

The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

By
Joseph Savirimuthu
Liverpool Law School
University of Liverpool
Liverpool, UK
0151 7942806
jsaviri@liverpool.ac.uk

Presented At The 35th Research Conference on Communication, Information and Internet Policy
George Mason University School of Law in Arlington, VA

Abstract

This article uses Luhmann's view of society as comprising of communications to deepen our understanding of why it is information insecurity is a problem that only society can solve, and accordingly, not through centralized frameworks provided by law, political or economic systems. Accordingly, as political and legal institutions do not have the monopoly for creating order and security, we need to broaden our understanding of governance and examine how best the structures and processes for information gathering, private ordering and standard setting will now have to be negotiated in decentralised and distributed networks.

Keywords: Complexity, Systems Theory, Regulation, Information Security, Computer Misuse Act 1990, Police and Justice Act 2006

I. Introduction

"Take note, theologians, that in your desire to make matters of faith out of propositions relating to the fixity of sun and earth you run the risk of eventually having to condemn as heretics those who would declare the earth to stand still and the sun to change position -- eventually, I say, at such a time as it might be proved that the earth moves and the sun stands still."¹

More than any other time in history, mankind faces a crossroads. One path leads to despair and utter hopelessness. The other, to total extinction. Let us pray we have the wisdom to choose correctly.²

¹ Quotations by Galileo Galilei. From the *Dialogue*, available at <http://www-gap.dcs.st-and.ac.uk/~history/Quotations/Galileo.html>

² Woody Allen, http://www.quotationspage.com/quotes/Woody_Allen/31

The bacteria *Yersinia pestis*, reputed to originate from the plains in Central Asia, killed over 20 million people during the Middle Ages.³ *Yersinia pestis* was an unknown known. Unknown to the inhabitants in Central Asia and Europe, the prevailing conditions in 1280-1350, of warm springs and wet summers were ripe for the emergence of a bacterium with fatal propensities.⁴ The ease with which the bacteria leveraged the resources of biological organisms and the physical landscape illustrates the importance of deepening our understanding of complex internally differentiated structures and components of unicellular microorganisms and the way these organise themselves and interact with other systems?⁵ Does the logic of self-referential systems have any explanatory value to the quest for order and security in the Internet?⁶ Legal regulations are generally perceived as having information gathering, private ordering and standard setting characteristics.⁷ This paper draws on Luhmann's conceptualisation of society as comprising of communications to deepen our understanding of why it is information insecurity is a problem that only *society* can solve, and accordingly, not through centralized frameworks provided by law, political or economic systems.⁸ The view that society is the framework for creating order and security compels us to re-examine how institutions like law, economics and politics can be integrated into the heterarchical networks of information gathering, private ordering and standard setting. Issues of risk, responsibility and good governance not only figured prominently in the amendments made to the Computer Misuse Act 1990 but is now given priority in the present administration in the United Kingdom.⁹ Current attempts to regulate denial of services attacks (DoS) will be used to examine some of the pervasive themes and strategies. The paper has two objectives: first, to use Luhmann's systems perspective as a framework for understanding legislative and juridical strategies regarding DoS activity and exploring the significance of their limitations and second, to assess the implications of viewing society as being constituted by communications for policymaking and governance in the field of information security.¹⁰

II. Framing Problems

“My Bill seeks to specify a new offence of denial of service. A denial-of-service attack occurs when a deliberate attempt is made to stop a computer performing. Examples include attempts to flood a network, thereby preventing legitimate network traffic; attempts to disrupt the connections between two machines, thereby preventing access to a service; attempts to prevent a particular individual

³ BBC, “Climate linked to Plague Disease” 26 July, 2006 (available at <http://news.bbc.co.uk/1/hi/sci/tech/5271502.stm>) (Accessed 15 April, 2007).

⁴ See Fact Sheet produced by Department of Health and Human Sciences at <http://www.cdc.gov/ncidod/dvbid/plague/resources/plagueFactSheet.pdf> (accessed, 26 July 2007) F Sebbane, “Adaptive response of *Yersinia pestis* to extra cellular effectors of innate immunity during bubonic plague” PNAS August 1, 2006, vol. 103, no. 31, pp 11766-11771.

⁵ M Castells, *The Rise of The Network Society* Volume 1 (Oxford: Blackwell, 2000) pp 3-25, 407-459.

⁶ Joint Economic Committee, *Security in the Information Age: New Challenges, New Strategies* (US Congress, May 2002).

⁷ C Hood, *The Government of Risk* (Oxford: OUP, 2004) pp 21-27.

⁸ M King and C Thornhill, *Luhmann on Law And Politics* (Oxford: Hart Publishing, 2006).

⁹ Government response to Better Regulation Commission report “*Risk, Responsibility, Regulation: Whose Risk Is It Anyway?*”. Available at <http://www.cabinetoffice.gov.uk/regulation/documents/reform/risk.pdf>.

¹⁰ The critiques of Luhmann's use of autopoiesis and current literature on Cyberlaw approaches to information security will be the subject of another extended article.

