carr
centre for analysis
of risk and regulation

centre for analysis
of risk and regulation
An ESRC Research Centre

# The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia

**Jeanette Hofmann**

E·S·R·C
ECONOMIC & SOCIAL RESEARCH COUNCIL

LSE THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

DISCUSSION PAPER NO: **62**
DATE: **April 2010**

# The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia

**Jeanette Hofmann**

---

**Contents**

The work was part of the programme of the ESRC Centre for Analysis of Risk and Regulation.

Published by the Centre for Analysis of Risk and Regulation at the
London School of Economics and Political Science
Houghton Street
London WC2A 2AE
UK



ISBN 978-0-85328-404-8



Printed and bound by Kube, April 2010

# The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia

**Jeanette Hofmann**

---

**Abstract**

Cybercrime and its potential ramifications exemplify 'one of those things that nobody wants' (Popper 1963). From today's perspective it would have been easy to foresee and at least partly prevent the mischief of cybercrime. One therefore wonders what early developers and users of the Internet actually envisioned, and how malpractices such as spreading damaging viruses relate to these visions. This essay approaches this question by interpreting cybercrime as an unintended consequence of the utopian dreams that flourished during the early days of the Internet. In itself a highly innovative activity, cybercrime can be seen as an ironic counterpart to the expectations of an egalitarian cyberspace whose technical and social norms condemned discrimination against any type of applications and uses.

## Introduction

The emergence of cybercrime may some day be added to the long list of examples and anecdotes that illustrate the discussion on unintended consequences. In this hypothetical story, the Internet began as an object of libertarian dreams of social autonomy and creativity; but became subject to growing state control and surveillance, ultimately restricting individual privacy and social liberty to a much higher degree than any other democratic communication media. The spread of cybercrime, or so this story would go, played an instrumental role in this transformation. With spam getting out of control and computer viruses becoming ever more dangerous, users welcomed or even asked for state action that would restrict individual freedom on the Internet.

The appearance of unintended consequences has been associated with the emergence of modernity. Hirschman (1982: 1463) beautifully made this connection by portraying the notion of 'unforeseen consequences or 'perverse effects'' as a counterpart to the 'idea of a perfectible social order'. Very generally speaking, modernity represents a way in which human beings conceive of and organize their life (Wagner 2008). The idea of a social order that is not longer (God-) given but open to self-determination is at the heart of most definitions of modernity. The concept of unintended consequences shares with that of modernity the assumption of deliberate, 'purposive' action in a Mertonian sense: unintended outcomes are only interesting in the context of deliberate social action.

Social theorists discovered the issue of unintended consequences against the background of a modern understanding of society which emphasizes virtues such as individual and collective responsibility and the capacity of self-determination. Following Hirschman (1982), unintended consequences thus form an ironic twin to the expectation that social development is amenable to planning and control, predictable in other words. Without the belief in a manageable future, there is no conceptual space in which outcomes of social action can be construed as 'unforeseen'.

Yet, the desire for governing society's future is just one modern origin of unintended consequences. De-traditionalization, growing social equality and weakening social ties have been identified as sources of unforeseen outcomes. Vernon (1979: 61) attributes this insight to Tocqueville who, comparing aristocratic and democratic societies, 'first suggested a strong linkage between social equality and the production of unintended consequences'.[1] As a result, social positions have become more diverse and the course of social developments less predictable. A similar point could be made about the Internet in comparison to the centrally managed telephone networks. In a certain way, the Internet broke the chain between engineers, operators and customers of communication networks. The original design didn't privilege any roles but created a new form of equality among producers and consumers of applications or content.

[1] Tocqueville (II, 2, 2, p. 99 ) observed that 'in aristocratic communities, all the citizens occupy fixed positions (…) aristocracy had made a chain of all members of the community, from the peasant to the king; democracy breaks that chain and severs every link to it.'

As a result of this equality, the development of the Internet has proven to be more dynamic and less predictable than that of telephone networks.

There are many variations of unintended consequences and, as Merton (1963) already pointed out, not all of them are undesirable. Adam Smith's account of the emerging market order is a popular example of the unintended cumulative effects of individual actions. Yet, if one subsumes social institutions such as markets under this category, unintended consequences become so ubiquitous that it is actually *intended* outcomes which call for explanations. As Popper (1963: 166) puts it, 'we hardly ever produce in social life precisely the effect we wish to produce (…) there are always certain unwanted consequences of our actions; and usually these unwanted consequences cannot be eliminated'. In other words, discrepancies between the intentions and the results of social action can always be expected, and no advances in societal knowledge will reduce the magnitude of unexpected outcomes.

Even if unforeseen outcomes of social action can neither be predicted nor prevented, it still proves to be useful to trace their origins. Reconstructing unexpected consequences is insightful in the sense that they promise to reveal the blind spots of original expectations. For, as Vernon (1979: 69) notes, 'what anyone can will depends upon what they currently know, and what they (or others) know later will change the meaning of what they have done'. Unintended consequences thus may serve as forensic tools for exploring worldviews once taken for granted in a given context and they may enlighten our understanding of their shortcomings. While both desired and undesired forms of unintended consequences have been characterized as an important cause of social change (Boudon 1982; Giddens 1987), it is chiefly the latter which are deemed relevant under the conditions of an emblematic 'risk society' which emphasizes the damages and dangers modern societies have been inflicting on themselves (Beck 2009).

Cybercrime and its potential ramifications exemplify 'one of those things that nobody wants' (Popper 1963). What is more, from today's perspective it seems it would have been so easy to foresee and at least partly prevent this kind of mischief.[2] One therefore wonders as to what early developers and users of the Internet actually did envision, and how malpractices such as spreading damaging viruses relate to these visions. This essay approaches this question by linking the occurrence of cybercrime to the early days of the Internet's development. It explores the dominant orientations of two groups, the engineering community which developed the Internet and the first generation of academic users, both of which largely shaped the public understanding of the socio-technical constitution of the Internet around the time when spam and viruses became a common issue in the late 1990s.

Public debates on rules for the Internet set off in a context of antagonistic visions. The new generation of digital network developers and users dismissed conventional top-down ways of regulating communication networks; they perceived the Internet as a radically different, essentially ungovernable new social space, and they argued in favor of a public hands-off approach to prevent governments from destroying it. For a short period of time, the Internet represented a landmark in the struggle for the

[2] For example, if the technical standard for email included a provision for authenticating the sender, it would have been more difficult to spread spam and viruses.

good social order, and government intervention seemed to represent the only real danger to this struggle.

Santos (2002: 2) has described the tensions revolving around the 'perfectible social order' (Hirschman) as the 'discrepancy between experiences and expectations'. While expectations of social change and progress have generally good connotations in modern societies, the distance between experiences and expectations remain contested. In Santos' understanding, 'modern regulation' aims to control the pace of change through a set of 'norms, institutions, and practices that guarantee the stability of expectations' (op. cit.) while a set of emancipatory 'oppositional aspirations and practices' aims at increasing the discrepancy between experiences and expectations and may thereby destabilize the institutional order in a given area. Santos' emphasis on expectations as an engine of social change helps relating to the visions driving the early development of the Internet to their blind spots.

