for Complete Freedom

Can any organization, particularly cyberspace, be completely free from any constraints--be they private, governmental, or quasi-independent? The answer to this question is a resounding NO.

As soon as people or organizations interact among each other, natural conflicts of interest arise that demand management by design. Even freedom must be designed. In van Gigch (1976), it was shown that the shape that freedom takes depends on many factors endogenous and exogenous to the situation. Political, sociological, cultural aspects of the situation decide the form that freedom takes. See also van Gigch (1995).

Complete freedom in the human realm does not exist. Starting from this premise, the freedom that will be allowed on the web for Internet activities must be **designed** to foster the greatest creativity and innovation possible, while respecting the rights of individuals and enterprises to thrive in their respective endeavors.

The Imperatives of Metacontrol

An argument can be made that control of the web should be left entirely in the hand of private enterprise. Whether this intent is entirely feasible must be thoroughly explored. It is painfully clear that it will be difficult to bridge the gap across nations solely on a private basis. As soon as an international government wants to impose levies on Internet commerce, it

invites the intervention of national interests that can only be treated on a diplomatic and political basis.

Resolving the conflicts of so many jurisdictions necessitates a discussion of what **imperatives** must be satisfied. An **imperative** can be regarded as a form of obligation that must be followed or respected. In a previous discussion, van Gigch (1997) proposed the following imperatives:

1. The Operational Imperative. The goals of the Operational Imperative are **productivity** and **efficiency**. This imperative is to be followed by the sectors of the enterprise that produce the main output. At this organizational level (which stands at the lowest level of control), the emphasis is on results, regardless of suboptimization of the higher goals of the firm or of society at large.

In a first instance, each of the firms that compose the web abide by this imperative. In the atmosphere pervading the Internet, each firm tries to outdo the other with higher performance, better service and, sometimes, practices that may be subject to question from ethical or even social points of view.

2. The Economic Imperative demands that the enterprise be **profitable in order to survive**. This imperative pervades all levels of the enterprise, regardless of its level in the organization. Many of the firms in the net are sacrificing immediate profits for greater output and higher stock valuations. How long this practice can continue is questionable.

3. The Technical Imperative. The goal of this imperative is to remain **technologically viable** in an environment where some new products have less than six-months shelf life. With this kind of threshold, firms must remain at the frontier of technological knowledge or risk obsolescence

4. The Political Imperative. This imperative applies to the government and non-government organizations whose jurisdictions place them in contact with the firms that operate in cyberspace. As an example, when the DoS attacks and foreign viruses occurred the Justice Department and the FBI were brought in to investigate their source. These agencies do not operate in a vacuum. They must abide by the legal imperative (see below) and, at the same time, operate according to the wishes and whims of the political environment, i.e. the pressure of the various lobbying groups that vie for advantage and that seek recourse through politicians and the various branches of government.

5. The Legal Imperative. The goal of this imperative is straightforward. Firms in cyberspace must abide by **the laws** imposed by the country in which they operate. International standards or supra-national organizations have not as yet been contemplated or imposed. However, they might be needed when actions in a far away country affect other countries to which they are connected. Two of the examples described above illustrate the international and supra-national reach of the web.

6. The Ethical Imperative is difficult to articulate. Unethical behavior can be represented in terms of the deleterious consequences on others that result from action(s) taken by firms constituting the net, or by anybody who acts in cyberspace, be they private individuals or otherwise. As an example, DoS attacks and the unleashing of viruses that disrupt legitimate traffic and commerce have detrimental effects upon customers paying for service. They clearly become unethical, if not always illegal, activities. The same can be said about attacks on government services and the defense establishment or invasions of privacy in the private sector.

7. The Strategic Imperative. This imperative applies at the highest level of metacontrol because it demands that regard be paid to the highest mission of the web. The perspective of interest must be that of an overseer who sits above and beyond the web--if ever that is conceivable. This is highest representation of metalevel control. As presently conceived, the web does not have a metacontroller at this level. However, recent events point to the need of designing a metacontroller that can satisfy most of **the imperatives of metacontrol**, without impairing any of its most precious results.

It is definitely not required that the **strategic metacontroller** be embodied in an official governmental organization. Responsibility to enforce the strategic imperative and all others could be placed in a private or international body, preferably from the private sector. It will demand a level of cooperation from all parties and agencies acting in cyberspace that is difficult to imagine at this time.

Suggestions for Compromise

Due to the web's size and scope, it may be impossible to conceive a metalevel controller that could embrace all of cyberspace.

It is obvious that no one organization, super-agency or enterprise private or public, could fulfill all the responsibilities a metacontroller demands, abide by the imperatives, and still be able to function as a single effective controller.