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

from accessing a service; and attempts to disrupt services to a specific system or person.”¹¹

Section 3 of the Computer Misuse Act 1990(as amended) broadly provides that a person will be guilty of an offence if he does any act in relation to a computer, which is intended to impair the operation of any computer, prevent or hinder access to any program or data held in any computer, or to enable any of the unauthorised acts to be done.¹² The perceived shortcomings of the previous statutory provisions as being limited to criminalising unauthorised acts like disseminating malicious code, deleting has now been addressed. It is however important not to confine our understanding of this section to issues relating to the deficiencies of the law, the “gaps” that have been filled and finally, prospective shortcomings. One reason is that DoS attacks cannot be seen purely as a problem that law, markets and politics can resolve. We can add a further dimension to the deterrent capacity of the 1990 Act by raising an epistemological problem. How do we know that the removal of the words ‘unauthorised modification’ in the section and the identification of “impairment” as an unauthorised act will provide the magic bullet and deliver the desired results envisaged in the Private Members Bill? The growing volume of literature expressing discontent with regulatory attempts to address the information security risks posed by cybercrime underscores the entrenched view that the orthodox approach to coercing potential cyber criminals into conformity, plainly needs to be re-examined.

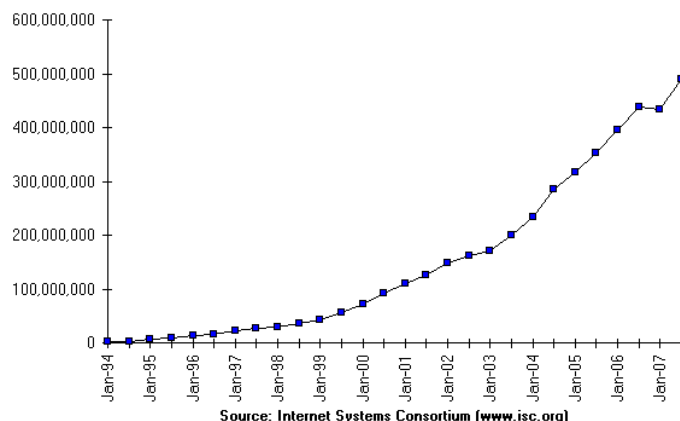
The scepticism legal systems attract in this sphere of governance is unlikely to recede if we take into account the technology and its context. DoS attacks achieve their potency by exploiting two fundamental attributes in the space of flows that complex network communication infrastructures make possible. First the technical infrastructure now enables asynchronous interactions in decentralised and distributed networks. The infrastructure and application layers provide the structures for information flows. Information flows between units in the network is facilitated by the adoption of specifications that permit interoperability between the layers. Applications in the form of browsers, software and security products permit interactions, for example, between software and hardware. The data link layer permits information now to be transmitted across the Internet. Second, the presumptive norm of access contributes to the ease with which DoS attackers mobilise the resources of the Internet to externalise the costs of their actions. Governance is now a global issue as the network of networks removes the traditional barriers of time and space. As society becomes increasingly networked at varying levels in the new space of flows of capital, goods and information the systemic

¹¹ Right Honourable Tom Harris MP, Hansard 12 July, 2005 Column 700. Available at <http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm050712/debtext/50712-05.htm>

¹² On DPP v Lennon, see J Oates, “Kid who crashed email server gets tagged”, 23 August, 2006. Available at http://www.theregister.co.uk/2006/08/23/email_bomber_guilty/. (accessed 7 June, 2007). Also A Savirimuthu and J Savirimuthu, “The Computer Misuse Act 1990, Denial of Services Attacks and the Insecure Panopticon” (forthcoming). The substantive provisions are set out in full at http://www.opsi.gov.uk/acts/acts2006/ukpga_20060048_en_7#pt5-pb2-11g36.

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

effects of DoS attacks are immense.¹³



Consider the amenability of juridical and enforcement mechanisms when directed at a brute force attack using botnets, in the following example. On 30th September 2007, you receive an email that is currently being sent virally across the Internet. The attacker, under the name of Lord Voldemort, will launch a brute force attack against all Harry Potter fan websites in the UK and US. It appears from the email that Lord Voldemort is unhappy that Harry Potter fans launched an attack on a P2P news website that released accounts of the final plot before the official scheduled public offering – Torrent Freak.¹⁴ Bots, are essentially software programs that act as intermediaries for another user or program.¹⁵ Internet relay channel bots are increasing at a rate of 1000 a month.¹⁶ DoS attackers exploit program flaws in peer-to-peer networks to impair network systems.¹⁷ All that this attacker has to do is insert bogus packets into the TCP SYN stream. STP protocols are particularly vulnerable to DoS attacks since the TCP/IP stack proceeds on the basis that the requests are legitimate.¹⁸ In the absence of exceptional intelligence, it is unlikely that social communication systems like law and politics will deter Lord Voldemort or even launch a prosecution.¹⁹ Could it just be that our constant preoccupations with law reform and the accompanying disappointments with its results have to do with the fact that we do not

¹³ See generally the panel papers organised by the Yale Information Society Project, *The Global Flow of Information* (2004) available at <http://islandia.law.yale.edu/isp/GlobalFlow/index.html>.