The architects and early users of the Internet envisioned cyberspace as a new, libertarian post-national social order and thereby expand the discrepancy to experiences grounding in existing, predominantly government regulated communication networks. Their 'oppositional aspirations' delegitimized traditional models of running and regulating communication networks but dismissed any comprehensive need for regulation beyond that of 'code'. Against the background of this utopian vision, cybercrime emerged as a different, entirely unforeseen and unwanted interpretation of the call for unrestricted freedom of innovation. Cybercrime, in itself a highly innovative activity, can be seen as an ironic counterpart to the expectations of an egalitarian cyberspace whose technical and social norms condemned discriminating against any applications. Hence, spam and viruses embody the 'perverse effect' which illuminates the flipside of the expectations that accompanied and to some extent shaped the early development of the Internet.

The next section of this paper focuses on the orientations of the engineering community which developed the Internet in the 1970s and 1980s and on their 'revolutionary' design philosophy which inspired its architecture. The section thereafter centers on the first generation of academic users who in the 1990s, as a response to pending government regulation, re-interpreted the network architecture along political claims of self-governance. The last empirical section describes the development of cybercrime as an unforeseen, yet increasingly dangerous way of making use of the freedom the Internet offers.

## Conflicting visions of communication networks: autonomy versus public service

On November 22, 1977, a computer network was set up that linked a van driving on a California freeway to the University College London and the University of Southern California. This experiment intended to demonstrate that 'internetworking', in other words the bridging of heterogeneous local data networks, is indeed possible. In retrospect, this experiment came to be known as the beginning of the Internet as an operational system (Abbate 1999: 132).

The emerging landscape of data communication in the 1970s lacked general standards for data transmission that would facilitate communication across different

computer networks. Among the various attempts to develop computer network architectures, two standard developing initiatives stood out that aimed at open, vendor-independent solutions that would enable universal data communication: the 'Internet protocol suite'[3] which originated in the US defense research environment, and 'X.25', a set of technical recommendations jointly developed by intergovernmental standardization bodies for telecommunication networks[4] (Salus 1995: 124). Both engineering communities pursued the same goal, a single network architecture that would enable digital communication across autonomous networks, organizations and countries. Yet, for those interested in the development of network standards, 'X.25 and TCP/IP became symbols of the carriers' and the Internet community's opposing approaches to networking' (Abbate 1999: 155). At first glance, these opposing approaches seemed to be of a mere technical nature. However, the technical controversy between the two engineering communities also reflected different ways of organizing and regulating infrastructures.

While the carriers' engineering community thought of data communication in terms of centrally controlled national networks, the opposing engineering community intended to delegate control to local networks and its users. The telephone companies envisioned data exchange as a public service that would basically follow the same organizational model as telephone networks. From the perspective of the large monopoly-based telephone carriers, the heterogeneous landscape of network architectures of the 1970s appeared as a mere interim stage soon to be replaced by a single public network (Hofmann 2007). Like voice transmission, data communication would be organized and controlled by national carriers which would connect their networks to those of other national carriers. As Abbate (1999: 156) notes to the developers of X.25, 'it seemed self-evident that the best service to customers would result from a system where a few large telecommunications providers controlled network operations'. From the perspective of the telephone carriers, new technologies and services would be adjusted to the present operating models. In Santos's terms, the discrepancy between past experiences and future expectations was small.

The engineers who developed the TCP/IP network architecture started from a different set of assumptions. While they also identified the incompatibility of existing network architectures as a problem, they did not expect the diversity of networks to disappear - not least because the lacked the authority to impose a common standard on network operators. Instead, the research community aimed for a network architecture that would acknowledge and tolerate heterogeneity. As Hafner and Lyon (1996: 225) put it, the challenge was to 'devise protocols that would cope with 'autonomous networks operating under their own rules, while still establishing standards that would allow hosts on the different networks to talk to each other'. The experiment carried out in 1977 that managed to connect a radio network on a moving van, a satellite network and the ARPANET, the actual forerunner of the Internet, meant to demonstrate just that: the possibility of connecting autonomous network architectures through a simple type of meta-network, an *Inter*net. Hence, the two competing concepts of data network design embodied opposing ideals of social organization which are in tension with each other: on the one hand the bureaucratic

[3] The Internet protocol suite consists of the Transmission Control Protocol (TCP) and the Internet Protocol (IP) and is usually referred to as TCP/IP; see http://en.wikipedia.org/wiki/TCP/IP.

[4] The International Telecommunication Union (ITU) and the International Organization for Standardization (ISO).

model which emphasizes collective security, stability and regularity, and on the other hand the liberal model which emphasizes local or individual autonomy, openness and equality. These two architectural answers to the common problem of creating a universal data network echo the political tensions between regulatory institutions and practices aiming to control the scope of social change and emancipatory movements seeking to expand it (Santos 2001: 253).

The different assumptions about the future organization of data communications – in simplified terms, centrally operated homogeneous national networks versus autonomously operated heterogeneous networks oblivious to national borders – had crucial implications for both the technical design of network architectures and the political control over their use. The paradigmatic 'tussle' (Clark et al. 2002) that broke out between the telephone community and the nascent Internet community revolved around these implications. One of them concerned the division of labour between the network and its endpoints, the devices or applications attached to the network (Blumenthal & Clark 2001: 80). While telephone networks traditionally achieved reliable performance by placing control functions in the network, the developers of the Internet chose to depart from this principle of central control and opted for the 'stupid network' approach (Isenberg 1997). The latter approach minimizes the functionality in the network in favor of maximum responsibility of the network's end points. Because the stupid network delegates the control over data transmission to the applications, the network itself neither controls if the data reach their destination, nor does it know which kind of data it transmits; it is 'oblivious' to the content it transports (Aboba & Davies 2007).[5]

The Internet engineering community offered several reasons for the stupid network approach, which later became known as the 'end-to-end argument', a now famous architectural principle that is still often quoted (Saltzer, Reed & Clark 1984; Blumenthal & Clark 2001; Kempf & Austein 2004; Russell 2006).[6] The advantages of placing the control at the endpoints of the network were that the network itself could be more easily modified and, more importantly, new applications could be added without changing the network. As the 'end-to-end' aficionados reminded the community:

> building complex function into a network implicitly optimizes the network for one set of uses while substantially increasing the cost of a set of potentially valuable uses that may be unknown or unpredictable at design time. A case in point: had the original Internet design been optimized for telephony-style virtual circuits (…), it would never have enabled the experimentation that led to protocols that could support the World-Wide Web (…) (Reed, Saltzer & Clark 1998).

[5] The 'guaranteed service approach' of the centralized telephone network was replaced by a 'best effort delivery' model which shifts the responsibility for error control to the endpoints. Today, the difference between these two approaches has somewhat decreased since Internet service providers have now technical means to inspect the data they carry and discriminate against specific applications.

[6] Given the military research environment, the original motivation for shifting control out of the actual network had to do with considerations of reliability and resilience: a network was assumed to survive hostile attacks more easily if the endpoints could re-establish communication after network failures (Clark 1988).

Thanks to the stupid network architecture, new services and applications could be introduced without changing the network's core and, hence, without asking anybody's permission (Kempf & Austein 2004). Thus, the key architectural principles of the Internet enabled a global communication space more or less free of barriers to access or use that allowed any user to implement any type of application. In light of the tight operational controls that are typical for public infrastructures, this sacrifice of central control functions seemed like an unprecedented, if not revolutionary approach that threw out many decades of operational experience. The stupid network approach reflected both military considerations of resilience against the backdrop of the Cold War and the academic background of the engineers who developed the architecture (Clark 1988; Abate 1999). The academic community consisted of computer scientists with a focus on building communication networks and 'little interest in exercising control over the network or its users' behavior (…) Keeping options open for growth and future development was seen as sensible, and abuse of the network was of little worry because the people using it were the very people designing it' (Zittrain 2006: 1989).