On the one hand, we believe that cyberspace will have to mature, step by step, in a natural and emergent mode. On an ongoing basis, already existing or to be created organizations and institutions will bridge the gap.

On the other hand, we also believe that a non-profit and non-political organization such as an established think tank (such

as The Rand Corporation or the World Wide Web Consortium http://www.w3.org) should be given the authority and mandate to embody the metalevel controller on a purely advisory manner. This metalevel controller would provide general systemic guidance based on sound knowledge and shared community wisdom.

The US government wants to exercise active control in cases involving the protection of privacy of financial information and medical records on the Internet. Furthermore, safeguards must be built in the system so that "computers users deserve notice about what information was being collected and how it would be used, and should be able to chose whether the data would be shared with others"(New York Times, 2000a).

Surprisingly, businesses seem to be in complete accord with these proposals. They would prefer "to keep cyberspace open and free because it sparks creativity and innovation," but they also acknowledge that "cyberspace must be a community of shared responsibilities and common values." (New York Times, 2000a, Silicon Valley Tech Week, 2000).

A metacontroller can nurture and guide the cyberspace community to achieve these goals through either gentle persuasion or allowing the forces of self-regulation to act on their own.

There is no doubt that there are still aspects of cyberspace where unanticipated and ill-designed results may occur from time to time. At that time, the normal governmental institutions will have to intervene on an ad hoc and case-by-case basis.

Conclusions

We surveyed the state of cyberspace to explore areas where the need exists for some form of control over new untested activities that may, in unanticipated ways, affect the normal and free activities on the web.

The concept of metalevel control was introduced and recommended as a self-regulating and advisory mechanism that could resolve some of the conflicts, and bring about acceptable solutions and compromise, among those who want some form of formal regulation, as well as those who want unfettered and complete freedom from any kind of interference--regulatory or otherwise.

References

Haney, C. (March 31, 2000). FTC investigating Yahoo data collection. *Computerworld*. Accessed on June 4, 2000 at http://www.computerworld.com/home/print.nsf/all/000331D00E

McGeever, C. (January 21, 2000), Webcaster Under Fire. *Computerworld*. Accessed on June 4, 2000 at http://www.computerworld.com/home/print.nsf/all/000121E26A

New York Times (2000a), Clinton Calls For Stronger Measures to Protect the Privacy of Computer Users, March 4, 2000.

New York Times (2000b), What's in a Name? Arcane Internal Bickering, Internet Agency Grimly Learns, March 13, 2000.

New York Times (2000c), Digital Commerce. Control Over Content: the Case of an Internet TV Provider Illustrates the Entertainment Industry's Copyright Power, March 14, 2000.

New York Times (2000d), Advisory Panel on Internet Taxes Unlikely to Reach Consensus, March 20, 2000.

New York Times (2000e), Yahoo Says It is Discussing Internet Privacy with the F.T.C., March 31, 2000.

New York Times (2000f), The Concept of Copyright Fights for Internet Survival, May 10, 2000.

New York Times (2000g), Ebay Cancels Sale and Suspends Seller In Painting Auction, May 11, 2000.

New York Times (2000h), US Said to Seek a Law to Bolster Internet Privacy, May 20, 2000.

New York Times (2000i), Report Proposes Update of Copyright Law, May 22, 2000.

New York Times (2000j), AgentÕs Role in Entertainment Site May Signal Shift in Fight for Copyright Protection, May 22, 2000.

New York Times (2000k), In Online Auction World, Hoaxes ArenÕt Easy to See, June 2, 2000.

Oxford Concise Dictionary (1976), Clarendon Press, Oxford, 6th Ed.

Silicon Valley Tech Week (2000), Strange Bedfellows: Tech Execs Join Feds to Fight Hackers, Vol. 3(5), March 6, 2000.

van Gigch J.P., (1976), Planning for Freedom. *Management Science*, 22: 949-961.

van Gigch J.P.,(1991), *System Design Modeling and Metamodeling*, Plenum, New York and Oxford.

van Gigch J.P., (1995), Liberté, Egalité, Fraternité in the International World of Publishing: How to Get Recognition as an Author. *Human Systems Management*, Vol. 14(3): 259-262.

van Gigch J.P., (1997), The Design of an Epistemology for the Management Discipline Which resolves Dilemmas Among Ethical and Other Imperatives. *Systems Practice*, 10(4): 381-394.

van Gigch J.P., (2000), *Problem Solving and Decision Making Through Metamodeling,* Sacramento & Sebastopol, CA., Copyright 1997, 2000.