¹⁴ See “Harry Potter and the DDoS of Destiny” July, 7 2007. Available at <http://www.broadbandreports.com/shownews/Harry-Potter-and-the-DDoS-of-Destiny-85828>.

TorrentFreak’s site at <http://torrentfreak.com/torrentfreak-under-attack/>

¹⁵ D Sancho, “The Future of Bot Worms”, available at www.antivirus.about.com (accessed 28, May 2007).

¹⁶ See J Canavan, “The Evolution of Malicious IRC Bots”. Available at <http://whitepapers.zdnet.co.uk/0.1000000651.260160051p.00.htm> (accessed 29, May 2007).

¹⁷ A recent report by the Internet Security Operations Task Force issued in July 2007 shows the pervasiveness of botnets and their mapping activities: http://www.isotf.org/?page_value=10 (accessed, August 1, 2007), N Lanelli, *Botnets as Vehicle for Online Crime*, CERT/CC (2005) available at www.cert.org/archive/pdf/Botnets.pdf (accessed 23, May, 2007). See also E Cook, F Jahanian, D McPherson, “The Zombie Roundup: Understanding, Detecting and Disrupting Botnets”, USENIX SRUTI’05 Available at www.usenix.org/events/sruti05/tech/talks/cooke.pdf (accessed 25, May 2007).

¹⁸ D Denning, *Information Warfare and Security* (UK: ACM, 1999) p 375

¹⁹ See M King, “What’s The Use of Luhmann’s Theory?”, *Luhmann On Law And Politics*, *supra* n8, p 56. It should be made clear that at no time I make the argument that law has no place in private ordering. My premise is that law is not the *sole* instrument of governance.

attach sufficient importance to the way social systems, including law are autonomous, whose unity is defined by self-reference? More importantly, could it be that societies evolve and adapt not only through its formal institutional constructs but also through interacting with other entities and systems that exist in different multi-levels of society? To understand why systems like law continue to be regarded as systems with suboptimal regulatory capabilities we need a theory that provides us with an epistemological and linguistic shift – social systems as autopoietic communication systems may be a possible heuristic.²⁰

III. Autopoietic Communication Systems

1. A Primer

Systems theory is an epistemological device popular in disciplines like computing, physics, biology and mathematics.²¹ The central idea of systems thinking revolves around the proposition that the organisation of living organisms cannot be understood without an understanding of the process by which components interact with each other, self-organise and self-produce whilst retaining the organisation's functional unity. Cilliers regards complex systems as those, which are not merely constituted by the sum of its components but also by their interactions with each other.²² Systems and their boundaries cannot be understood by reference to each component part or parts.²³ In simple terms, it can be said that what distinguishes a burglar alarm on the other hand from complex systems like the brain, society, markets or law on the other is that in the case of the former the components in the device cannot be said to interact with each other, and do not possess structures for self-organisation and adaptation.²⁴ Ongoing changes in the structure of the system are influenced by interactions between element within or as a result of changes resulting from interactions with the environment. The market economy is an example of a complex system. Its organisation comprises of a set of relations that distinguish it from, let us say, a family, a political or legal system. For a market to exist there must be buyers and sellers and a mechanism for facilitating transactions. The buyers and sellers can be viewed as constituting a dynamic network of interactions. These ongoing interactions may either produce additional buyers and sellers or result in a boundary being created to foreclose further transformations. For example, whilst auctions, B2B and B2C transactions can be viewed as sub-systems of markets, their structures differ from each other. A systems view of the vibrancy of markets in Second Life, for example, would be that buyers and sellers interact with each other in the organisation, with their own phenomenology. The key point here is that any changes to the system will be determined not by the elements but by the system and its structure. The relative autonomy of the component parts and their ability to self-organise and interact is what makes predictability

²⁰ See GAO Report, "Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses", available at <http://www.gao.gov/new.items/d07837.pdf> (accessed, 17 August, 2007).

²¹ N Wiener, *Cybernetics: or Control and Communication in the Animal and the Machine* (Cambridge, MA: MIT Press, 1961) (Orig Pub 1948) p162, H Maturana and F Varela, *Autopoiesis and cognition* (D Reidel: Dordrecht, Holland, 1972) pp xi-xvii.

²² P Cilliers, *Complexity and Postmodernism* (Oxford: Routledge, 1998) pp 2-4.

²³ N Luhmann, *Law as a Social System* (Oxford: OUP, 2004) pp 64-66.

²⁴ Y Bar-Yam, *Dynamics of Complex Systems* (US: Westview Press, 2003) p1, WR Ashby, *Design for a Brain: The Origin of Adaptive Behaviour* (New York: Wiley, 1960) (2nd rev ed) p 36, L Von Bertalanffy *General Systems Theory: Foundations, Developments, Applications* (New York: Braziller, 1968) and H Von Foerster, *Observing Systems* (Seaside, Cal: Intersystems, 1981).