From the point of view of the telephone carriers and the major vendors, the TCP/IP architecture looked like an 'academic toy', a 'research curiosity' (Clark et al. 2002; Hafner & Lyon 1996: 247-8.; Malamud 1992) soon to be replaced by proper public networks with a guaranteed high quality service delivered by public carriers. The 'David versus Goliath' constellation between the small Internet engineering community and the powerful telecommunication carriers notwithstanding, the 'stupid network' approach became subject to a heated technical argument and power struggle. While this controversy focused on technical issues of performance, reliability and cost, the contested design options had obvious social implications which were later framed in more political terms.

The obvious example is the end-to-end principle, a true 'boundary object' (Star & Griesemer 1989) with technical (reliability, resilience) as well as political (freedom of innovation) connotations. Another example refers to the differing visions of the future networking landscape. The libertarian model of a network connecting autonomous local networks emerged in contrast to the paternalistic model of data communication as a public service provided – and controlled – by a state-run carrier. While the latter vision centralized authority at the expense of freedom of use, the first maximized autonomy at the expense of network security. The Internet engineers alluded to these different design philosophies in the form of numerous jokes: 'Many web generations ago, the ARPA knights started a revolution against the telco circuit-switching empire and determined to destroy the death stars and their twisted pairs' (Metcalf 1997[7]). Obviously, both models of data networking have specific advantages and disadvantages some of which became apparent only when the Internet advanced as a mass medium.

The first generation of academic users framed the network's technical design as a cultural counter project to hegemonic forms of political organization and authority. Described in Santos' (2001: 253) terms, they articulated expectations of self-determination against the common experience of state-controlled communication

[7] Quoted from http://cyber.law.harvard.edu/archived_content/people/reagle/inet-quotations-19990709.html.

services. Yet, neither the engineering community nor the early generations of users were aware of the risks inherent to the open architecture model. As Clark et al. (2005: 93) recall, 'the Internet was designed in simpler times, when the user community was smaller. It was reasonable to trust most of the users, and it was possible to track down and deal with misbehavior'.

## The utopian moment: framing the Internet architecture in modernity's terms

Until the privatization of its backbones, the networks' main data routes, in the mid 1990s, the Internet constituted a public research network whose access was more or less restricted to academic institutions (Shah & Kesan). Universities and research institutions were the first organizations providing access to the Internet in the early 1990s which explains why 'as a form of life, its birth was tied to university life' (Lessig 2006: 33). Not surprisingly, the early academic users experienced the Internet as a homogeneous social space populated by like-minded people. As a student noted, 'it feels like walking into a room full of friends' (Harasim 1994: 15). In retrospect, authors such as Lessig (2006) and Zittrain (2006) have stressed the extent to which the academic environment of the 1990s shaped the optimistic expectations of the Internet's future. To the first generation of academic users, the Internet appeared as a radically different social space that challenged or even broke with the familiar structures and principles of the modern society that had enabled the Internet to begin with. In 'Coming of Cyberspacetime and the End of the Polity' Nguyen and Alexander (1996: 107) asserted the 'breakdown of modernity' underpinned by examples of the transformation or erosion of conventional forms of power. The distributed character, in other words, the lack of a central agency in charge of the communication services and data flows was a popular case in point for the observed transformation of power. This lack of 'change control' has been regarded as one of the unique features of the Internet: '…the result is a grid that is nearly completely open to the creation and rapid distribution of (…) innovations' (Zittrain 2006: 1980).

Due to the stupid network approach, users – not network operators – would determine the preferred choice of applications. More by accident than design, the Internet became the first 'many-to-many mass medium' (Walker 2003): 'Individuals, all over the globe, were empowered to create and exchange information of all kinds, spontaneously form virtual communities, and do so in a totally decentralized manner, free of any kind of restrictions' (Walker 2003). A particularly enthusiastic observer expressed this new experience of liberty and communality by characterizing the Internet as 'the best and most original American contribution to the world since jazz. Like really, really good jazz, the Internet is individualistic, inventive, thoughtful, rebellious, stunning, and even humorous. Like jazz, it appeals to the anarchist in us all' (Valauskas 1996). The allusion to anarchism was not just coincidence. To Valauskas and others, the lack of governmental control made the Internet 'the closest approximation of perfect anarchy', that is 'a utopian society of individuals, individuals who enjoy complete and utter freedom of government' (ibid). Hence, by minimizing regulation in the form of institutions and norms, the Internet helped to increase the distance between social (offline) experiences and (online) expectations. The net turned into a landmark of emancipatory visions.

Until the mid 1990s, the Internet was more or less left to its own devices (Handley 2006). As Goldsmith and Wu observe (2006: 32), 'from the 1970s through much of the 1990s, the U.S. government was passive, happy to let the engineers do their thing' and act as an 'absentee custodian' (see also McConnell 1997: 72). The political zeitgeist in the US at the time suggested deregulation whereas from the perspective of European governments, the Internet appeared as an interim phenomenon rather sooner than later to be replaced by a proper data network architecture, which therefore didn't merit much political attention (Werle 2002: 146; Christou & Simpson 2007: 153).[8] The question of state regulation appeared on the political agenda only after 1995 when it became obvious that the Internet was rapidly turning into a mass medium. An early attempt to regulate the Internet presented the US Government's 1996 'Communications Decency Act', which was later ruled as unconstitutional for violating the First Amendment.[9] The Communications Decency Act constituted a governmental response to rising public fears of the Internet as an ungovernable space that encourages pornography and puts minors at risk. The statutory act intended to regulate indecency by subjecting the Internet to rules similar to those that govern the broadcasting media (Lemley 2002). Internet cybercrime was just about to move into the public eye at that time.

However, the mere possibility of bringing the Internet under public control and submitting it to the rules of the 'real world' evoked a passionate academic debate on the feasibility and implications of state control over the Internet. The specific 'distributed' attributes of the network architecture featured prominently in this debate. As many contributors confidently argued, the Internet would prove immune to attempts of hierarchical control. As Walker (2003) put it, 'the very design of the Internet seemed technologically proof against attempts to put the genie back in the bottle'. Among academia, it seemed commonplace that 'the Internet could not be regulated' (Lessig 2006: 27) and, hence, the grassroots revolution not be stopped. The Internet's characteristic resilience against technical failure or military aggression would also protect it from any form of political control. John Gilmore's (1993) maxim that 'the Net interprets censorship as damage and routes around it' became a popular dictum that reflected both the military heritage of the Internet architecture and confidence in its ungovernability.

In a famous article on law in cyberspace, Post and Johnson (1996: 3; 6) argued that the decentralized, cross-border architecture of the Internet prevented it from coming under public control because national laws can only be effective within a system of territorial states and geographical borders:

> Global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility—and legitimacy—of applying laws based on geographic boundaries (…) The Net thus radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules.

[8] According to Genschel (1995: 138), the EU Commission excluded TCP/IP products from public procurement until the early 1990s. Yet, governments kept funding the networks that connected universities, and the US government also funded administrative functions such as the 'Internet Assigned Numbers Authority'. The funding didn't imply any form of regulation.

[9] For details see http://en.wikipedia.org/wiki/Telecommunications_Act_of_1996.