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

and analysis of living and social systems complex. Complex systems are regarded as possessing the following characteristics:²⁵

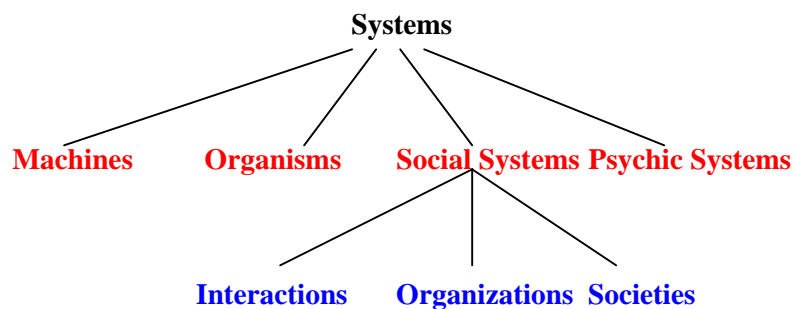
Mutual Interactions	The interactions and relationships between the component parts are distributed and highly integrated. The interactions involve the transference of information and not limited to physical interaction
Behaviour	The relations between the elements in the system produce a responsive behaviour and patterns of interaction. Loops in the interactions ensure recurrent negative or positive responses
Non-linear Interactions	Non-linearity ensures the self-organising and self-reproduction capacity of the system. The result of the interactions may also produce unexpected or unintended outcomes.
Open Systems	Complex systems are open and accordingly interact with its environment. As the boundaries between the system and its environment are fluid. Operational closure involves an observer determining the purpose of the system.
Equilibrium	Conditions for interaction are far from stable. The continued dynamism of the system requires an ongoing process of self-organisation, natural selection and self-reproduction.
Self-organization	A pre-condition for complex system is the capacity of individual components for self-organisation
Adaptive behaviour and history	Complex systems have a history and their ability to adapt their structures is not limited to its responses to changes in the environment.
Isolation	Each component operates in isolation and does not know what is happening in the system. Each element only responds to information available locally

2. Niklas Luhmann and *Law as a Social System*

The constructivist epistemology advocated by Niklas Luhmann, deploys a second order observation of society (ie the communications involve observations about communications taking place).²⁶ Communication is the basic component of the social system and it is these that constitute society. The social system can only communicate about itself. It cannot communicate outside itself, as there is 'no other'. Systems, according to Luhmann, exist *a priori* and classified in terms of:

²⁵ P Cilliers, *supra* n19, pp 3-5.

²⁶ This section provides a synthesis of Luhmann's ideas. Extracts and citations have not been included in this draft. According to Luhmann social systems communicate by talking about talking or writing about writing: N Luhmann, *Observations on Modernity*. (Translated W Whobrey) (Stanford University Press: Stanford, CA, USA, 1992) and N Luhmann, *Social Systems*, (Translated J Bednarz Jr, D Baecker). Stanford University Press: Stanford, CA, USA, 1995).



Social systems comprise of three sub-systems – societies, organisations and interactions. Luhmann regards communications, not individuals as the focal point of society. This methodology departs from the prevalent liberal ideology, that rational, utility maximising individuals constitute society. Society comprises of self-referential and independent sub-systems, which retain their autonomy. For societies, it is only those communications that take place within each type of system (e.g. law, economics, politics, media, education, medicine and arts) are deemed to give rise to meaningful communications.²⁷ This is not to say that society does not incorporate communications from individuals and those belonging to the lifeworld. Luhmann’s aim in distinguishing meaningful communication between systems like politics, law and economics from those communications those taking place in organisations or interactions is a prelude to his construction of functionally differentiated systems. Communications between individuals are viewed as interactions. Meaningful communications, however, can only take place between systems. Communications comprise of the unity of utterance, information and understanding. The elementary units of meaningful communications are constituted by the synthesis of information, communication and comprehension. Interactions between individuals are not viewed as meaningful communication until these have been transformed as such by society’s sub-systems. For example, information about the spread of the foot and mouth disease or SARS will not be viewed as meaningful communications, until they are processed by law (in the form of the legal and evidentiary rules on Health & Safety), health (in the form of medical statistics), economics (in the form of communities and authorities assessment of the impact on tourism and health services) and politics (in the form of public opinion and need for legislation).²⁸ Society and the other types of systems do not communicate with the environment. Society is a closed system but it communicates about its environment. Other sub-systems part of a system’s environment. The environment may cause perturbations or irritations but it is the system that determines how the disturbance is to be processed.²⁹ Sub-systems interact with each other in a way that a system and its environment cannot. Since legal systems are normatively closed but cognitively open, interaction with the psychic, organisation and other functional subsystems is now made possible. For example, concerns that prosecution for DoS attacks may be obstructed owing to the ambivalence of section 3 of the Computer Misuse Act 1990, can be illustrated by the nature of the amendment made by Parliament. Another illustration of the autonomy of sub-systems and their interdependence with each other can be seen in the response of markets in the area of cybercrime. Perceptions of the expanding risk environment and the constraints imposed on political and legal systems have a bearing on the

²⁷ N Luhmann, *Law as a Social System*, *supra*, n3.

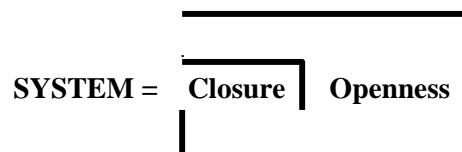
²⁸ I modify the example provided in M King and C Thornhill, *Niklas Luhmann’s Theory of Politics and Law* (Hampshire: Palgrave Macmillan, 2005) p8.

²⁹ It is beyond the scope of this paper to examine whether the distinction between societies, organizations and interactions is necessary or how we determine which communication is to be prioritised or differentiated – the system/environment distinction is not particularly clear. Indeed, what is “differentiation”, particularly as the distinctions would be subject to the caveat of contingency?

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

markets response to the growing of anti-virus and security solutions.³⁰ The market is now worth \$4.684 billion, and has increased by 17.1 per cent in the previous year. Structural coupling, according to Luhmann is one way through which systems respond to irritations and perturbations emerging in its environment and re-constitute themselves. Luhmann's account of law as an autopoietic system draws on biological, systems and cybernetic theories.³¹ Self-organisation is not the product of some *a priori* normative or procedural process that gives the system its unity. The nature of the autopoietic organisation is such that the process of self-production emerges from links being made between events and operations within its structures. One possible view is that systems aim to reduce complexity. Another is that a system is designed to fulfill its particular needs and problems. The unity cannot emerge unless the system differentiates itself from its environment and other systems.

An autopoietic system can be depicted in the following manner:³²



Codes and functions are central to a system's autonomy and its ability to differentiate itself from both the environment and other systems. The term 'functional' is not to be understood in its utilitarian sense of usefulness as we may understand when we talk about the function of a car or tool. A system is regarded as functional when it structures, processes and disseminates communications. Without autonomy, many of the attributes of a self-organising and self-reproducing system are unlikely to be present. Whatever emerges in a system stems from both its unity and differentiation. The unity of a system and its differentiation is produced through autonomous and recursive elements within the system. Each system has functions, which differentiate it from other systems (ie law, economics and politics). The question may be asked – what differentiates a legal system from other systems? The answer will be the juridical rules, norms and values, the binary code of legal/illegal and the conventions for fulfilling law's function of communicating expectations.³³ Law's function is to stabilise normative and cognitive expectations and it does by transforming "information" into meaningful communications consistent with its autopoietic unity. Law is normatively closed but cognitively open. Consequently, the legal system retains its autonomy to determine the legally normative quality on its elements. It is the legal system that determines whether the meaningful communication is legal/illegal. If the communication cannot be processed in these terms, it ceases to be part of the system. The economic system, for example, transforms "information" into meaningful operations via the price mechanism in response to the problem of scarcity. It is implicit in Luhmann's view of a system being functionally differentiated both from its environment and other system that observations are an ongoing process. It is through these observations of its environment that a sub-system gets to 'know' its own world, which may include other sub-systems. The point here is that each system classifies events, situations and communications according to its self-referential structures. For example, a DoS attack will be viewed in terms of legal/illegal acts by the legal system. Political systems will frame the activity as behaviour, which undermines order and security. This does not however mean that subsystems in society operate in isolation. Luhmann's concept of functional differentiation is intended to explain why it is systems retain their functional identity and do

³⁰ <http://www.frost.com/prod/servlet/svcg.pag/ITNT>

³¹ G Teubner, *Law as an Autopoietic System* (Oxford: Blackwell, 1993) p 9-10

³² D Beacker, "Why Complex Systems are Also Social and Temporal", Paper submitted to, and not accepted by, European Conference on Complex Systems, Dresden (October 1-5, 2007).

³³ N Luhmann, *Law as a Social System*, *supra*, n23, p467.

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

not, for example, mirror the functions of other sub-systems.³⁴ By functional differentiation, Luhmann views each sub-system as comprising of an organisation with distinctive structures and processes for evolution, adaptation and communication. Each sub-system has its own environment and the interaction takes place through the process of coding and programming. This environment also includes other sub-systems. For example, the economy consists of the buyers and sellers and exchanges. The legal system defines its environment in terms of what is illegal and legal. The observations leading to this classification is initiated through its codes. Each sub-system has its own code. The binary code also enables a system to organise itself autopoietically. The code is the system's internal structure. Coding and programming enable the components in the system to differentiate itself from other systems whilst facilitating the system to organise complexity at different levels.³⁵

Since systems like law, politics and economy operate within their own environments, coding and programming enable each system to make sense of its own world and process information into meaningful communications. Communicative media undertakes these meaningful communications within the system. In economics, money becomes the medium for communication and in the legal system, law would be a common example. As society is viewed as meaningful communications between systems, it follows that coding and programming are central to a system's ability to develop its processes of closure and openness. Coding of the external world ensures that the decision-making processes and structures can function in the sense of providing "legal" solutions to problems encountered in the environment that are juridicalised. The legal system uses its programs to differentiate its functions from those of the environment and other systems. A legal act triggers the operation of the system as it proceeds to utilize the binary code of legal and not legal.

Luhmann also incorporates ideas about self-production and self-organisation (autopoiesis). His integration of autopoiesis ensures that the system has structures and processes that enable it to maintain its functional differentiation from the environment and other sub-systems. The autopoietic and operational closure of systems ensure that their structures are not collapsed into other systems.³⁶ The system uses the linkages created by its decisions, its memory of previous operations and patterns as a means by which functional closure is achieved and which then acts as a filtering mechanism to exclude communications from other systems. It is this process of operational closure that enables a system to retain its autonomy and identity.