This view that state sovereignty could not be effectively exercised on the Internet came close to a truism throughout the 1990s (for a critical review, see Drezner 2004: 479-81). The Internet would not only route around regulatory impediments, by virtue of its global architecture it would also delegitimize attempts to enforce regulation on cyberspace. Laws are valid only within clearly defined geopolitical boundaries, Johnson and Post argued, and the Internet basically negates such boundaries. Public authority in the form of territorial control would therefore be replaced by the 'law of the Internet', an aggregate of (individual) choices made by engineers and individual users (Post 1998: 539). Again, genuine modern goals such as self-determination and emancipation, expressed in strictly libertarian disguise, were mobilized in the face of a pending intrusion by public authorities. Governments were associated with the experience of stifling regulation while the Internet epitomized the expectation of unrestricted freedom.

In the context of the debate on Internet regulation, academic observers such as Johnson, Post and Lessig and political advocates, among them Kapor and Weitzner (1993), interpreted the TCP/IP architecture as the basis of a new form of social organization constituted partly by technical, partly by social norms. Technical and social rules were thought to reflect each other. Well-known expressions of this idea are Reidenberg's (1998) 'Lex informatica' and Larry Lessig's (2006) 'Code is law', the latter of which suggests that technical code, namely the TCP/IP architecture, is a regulator of cyberspace and second that its regulatory effects are intentional:

> The Internet is built on a simple suite of protocols—the basic TCP/IP suite…. Like a daydreaming postal worker, the network simply moves the data and leaves interpretation of the data to the applications at either end. This minimalism in design is intentional. It reflects both a political decision about disabling control and a technological decision about the optimal network design (Lessig 1999: 32).

The first generation of academic users thus translated specific technical features of the Internet, particularly the end-to-end principle, into a political language of regulation and held that, within this architectural framework, users are capable of setting their own rules. Some of these rules were thought to already exist; and so did its 'governors', humans and code who 'impose values on the space' (Lessig 1998). In more general terms, the argument against regulation by governments was that laws are not the only means of rulemaking and that, on the Internet, technical standards fulfill a similar role. As Reidenberg (1998) saw it, technical norms form a 'lex informatica' much like the 'lex mercatoria', which evolved in the Middle Ages in response to the practice of cross-border trading. The Internet architecture was believed to protect cyberspace against governmental intervention and, at the same time, provide its community with values and (minimal) rules to govern their interaction. In short: 'architecture is politics!' (Mitchell Kapor). The political interpretation of the network architecture as a set of constitutional rules for cyberspace formed a central part of the utopia that characterized the early academic writing about the Internet. Indeed, the inclusion of the network design in the digital body politic was considered a hallmark of the early Internet culture. The net's dispersed forms of control and power were regarded as a unique opportunity for creating the good social order that would emancipate itself from the physical world.

Old dreams of social emancipation, equality and autonomy seemed to be getting within reach.

Another, perhaps more vague, element of this new social order consisted of the 'we', an imaginary global community of Internet users or 'netizens' who identified with the virtual world and claimed to live a social life significantly different from that of the *real* world society. As Lessig (1995: 1746) put it, 'People meet, and talk, and live in cyberspace in ways not possible in real space. They build and define themselves in cyberspace in ways not possible in real space'. The iconic expression of this claim of 'otherness' and 'elsewhereness' is John Perry Barlow's often-cited 'Declaration of the Independence of Cyberspace'. Barlow modeled his manifesto after the American Constitution and wrote it in response to the adoption of the US government's 1996 Communication Decency Act, which intended to regulate content on the Internet. It opens with a direct attack of modern society – on behalf of 'liberty itself':

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear (Barlow 1996).

Even if Barlow's declaration of independence may sound somewhat histrionic from today's perspective, its rhetoric dichotomies between the past 'giants of flesh and steel' and the new space of the 'Mind', between the tyranny of democratically legitimate laws and the great promises of liberty, did indeed echo the sentiments of many Internet users in the 1990s. It cited the 'American revolutionary political tradition', and it set 'a decidedly righteous, anti-colonialist, Boston Tea Party tone' to the text (Morrison 2009: 58). Many Internet users in the mid 1990s shared the feeling of superiority that Barlow's declaration conveyed. As Geist (2003: 325) recalls, it 'served as a clarion call for a new regulatory approach to the Internet and gave a voice to thousands of 'netizens''. The early generation of Internet users did not only hold strong reservations about the hierarchical structures of the real world's society but also believed that, thanks to the Internet, radically different ways of social self-organization were possible.

The anti-government attitude, bolstered with references to the (temporarily fashionable) swan songs of the nation state, formed another important element of the 1990's cyberspace culture. Academic observers portrayed democratic forms of political organization as territorial institutions of the pre-digital past and assumed the 'death of the nation state' and the end of 'geographical tyranny' to be in close reach. They associated governmental regulation with central control and inflexibility, bureaucratic tardiness and outdated business models (Spar 1999), an attitude echoed

by some parts of the US government.[10] Governments epitomized the antithesis of the unbridled, dynamic Internet. As Lessig (1998) summarized the zeitgeist of cyberspace: 'so, while we believe that there is a role for collective judgments, we are repulsed by the idea of placing the design of something as important as the internet into the hands of governments'. In other words, governmental regulation of the Internet was regarded as a bad thing while ungovernability and powerlessness were regarded as good things. Ungovernability would ensure that, to use the terminology of Santos (2001: 253), the project of social emancipation could not be cannibalized by the project of social regulation.

The 'epistemic community of elite citizens' (Morrison 2009: 55) was intent on building a virtual world for people like themselves, people who believed in the virtue of principles such as self-determination, freedom, equality and openness. One of the few concrete models for this utopia of self-governance was the Internet Engineering Task Force (IETF) and its standard setting process. The IETF has been frequently cited as proof that the Internet enabled new, and superior, forms of collaboration and decision-making. In contrast to its intergovernmental equivalent, the International Telecommunication Union (ITU), the IETF is an informal association without legal status, organizational boundaries or formal membership rules. Standards were, and still are, developed by open working groups, which keep public archives of their discussions. There is neither representation nor voting in the IETF but institutions such as 'rough consensus', among working group members, and 'running code', i.e. working implementations of proposed standards. The explicit rejection of governmental standard setting procedures became a defining slogan of the IETF that has adorned several t-shirts: 'We reject: kings, presidents and voting. We believe in: rough consensus and running code' (David Clark). Self-regulatory structures committed to openness, inclusiveness and bottom up decision-making such as those developed by the IETF were believed to work also in other social contexts and therefore provide an ideal for the future management of the Internet.

On the whole, the utopian project of self-determination in cyberspace in the 1990s oscillated between overconfidence and fear of external interference (Drezner 2004). The latter referred to one specific threat, the regulatory power of governments. Governmental regulation constituted the single danger unanimously recognized by the epistemic community in cyberspace. Because unlimited freedom was deemed an absolute positive thing, nearly any form of hierarchical restriction seemed condemnable. This Manichaean worldview, which contrasted emancipation with regulation, freedom with tyranny, and 'Internet natives' with 'Internet immigrants' (Barlow 1996), didn't allow for any concerns about dangers or evils emanating from cyberspace or the community of netizens itself. The belief in self-regulation implied a great trust in the composition of this 'self', the individual users on the Internet.

The online community, the imaginary 'we', was thought to consist of enlightened human beings who could be trusted to make good use of the freedom the Internet offered. Users trusted each other because until the network was privatized, they

[10] As the US government (1998) stated in the White Paper that preceded the founding of ICANN: 'Certain management functions require coordination. In these cases, responsible, private-sector action is preferable to government control. A private coordinating process is likely to be more flexible than government and to move rapidly enough to meet the changing needs of the Internet and of Internet users.'

shared a similar university-based cultural background. The Internet community's concept of the enemy of cyberspace was remarkably narrow; it focused on governments and their intention to apply 'real space regulations' to the Internet. Such intentions were countered with freedom of expression arguments (Wall 2005). The possibility of other forms of abusing the freedom on the Internet formed a blind spot. The defense of unconditioned freedom on the Internet didn't take into account the explosive growth and diversification of users that accompanied the stunning success of the open network architecture. Furthermore, it didn't prepare for the 'people with a wider range of motivations for using the Internet', as Blumenthal & Clark (2001: 72) elegantly paraphrased the emerging group of new 'immigrants' who violated the unwritten ethical code on the Internet.

## Disenchantment of the Internet: the emergence of cybercrime

Throughout the Internet's first decade as a research network, social interaction in cyberspace was regulated by conventions known under the term 'netiquette'.[11] Netiquette prescribed acceptable social behavior in the various public fora on digital networks. Notwithstanding the libertarian culture in cyberspace, the netiquette rules were quite explicit about what constituted an abuse of the common communication resources:

> Never send chain letters via electronic mail. Chain letters are forbidden on the Internet.
> Your network privileges will be revoked (…)
> - Don't send large amounts of unsolicited information to people. (…)
> Unsolicited advertising that is completely off-topic will most certainly guarantee that you get a lot of hate mail (Hambridge 1995).

The first striking violation of netiquette in the form of mass postings[12] on the Internet occurred in 1994. The 'green card spam', which offered (superfluous, as many observers pointed out) support for enrolling in the American 'Green card lottery', became notorious as a turning point in the history of the Internet. Canter and Siegel, the authors of the advertisement, were retrospectively described as 'innovators with a penchant for technology' (Everett-Church 1999); retrospectively because spam wasn't recognized as an unintended but plausible consequence of the call for unrestricted innovation. Instead, the freedom to innovate was associated only with desirable novelties.

The first commercial spammers on the Internet had commissioned a 'script', a little program developed specifically for mass-posting, which sent their advertisement to roughly 6000 USENET discussion groups. As a response to what was deemed an outrageous violation of netiquette, angry users intent on making a public example flooded the spammers' email account and phone lines. While Canter and Siegel lost their email account as a result of their spamming activity, they apparently won more

[11] Most forms of netiquette emerged on the USENET, originally a communication network independent of the Internet, but there were also collections of rules designed for Internet applications.
[12] For details about the history of spam, see Templeton. For a timeline, see [http://keithlynch.net/spamline.html].

than 1000 clients and thus made a big profit (Specter 2007). As the article on Wikipedia about Canter and Siegel notes, the green card spam:

> Coming not long after the National Science Foundation lifted its unofficial ban on commercial speech on the Internet, marks the end of the Net's early period, when the original Netiquette could still be enforced through social pressure.[13]

Spam was perceived as 'the first really bad thing that people started doing on the internet, in terms of letting the small town rules break down and start abusing people' (Templeton cited in Kleiner 2008). Utopian dreams of unrestricted freedom flourished against the background of a 'small town' or a 'room full of friends' (Harasim) atmosphere on the pre-commercial Internet. As a consequence of spam, the efficacy of 'small town rules' could not longer be taken for granted. Yet, due to its strong reservations about regulation, the early Internet community had not much to offer to enforce netiquette on the Internet beyond the flooding of mailboxes and similar techniques of vigilante justice.

Over the following years, 'malware' (malicious software; for an overview see OECD 2009) became a regular occurrence on the Internet and the Netiquettes rules fell quickly into oblivion. In 1998, four years after the 'green card' advertisement, the new meaning of the term spam made it into the Oxford dictionary.[14] The growing spread of spam, viruses and other misdoings on the Internet made it obvious that a new type of users had discovered the amazing openness, innovativeness, and ungovernability of the Internet and set out to explore new ways of making use of it.

The first decade of cybercrime was characterized by a steady and rapid increase of, often fraudulent, spam, viruses and other types of malware. Yet, the early cybercrime profession itself appeared to be rather scattered and heterogeneous, a mixture of professionals and amateurs, most of them working on their own. Viruses and self-replicating worms, for example, used to be simple programs that emerged as part of a more or less reputation driven sport. The authors tended to be 'kiddies writing scripts in their bedrooms' (Specter 2007) who wanted 'to become famous and gain the admiration of their peers (…) demonstrated most famously by the 'ILOVEYOU' worm of May 2000, created by a disaffected student in the Philippines' (House of Lords 2007:13). 'Sasser', a rather harmless worm which just stalled the networks of a news agency, an airline, a coastguard, an investment bank and the European Commission, was released in spring 2004 – on the 18th birthday of its author. The fact that viruses could be developed so easily and at the same time cause so much damage is indicative of the vulnerability of the Internet as well as the commercial software installed on users' computers. The design of the Internet architecture and the transmission and communication services reflected the risk of network failure, e.g. caused by military attacks, but it wasn't prepared for malicious behavior of its own users. Abuse of network resources by users were outside the imagination of its developers.

[13] http://en.wikipedia.org/wiki/Canter_&_Siegel

[14] The Oxford dictionary's first definition for 'spam' was: 'trademark, a tinned meat product made mainly from ham.' The second definition was: 'irrelevant or inappropriate messages sent on the Internet to a large number of newsgroups or users.' (http://news.cnet.com/2100-1023-214535.html).

Sending out messages from their 'throw-away' dial-up accounts (Steward 2003), early spammers imitated traditional mass-market mail practices. Sanford Wallace, one of the first 'spam kings', had started his career with junk fax marketing. Spammers like Wallace benefited from the trans-border structure of the Internet that allowed a global distribution of millions of emails at very low cost and also, thanks to the unclear jurisdiction over cyberspace, at almost no risk of prosecution. As Specter (2007) notes about early spamming practices, 'it wasn't hard to find out who the e-mail came from, and almost nobody lied about his identity'. Email addresses, automatically collected by 'bots' (short for robots) crawling through the Internet, could be bought on CD together with simple spamming tool kits, the trade of which evolved into a lucrative side business of spamming: '2 Million Email Addresses for $19.95' (Anderson 2004).

As a cheap alternative to the dial-up account, spammers discovered so-called 'open mail relays' to send out spam. 'Open relay' refers to the original default configuration of mail servers, the program responsible for sending emails, which allowed anyone, including unknown users, to send their email through them.[15] The increasing abuse of open mail relays for spamming transformed the initially convenient feature into a vulnerability of the Internet. As a result, open relays became controversial[16] and eventually blacklisted[17] as notorious sources of spam and other forms of malware. Sadly though, the closing down of open relays contributed to the Internet's receding openness while the amount of spam remained largely unaffected and kept increasing. Their originators quickly figured out new ways of spreading spam (see also van Eeten 2008: 10), for example by using free email accounts. In 2008, spammers managed to break the security system that prevented the automatic registration of free email accounts. CAPTCHA (Completely Automated Public Turing test to Tell Computers and Human Apart) usually consists of a number of characters that a user needs to decipher and copy in order to prove that a human and not a 'bot' is trying to set up a new account. Automatically created email accounts or websites have been used to a growing extent for hosting and circulating spam (MessageLabs 2008).