3. Summary

Luhmann's framing of relations in social systems as being constituted by communications between systems opens up a new line of exploring social systems which are internally and functionally differentiated. It is often assumed in discussions on the relationship between law, technology and society on the one hand and governance, risk and accountability on the other that software code, law or policy prescriptions from the government will be adequate to manage society which is becoming increasingly differentiated and specialised. Luhmann reminds us that ultimately sustainable systems must either model the complexity of its environment (and become more complex) or reduce the complexity of the environment. Pulling the plug of the computer from the socket is not an option. Communications taking place in almost invariant autonomous systems underscores the growing interest in seeking alternative regulatory solutions.³⁷

³⁴ Ibid, *supra*, n23 p 15.

³⁵ N Luhmann, *The Reality of the Mass Media*, (Stanford: Stanford UP, 2000) chapters 1-4 pp 1-24, N Luhmann, "What is Communication?" in W Rasch (ed) *Theories of Distinction: Redescribing the Description of Modernity* (Stanford: SU Press, 2002) pp 155-168, L Leydesdorff, "Is Society a Self-Organising System?" *Journal for Social and Evolutionary Systems* 16 (1993) 331-349.

³⁶ N Luhmann, "Closure and Openness: On Reality in the World of Law" in G Teubner (ed), *Autopoietic Law: A New Approach to Law and Society* (Berlin: Walter de Gruyter, 1988) pp 12-36.

³⁷ M King, *supra* n8, pp 46-47.

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

“Law, as a social communication system, simply has no way of understanding getting caught/not getting caught through its lawful/unlawful coding. All that the law may do is to encourage burglars to own up to the times when they did not get caught by making it lawful for courts to take them into account in sentencing and in doing so rule out any future prosecution...[the law] sees only what it can see using the restricted vision of its coding.”

The basic assumption underpinning Luhmann’s framing of society as meaningful communications and the role of law in this environment is as many have pointed out, to demonstrate the complexity of society and the reasons positivist or economic theorising fail to account for the richness and density of society and the systems that constitute it.³⁸ The body of knowledge is concerned with understanding the structures and processes by which each system transforms information into communications that serve as inputs and outputs.³⁹ Social sub-systems can be viewed as bounded systems with structures and components that seek to reconcile the functions and goals of the system with the disturbances and conditions of the environment.⁴⁰ Communication systems engage in a complex process of information gathering, ordering and standard setting. This is a non-linear and recursive process that involves not only using existing information but also those, which are created as a result of the autopoietic activities. We need not restate King’s damning (and possibly) correct conclusion about the reduced capabilities of systems like law, politics and economics. Instead of viewing governance in terms of the coordinating instruments provided by law, norms, market and technology, we can instead regard the process of self-organisation as involving complex differentiated and deconstructive processes. If we accept that communications constitute social systems, it becomes important to reflect this process of differentiation and deconstruction when attempting to analyse political and juridical mechanisms and the implications for policymaking resulting from their limitations.⁴¹

IV. The Computer Misuse Act 1990

1. Information Security Threats and The Emerging Regulatory Landscape

What can governments do to arrest the growing information security threats and their implications for trust and integrity in the online environment?⁴² The “G8 Principles for Protecting Critical Information Infrastructures”, which was adopted by the G8 Justice & Interior Ministers, regarded information security as a global problem.⁴³ Information security is an umbrella term describing the range of processes relating to the protection of the integrity, authenticity, accessibility, and confidentiality. Threats from malware, hacking, DoS attacks, dissemination of viruses can compromise the integrity, confidentiality, authenticity and availability of information and network systems. Serious organised crime is now seen as being behind many of the malware and DoS attacks. The overall threat to the United Kingdom from organised crime is at a very high level. Current estimates of the social and economic costs of serious organised crime include deterrent and enforcement costs exceeding

³⁸ N Luhmann, *Law as a Social System*, *supra* n23, p 64-65.

³⁹ *Ibid.* p 73.

⁴⁰ C Hood, *The Government of Risk*, *supra* n7 pp 148-9.

⁴¹ See also G Teubner, *Law as an Autopoietic System* (Oxford: Blackwell, 1993) Chapters 5 and 6.

⁴² See Ernst & Young, “Global Information Security Survey” 2005

http://www.ey.nl/download/publicatie/Global_Information_Security_Survey_2005.pdf, PWC “The State of Information Security” Survey

[http://www.pwc.com/extweb/pwcpublications.nsf/docid/3929AC0E90BDB001852571ED0071630B/\\$file/2006CIOPWC_GISS_web.pdf](http://www.pwc.com/extweb/pwcpublications.nsf/docid/3929AC0E90BDB001852571ED0071630B/$file/2006CIOPWC_GISS_web.pdf)