A satire about a fictitious 'spammer-in-training', an amateur who quickly succeeds in creating his own 'spam empire', illustrates the dynamic arms race that has emerged between spammers and anti-spam groups or companies (Anderson 2004). Stan, the spamming trainee, escapes anti-spam legislation by operating his business via 'bulletproof hosting services'[18] in China. A similar amount of spam originates from the United States though, one of the many countries with anti-spam legislation.[19] It is well known that legal efforts to combat cybercrime haven't had noticeable effects on the amount of spam on the Internet. The actual arms race takes place between the cybercrime industry and the security industry, both of which have grown into interrelated markets: The higher the level of cybercrime (measured by the security

[15] For details see http://en.wikipedia.org/wiki/Open_mail_relay

[16] Controversial because some cyber-libertarians regarded open mail relay is a matter of free speech and refused to close them down. Ironically, John Gilmore's open mail relay was used in 2006 to spread a virus.

[17] Blacklisting refers to the practice of filtering incoming traffic according to blacklists (DNSBL), see van Eeeten et al. (2008: 28).

[18] Bulletproof hosting companies help their customers evade content regulation, see http://en.wikipedia.org/wiki/Bulletproof_hosting.

[19] Daily updates about the top 10 worst 'spam origin countries' can be found on the spamhouse website www.spamhaus.org/statistics/countries.lasso.

industry, see Anderson et al. 2008), the larger the market for security services (van Eeten et al. 2008: 18). As some observers note, the arms race does not only transform the Internet, it also drives the inventiveness of the cybercrime industry. Anti-spam techniques have been compared to pesticides 'that do nothing more than create a new, resistant strain of bugs'.[20] Each generation of spam or virus detection and blocking techniques is counteracted by new methods of evading those filters. The more spam gets successfully blocked, the greater the volume of spam that has to be sent out to keep up the profit. 'If you used to have to send fifty thousand pieces of spam to get a response, now you have to send a million' (Sorrow, quoted in Specter 2007). Like every year before, '2008 set a new record for overall spam volume' and 'the average unprotected user would have received 45,000 spam messages in 2008 (up from 36,000 in 2007). All indicators suggest that this trend will continue' (Google 2009). It seems that Gilmore's famous verdict that the Internet interprets censorship as damage and routes around it, applies in a similar way to the filtering of spam. Spammers have managed to successfully route around any type of filtering mechanisms.

Until 2003 cybercrime used to be an annoying but ultimately harmless business (van Eeten et al. 2008: 6). In 2003, spamming techniques began to change and cybercrime underwent reorganization. The forerunner of this transformation was a virus called Sobig,[21] first noticed 'in the wild' in early 2003. Sobig combined elements of a self-replicating worm and a 'metamorphic Trojan horse'[22]. It was designed to modify itself by autonomously downloading additional files from various websites over several stages. In its final phase, the original virus had completely disappeared and was replaced by a hidden Trojan configured to function as an open mail relay to send out spam. Computers infected by Sobig turned into 'zombies' that were no longer controlled by their owners but by third parties who ran networks of zombies known as 'botnets' (for an overview, see OECD 2009: 28-34).

A few years after open mail relays had more or less disappeared from the Internet, spammers had figured out a way to re-create them, ironically by turning individual computers into open relays. The breathtaking Sobig became the fastest spreading virus ever in 2003 with one million copies reported to be caught within 24 hours by one security company. Botnets have made it possible to send out spam anonymously and in ever growing quantities. Due to this new virus-based spamming technique, two third of all spam circulating on the Internet in 2003 originated from infected zombie computers and for the first time, spam at times exceeded the volume of legitimate mail. More recent data suggest that spam by now oscillates between 75% and 80% of all email (OECD 2009: 34) and that between 5 and 20% of all computers may be infected with malware that can turn them into zombies (House of Lords 2007: 14; van Eeten 2008: 6).

Whereas Sobig infected computers by conventional means in the form of 'email attachments', more recent versions of malware programs have been propagated through malicious websites, thereby exploiting another vulnerability of the Internet,

[20] Paul Graham, Aug. 2002 [http://www.paulgraham.com/spam.html].

[21] A good explanation of the 'sobig family' can be found in Steward (2003) (www.secureworks.com/research/threats/sobig/?threat=sobig).

[22] Trojans are pieces of malware that appear like a legitimate program, e.g. a screensaver, but are designed to do something malicious such as creating a backdoor on a computer that can be used by spammers.

the weak protection of web browsers. About 10 per cent of all websites were found to be malicious in a 2007 study (Provos at al. 2007). Visiting a compromised website causes 'drive-by downloads', an automatic, unnoticeable installation of malware that implants a 'ghost' in the browser, henceforth recording every key stroke of the user and spying on passwords and other forms of sensitive information (Provos et al. 2007; Thomas & Martin 2006). A recent example of this sophisticated technique is a botnet called Torpig, which was coordinated, 'harvested' and hidden through regularly changing Internet addresses and domain names.[23] The arms race between the cyber crime and the security industry is expansive and, following the tradition of self-regulation on the Internet, predominantly occurs below governmental intervention.

The trading of illicit digital goods on the Internet takes place with the help of one of its oldest communications services called Internet Relay Chat (IRC). This communication service provides the exchange of messages in real-time through dedicated virtual channels. The so-called 'underground economy' has re-interpreted these virtual channels as a means to create open markets for goods and services. The trading of illicit products has become a fast and very lucrative business. Thomas & Martin (2006) calculated that within 24 hours and in just one of the many IRC channels operating in parallel, access information to accounts worth at least 1.5 million US Dollars changed hands (see also Franklin et al. 2007 for more empirical data).

The year 2003, when the first botnets appeared on the Internet, has been recognized as a turning point in the organization of cybercrime. Anderson et al. (2008: 10) portray this change as an 'online criminal revolution' and liken it to the 'rapid specialization by artisans' in the eighteenth century that let to the Industrial Revolution. Cybercrime has evolved from a 'reputation economy (i.e., receiving 'street cred' for defacing Web sites or authoring viruses)' into a 'bustling underground economy (…) that actively flaunts the laws of nations and the rights of individuals' (Franklin et al. 2007). Characteristic of this new underground economy are specialized networks of skills and functions. There is the new profession of the 'botnet herder' or 'botnet master' responsible for managing the networks of computer zombies and rents them out as a service (see Stone-Gross et al. 2009: 8) to spammers or to 'phisherman'[24], another new profession which specializes in operating bogus websites of banks or shops to obtain access to credit cards, passwords and other personal information (Anderson et al. 2008: 10). Other relevant functions are the 'malware writers' who produce malicious software on commission, the brokers who manage the trading of tools, credit cards or social security numbers and the 'mules' and 'drops' which facilitate the money laundering (see Thomas & Martin 2006). Botnets have become a 'contracted commodity' with 'weekly rental rates for a botnet at USD 50-60 per 1000-2000 bots, or around 33 cents per compromised computer' (OECD 2009: 32f). The underground networks now also invest some of their profits in 'proper research, development, quality control and customer service' (Anderson et al. 2008: 11). Even statistics are collected to measure performance and 'to make sure their revenue stream is maintained' (Evron 2008).

[23] Torpig has been hijacked for 10 days by a group of researchers who monitored about 180,000 infections and the collection of 70 GB of data (Stone-Gross et al. 2009).

[24] According to the report of the House of Lords (2007: 14), the cost of renting a botnet for spamming amounts to 3–7 US cents per zombie per week.

Hence, cybercrime has evolved from an amateur business into a highly profitable global industry, which applies similar marketing, accounting and product development strategies as other international businesses. They make creative use of various Internet services such as Internet Relay Chat, Email and the WordWideWeb; and they constantly renew their strategies. Malware producers have proven to be as flexible, anticipatory and inventive as other industries on the Internet and indeed, to some extent, they mirror the dynamic development of e-commerce. Cybercrime represents ways of using the Internet and driving its further transformation that were totally unforeseen. The developers of the architecture and its basic services assumed like-minded and well-meaning users; more precisely perhaps, they created a communication infrastructure primarily for themselves. Their high expectations of this new network were grounded in the interpretive openness of digital technology. This flexibility was regarded as a feature, not a risk; precautions against its abuse were not seriously considered. Against this background, cybercrime emerged as an unintended consequence.

### The flip side of the utopian dream

The advent of spam, fraud and theft has lasting technical and political implications for the Internet, its tradition of ungovernability and its spirit of openness. The explosive growth of cybercrime has shown that the Internet does indeed empower all users and usages. The Internet has come to be regarded by more and more users as a dangerous place, and the networks' endpoints, once the privileged locus of innovation, have disappeared behind walled gardens and firewalls. Yet, firewalls are not well suited to discriminate. Since they are designed to treat everything new and unknown as a potential threat, they create barriers against malicious as well as desirable innovations (Handley 2006: 124). Cybercrime also affects the general attitude towards self-regulation on the Internet. Lessig (2006: 27) probably reflects the zeitgeist with his observation that, notwithstanding the old belief in the Internet's unregulability, ‘in a world drowning in spam, computer viruses, identity theft, copyright 'piracy', and the sexual exploitation of children, the resolve against regulation has weakened. We all love the Net. But if some government could really deliver on the promise to erase all the bads of this space, most of us would gladly sign up.’ On the same note Zittrain (2006: 1977) predicts a shift in consumer demand for more security which could lead to ‘an outright elimination’ of what he calls the ‘generativity’ of the Internet. Unless we, the users, accept a revision of the end-to-end principle, Zittrain (2006: 1978) warns, ‘our PCs may be replaced by information appliances or may undergo a transformation from open platforms to gated communities to prisons, creating a consumer information environment that betrays the very principles that animate end-to-end theory’.

The imminent death of the Internet has been predicted many times and for changing reasons. In this case, however, the danger does not emanate from the outside world; its source is inherent to the Internet architecture itself. The end-to-end principle has enabled an impressive flow of innovations but it also allows for a growing amount of destructive and malicious activities. In retrospect, the development of the Internet seems to have brought about its own specific set of unintended consequences. The emancipatory aspirations for a libertarian cyberspace that would, to unparalleled extents, privilege social freedom over regulation, may end up in a socio-technical

regime that largely undermines and reverses the freedom it once enabled. Lessig (2006: 32) goes so far as to predict that ‘cyberspace will be the most regulable space humans have ever known. The 'nature' of the Net might once have been its unregulability; that 'nature' is about to flip.’ Lessig's bleak foresight seems to confirm Merton's (1936: 903) observation that ‘activities oriented toward certain values release processes which so react as to change the very scale of values which precipitated them’.

When the engineering community chose to delegate control over the network to its endpoints and thus preclude hierarchical forms of governance, it was assumed that users could be trusted and comprehensive regulation would therefore be unnecessary. In the 1990s, the idea of public regulation even evoked a political counter movement. The expectation of cyberspace as an enabler of a new social order implied explicit disregard for the norms, institutions and practices regulating other types of communication media. However, Internet users turned out to be more diverse than expected, and so were the ways they made use of the freedom the Internet provided. The advent of cybercrime, understood as a form of abusing collective Internet resources, indicated that experiences in cyberspace would after all be not that different from those of the society that brought forward the Internet in the first place.

Describing cybercrime as an unintended consequence of the political and technical norms constituting the Internet does not imply that the actions of engineers and early academic users caused cybercrime. Furthermore, malicious activities on the Internet have recently become so complex themselves that relating them solely to architectural decisions in the 1980s and their interpretation in the 1990s would oversimplify matters. Rather, the notion of cybercrime as a perverse effect sheds light on the tacit assumptions underlying the expectations and visions of those who believed in the feasibility of a superior social order on the Internet.

One of the telling assumptions was that government regulation constituted the main if not the only threat to the libertarian vision of life in cyberspace. Other, obviously problematic, assumptions were that the plastic, innovation-friendly character of digital technology did not entail any risks (and therefore no need for precautions against malpractices) and that the Internet would remain as socially homogeneous a space as it was until the mid 1990s. The insight that might be gained beyond the shortcomings of these expectations pertains to the relation of freedom and regulation. The anti-regulatory, libertarian spirit of the1990s framed this relation as an antagonism. Regulation was bluntly associated with the death of the Internet's free culture. One might wonder if a less confrontational understanding of the relation between freedom and regulation would have led to more advanced forms of self-governance on the Internet – and hence a different set of unforeseen outcomes.

## References


Abbate, J. (1999) *Inventing the Internet*. Cambridge (MA): MIT Press

Aboba, B. and D. Elwyn (2007) *Reflections on Internet Transparency*. Request for Comments (RFC ) 4924, July 2007. Available at www.rfc-editor.org/rfc/rfc4924.txt

Anderson, M. (2004) *Spamming for dummies. A cautionary tale*. The Register, 27 July 2004. Available at www.theregister.co.uk/2004/07/27/spamming_for_dummies/

Anderson, R, R. Böhme, R. Clayton and T. Moore (2008) *Security Economics and the Internal Market*. Report to the European Network and Information Security Agency (ENISA). Available at www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/?searchterm=Security Economics and European Policy

Barlow, J.P. (1996) *A Declaration of the Independence of Cyberspace*. 8 February 1996. Available at www.eff.org/~barlow/Declaration-Final.html

Beck, U. (2009) *World at Risk*. Cambridge: Polity

Blumenthal, M.S. and D.D. Clark (2001) 'Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world', in *ACM Transactions on Internet Technology* 1(1): 70–109

Boudon, R. (1982) *The Unintended Consequences of Social Action*. London: Macmillan

Christou, G. and S. Simpson (2007) 'Gaining a stake in global Internet governance – the EU, ICANN and strategic norm manipulation', in *European Journal of Communication* 22(2): 147–64

Clark, D.D., C. Partridge, R.T. Braden, B. Davie, S. Floyd, V. Jacobson, D. Katabi, G. Minshall, K.K. Ramakrishnan, T. Roscoe, I. Stoica, J. Wroclawski and L. Zhang (2005) 'Making the world (of communications) a different place', in *ACM SIGCOMM Computer Communication Review* 35(2): 91–6

Clark, D.D. (1988) 'The design philosophy of the DARPA Internet protocols', in *Computer Communication Review* 18(4): 106–14

Drezner, D.W. (2004) 'The global governance of the Internet: bringing the state back in', in *Political Science Quarterly* 119(3): 477–98

van Eeten, M.J.G. and J.M. Bauer (2008) *Economics of Malware: Security Decisions, Incentives and Externalities*. STI Working Paper Series. Paris: OECD

Everett-Church, R. (1999) *The Spam that Started it All*. Wired, 13 April 1999. Available at www.wired.com/politics/law/news/1999/04/19098

Evron, G. (2008) *Cyber Crime: An Economic Problem*. CircleID, 6 September 2008. Available at www.circleid.com/posts/89610_cyber_crime_an_economic_problem/

Franklin, J., A. Perrig, V. Paxson and S. Savage (2007) *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*. ACM Conference on Computer and Communications Security, Alexandria (VA), 29 October – 2 November 2007

Genschel, P. (1995) *Standards in der Informationstechnik. Institutioneller Wandel in der internationalen Standardisierung*. Frankfurt am Main: Campus

Geist, M. (2003) 'Cyberlaw 2.0', in *Boston College Law Review* 44(2): 323–58

Giddens, A. (1987) *Social Theory and Modern Sociology*. Stanford University Press

Goldsmith, J. and T. Wu (2006) *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.