⁴³ See http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

£20 billion.⁴⁴ In the United States, the 2007 'State of the Net' survey conducted by the Consumer Reports National Research Center estimated that consumers lost more than \$ 7 billion during the past 2 years to online security threats.⁴⁵ The US Federal IT security spending is estimated to reach \$6 billion by 2008. One reason why information insecurity is increasingly defying easy prescriptions stems from the fact that the space of flows in the Internet have been leveraged by serious organised criminals to exploit flaws in information communication system to steal financial data, infect computers and blackmail businesses and companies with an online presence.⁴⁶ The UK government has, like most economies seeking to promote a secure environment for electronic commerce, enacted laws which characterize acts like hacking, dissemination of viruses into the digital environment and harm caused through misuse of computers as giving rise to criminal sanctions. Compliance and enforcement issues may also provide another explanation for the growing online security threats. Price Waterhouse Coopers draw attention in their 2006 survey on global information security to the increased information security budgets and concern that many companies were not complying fully with privacy and security laws both nationally and internationally.⁴⁷ In addition to laws criminalising computer misuse, the scope of governance measures has now embraces judicial, statutory and international rule making.⁴⁸ The principal US and EU/UK regulations include European Directive on Personal Data Protection, the Computer Misuse Act 1990 (as amended), the Fraud Act 2006 the US Computer Fraud and Abuse Act, Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act and the Federal Information Security Management Act.⁴⁹ Before looking at the significance of Luhmann's theorising for the increasing coupling of the political, legal and economic systems a brief observation needs to be made about the notion that the World Wide Web can be seen as a self-organised system.

⁴⁴ Serious Organised Crime Agency, *United Kingdom Threat Assessment 2006/2007*, paras 2.1, 2.39 - 2.40 Available at

http://www.soca.gov.uk/assessPublications/downloads/threat_assess_unclass_250706.pdf

⁴⁵ http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07/state-of-the-net/0709_state_net.htm (accessed, 7 August, 2007).

⁴⁶ Ibid.

⁴⁷ PWC "The State of Information Security" Survey

[http://www.pwc.com/extweb/pwcpublishings.nsf/docid/3929AC0E90BDB001852571ED0071630B/\\$file/2006CIOPWC_GISS_web.pdf](http://www.pwc.com/extweb/pwcpublishings.nsf/docid/3929AC0E90BDB001852571ED0071630B/$file/2006CIOPWC_GISS_web.pdf). See also the 2005 Survey by Ernst & Young at Ernst & Young,

"Global Information Security Survey" 2005

http://www.ey.nl/download/publicatie/Global_Information_Security_Survey_2005.pdf.

⁴⁸ See T Smedinghoff, "Where We Are Headed: New Developments and Trends in the Law of Information Security" (November 2006). Available at

<http://www.wildman.com/index.cfm?fa=news.pubArticle&aid=5072F372-BDB9-4A10-554DF441B19981D7> (accessed 1 June, 2007) and Final Report of the FTC Advisory Committee on

Online Access and Security, May 15, 2000, available at

<http://www.ftc.gov/acoas/papers/finalreport.htm> (accessed 15 May, 2007), Prepared Statement of the Federal Trade Commission before the Subcommittee on Technology, Information Policy,

Intergovernmental Relations, and the Census, Committee on Government Reform, U.S. House of Representatives on "Protecting Our Nation's Cyberspace," April 21, 2004, available at

<http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf> (accessed 15 May, 2007).

⁴⁹ Directive 2002/20/EC of the European Parliament and of the Council on the authorization of electronic communications networks and services, Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities, Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal service and users' rights relating to electronic communications networks and services, COM 96/C329/01: "European Union Council Resolution COM 96/C329/01 of 17 January 1995 on the Lawful Interception of Telecommunications", Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

2. The World Wide Web as a Self-Organised System?

Are DoS attacks like the World Wide Web systems separate from social systems?⁵⁰ To put it another way, is the Internet an environment that requires specialised laws?⁵¹ These questions continue form much of the staple diet when attention turns to governance on the Internet. The codes and programs in DoS attacks give the appearance of behaviours taking place in complex emergent networks. Spulber and Yoo, for example, argue that networks display complex behaviours, and use graph theory to propose an analytical framework that should inform policymakers to factor the complexities of emergent behaviour into regulatory decisions.⁵² There are some justifications to approaching governance in this manner. The technical infrastructure now enables asynchronous interactions in decentralised and distributed networks. The World Wide Web is a medium with complex transformative capacities. Benkler for example, conceives the networked information economy and the mass media has central to transformation of the relational dynamics between the State and individuals in society and the systems of politics and economics.⁵³ Three principal features are suggestive of the emerging relational dynamics in this space of flows: first, the transaction costs for information production, capture and transmission are minimal; second, the distributed network now makes possible new spaces for information flows; and third the exponential resources of the Internet now democratise and decentralises power.⁵⁴ We are said to be in the age of the information society. Our individual and collective identities are being processed and defined by electronic information networks.⁵⁵ The process of constructing the information society, the content and meaning we ascribe to it cannot be separated from the institutions, rules and norms that govern these activities.⁵⁶ New opportunities are being created for expression and the constitution of constituencies.⁵⁷ This new medium facilitates the formation of new communities, social, cultural, political and economic interaction. The

⁵⁰ See for example P Bøgh Andersen, "WWW as a Self-Organizing system", available at <http://imv.au.dk/~pba/Homepagematerial/publicationfolder/WWWSelfOrg.pdf>.