Google Enterprise Blog (2009) *2008: The Year in Spam*. Available at http://googleenterprise.blogspot.com/2009/01/2008-year-in-spam.html

Hafner, K. and M. Lyon (1996) *Where Wizards Stay Up Late*. New York: Simon & Schuster.

Hambridge, S. (1995) *Netiquette Guidelines*. Request for Comments (RFC) 1855. Available at http://tools.ietf.org/html/rfc1855

Handley, M. (2006) 'Why the Internet only just works', in *BT Technology Journal* 24: 119–29

Harasim, L.M. (1994) 'Networlds: networks as social space', in L.S. Harasim (ed.) *Global Networks. Computers and International Communication*. Cambridge: MIT Press, 15–34

Hirschman, A.O. (1982) 'Rival interpretations of market society: civilizing, destructive, or feeble?' in *Journal of Economic Literature* 20(4): 1463–84

House of Lords (2007) *Personal Internet Security. 5th Report of Session 2006–07*. London: Science and Technology Committee

Isenberg, D. (1997) 'The rise of the stupid network', in *Computer Telephony*, August 1997: 16–26

Kempf, J. and R. Austein (2004) *The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture*. Request for Comments (RFC) 3724. Available at ftp://ftp.rfc-editor.org/in-notes/rfc3724.txt

Kapor, M. and D. Weitzner (1994) 'Social and industrial policy for public networks: visions for the future', in L.M. Harasim (ed.) *Global Networks: Computers and International Communication*. Oxford University Press

Kleiner, K. (2008) *Happy Spamiversary! Spam Reaches 30*. NewScientist, 25 April 2008. Available at www.newscientist.com/article/dn13777-happy-spamiversary-spam-reaches-30.html

Lemley, M.A. (2002) *Place and Cyberspace*. Research Paper No 102, Berkeley School of Law, University of California

Lessig, L. (1999) *Code and other Laws of Cyberspace*. New York: Basic Books

Lessig, L. (1998) *Governance Keynote speech*. CPSR Conference on Internet Governance. Available at http://cyber.law.harvard.edu/works/lessig/cpsr.pdf

Lessig, L. (1995) 'The path of cyberlaw', in *The Yale Law Journal* 104(7): 1743–55

Malamud, C. (1992) *Exploring the Internet: A Technical Travelogue*. Englewood Cliffs (NJ): Prentice Hall

McConnell, B.W. (1997) 'Governance and the Internet', in *The Internet as a Paradigm*. Queenstown (MD): The Aspen Institute for Information Studies: 71–84

Merton, R.K. (1936) 'The unanticipated consequences of purposive social action', in *American Sociological Review* 1(6): 894–904

MessageLabs (2008) *MessageLabs Intelligence: 2008 Annual Security Report*. Available at www.messagelabs.co.uk/intelligence.aspx

Morrison, A.H. (2009) 'An impossible future: John Perry Barlow's "Declaration of the Independence of Cyberspace"' in *New Media & Society* 11(1-2): 53–72

Nguyen, D.T. and J. Alexander (1996) 'The coming of cyberspacetime and the end of the polity' in R. Shields (ed.) *Cultures of Internet. Virtual Spaces, Real Histories, Living Bodies*. London: Sage, 99–124

OECD (2009) *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*. Paris: OECD.

Popper, K. (1963) *Towards a Rational Theory of Tradition. Conjectures and Refutations: The Growth of Scientific Knowledge*. London: Routledge, 161–82

Post, D.G. (1998) 'The "unsettled paradox": the Internet, the state, and the consent of the governed', in *Indiana Journal of Global Legal Studies* 5(2): 521–43

Post, D.G. and D.R. Johnson (1996) 'Law and borders: the rise of law in cyberspace', in *Stanford Law Review* 48: 1367–1402

Provos, N., D. McNamee, P. Mavrommatis, K. Wang and N. Modadugu (2007) *The Ghost In The Browser. Analysis of Web-based Malware*. Available at www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf

Reed, D.P., J.H. Saltzer and D.D. Clark (1998) *Active Networking and End-To-End Arguments*. Available at http://web.mit.edu/Saltzer/www/publications/endtoend/ANe2ecomment.html

Reidenberg, J.R. (1998) 'Lex informatica: the formulation of information policy rules through technology', in *Texas Law Review* 76(3): 553–84

Russell, A.L. (2006) '"Rough consensus and running code" and the Internet-OSI standards war', in *IEEE Annals of the History of Computing* (July-September): 48–61

Saltzer, J.H., D.P. Reed and D.D. Clark, (1984) 'End-to-end arguments in system design', in *ACM Transactions on Computer Systems* 2(4): 277–88

Salus, P.H. (1995) *Casting the Net. From Arpanet to Internet and Beyond*. Reading (MA): Addison-Wesley

Santos, B. de S. (2002) *Toward as New Legal Common Sense. Law, Globalization and Emancipation*. London: Elsevier

Santos, B. de S. (2001) 'Toward an epistemology of blindness. Why the new forms of "ceremonial adequacy" neither regulate nor emancipate', in *European Journal of Social Theory* 4(3): 251–79

Shah, R.C. and J.P. Kesan (2007) 'The privatization of the Internet's backbone network', in *Journal of Broadcasting & Electronic Media* 51(1): 93–109

Spar, D.L. (1999) 'Lost in (cyber)space: the private rules of online commerce', in A.C. Cutler, T. Porter and V. Haufler (eds.) *Private Authority and International Affairs*. Albany: SUNY Press, 31–52

Specter, M. (2007) *Damn Spam. The Losing War on Junk E-mail*. The New Yorker, 6 August 2007

Star, S.L. and J.R. Griesemer (1989) 'Institutional ecology, "translations" and boundary objects: amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39.' in *Social Studies of Science* 19(3): 387–420

Steward, J. (2003) *Sobig.a and the Spam You Received Today*. Available at www.secureworks.com/research/threats/sobig

Stone-Gross, B., M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel and G. Vigna (2009) *Your Botnet is My Botnet: Analysis of a Botnet Takeover*. Available at www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf

Thomas, R. and J. Martin (2006) *The Underground Economy: Priceless*. Available at www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf

Tocqueville, A. de (1945) *Democracy in America*. Vol. II. New York: Vintage Books

Valauskas, E.J. (1996) *Lex Networkia: Understanding the Internet Community*. First Monday 1(4-7).

Vernon, R. (1979) 'Unintended consequences', in *Political Theory* 7(1): 35–73

Walker, J. (2003) ‘The digital imprimatur - how big brother and big media can put the Internet genie back in the bottle’, in *Knowledge, Technology & Policy* 16(3): 24–77

Wall, D.S. (2005) ‘Digital realism and the governance of spam as cybercrime’, in *European Journal on Criminal Policy and Research* 10(4): 309–35

Wagner, P. (2008) *Modernity as Experience and Interpretation. A New Sociology of Modernity*. Cambridge: Polity Press

Werle, R. (2002) ‘Internet @ Europe: overcoming institutional fragmentation and policy failure’, in J. Jordana (ed.) *Governing Telecommunications and the New Information Society in Europe*. Cheltenham: Edward Elgar, 137–58

Zittrain, J.L. (2006) ‘The Generative Internet.’ *Harvard Law Review* 119: 1974–2040