⁵¹ Joel R. Reidenberg, "Governing Networks and Rule-Making in Cyberspace", 45 Emory L. J. 912 (1996), Michael Froomkin, "The Internet as a Source of Regulatory Arbitrage" in B Kahin and C Nesson (eds) *Borders in Cyberspace* (Mass: MIT Press, 1997), Joel R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology", 76 Texas L. Rev. 553 (1998) Lawrence Lessig, "Foreword: Conference on Internet Privacy" 52 Stanford Law Review 987 (2000), Lawrence Lessig, "Code is Law, On liberty in Cyberspace", Harvard Magazine, January-February 2000 and D Spulber and S Yoo, "On the Regulation of Networks as Complex Systems", (2005) American Law & Economics Association Meetings Paper 38 <http://law.bepress.com/cgi/viewcontent.cgi?article=1107&context=alea>.

⁵² Ibid. Spulber and Yoo, *supra*.

⁵³ Y Benkler, *The Wealth of Networks* (New Haven: Yale UP, 2006) p212, David R. Johnson & David Post, *Law and Borders--The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367 (1996)

⁵⁴ M Castells, *The Internet Galaxy* (Oxford: OUP, 2001) p2

⁵⁵ See for example Manuel Castells, *The Rise of the Network Society* (Oxford: Blackwell, 2002) p7

⁵⁶ Ibid. at pp 7-8: "...the social construction of identity always takes place in a context marked by power relationships...a distinction [must be made] between three forms and origins of identity building: *Legitimizing identity*: introduced by the dominant institutions of society to extend and rationalize their domination *vis a vis* social actors, a theme that is at the heart of Sennet's theory of authority and domination, but also fits with various theories of nationalism. *Resistance identity*: generated by those actors that are in positions/conditions devalued and/or stigmatised by the logic of domination, thus building trenches of resistance and survival on the basis of principles different from, or opposed to, those permeating the institutions of society, as Calhoun proposes when explaining the emergence of identity politics. *Project identity*: when social actors, on the basis of whichever cultural materials are available to them, build a new identity that redefines their position in society and, by so doing, seek the transformation of overall social structure."

⁵⁷ See Bonnie A Nardi and Vicki L O'Day, *Information Ecologies* (Cambridge: MIT Press, 1997) and Karen Mossberger, Caroline J Tolbert and Mary Stansbury, *Virtual Inequality, Beyond the Digital Divide* (Washington: Georgetown UP, 2003).

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

expansion of the Internet, the growth of search engines, and web pages and emergence of complex systems and behaviour could be viewed as displaying (semi) autopoietic patterns.⁵⁸

The space of flows created in this environment has attracted the interests of scholars. Digitalisation of information and interconnectivity has for example been viewed as giving rise to a problem of appropriability,⁵⁹ the transformation of the relational dynamics between governments and civil society,⁶⁰ led to the emergence of public spheres of communication,⁶¹ and impacting the processes by which traditional markets have functioned.⁶² That said, it must not be overlooked that the Internet is ultimately a sophisticated medium for communication. As Capra observes:⁶³

“We are autonomous individuals, shaped by our own history of structural changes. We are self-aware, aware of our individual identity – and yet, when we look for an independent self within our world of experience we cannot find any such entity. The origin of our dilemma lies in our tendency to create the abstractions of separate objects, including a separate self, and then to believe that they belong to an objective, independently existing reality. To overcome our Cartesian anxiety, we need to think systematically, shifting our conceptual focus from objects to relationships. Only then can we realize that identity, individuality, and autonomy do not imply separateness and independence.”

In his polemic study of the network society, Castells draws on some basic ideas of systems theory in his use of the metaphor of the space of flows to describe the emerging organisational logic that is not dependent on functional and centralised hierarchical systems of ordering and control as such.⁶⁴ Interconnectivity is enabling a new system of communication that enables non-state actors and individuals to transform information into meaningful communications.⁶⁵ Castells does not however dissent from the view that the Internet is a medium populated by interdependent social actors as embodied in the:⁶⁶

“...flows of capital, flows of information, flows of technology, flows of organizational interaction, flows of images, sounds, and symbols. Flows are not just one element of the social organization: they are the expression of processes, *dominating* our economic, political, and symbolic life. If such is the case, the material support of the dominant processes in our societies will be the ensemble of elements supporting such flows, and making materially possible their articulation in simultaneous time. Thus, I propose the idea that there is a new spatial form characteristic of social practices that dominate and shape the network society: the space of flows. *The space of flows is the material organization of time-sharing social practices that work through flows.* By flows I understand purposeful, repetitive, programmable sequences of exchange and interaction between physically disjointed positions held by social actors in the economic, political, and symbolic structures of society.”

3. Information Security Law: A Reflexive Security Space?

⁵⁸ P Bøgh Anderson, “WWW As a Self-Organising System”

<http://imv.au.dk/~pba/Homepagematerial/publicationfolder/WWWSelfOrg.pdf>

⁵⁹ F Abbott, Patents, Data Protection and Global Information Flow in the Field of Medicines: Power, the Stratification of Wealth and the Consequences for Access and Public Health
<http://islandia.law.yale.edu/isp/GlobalFlow/paper/Abbott.pdf>

⁶⁰ D Drezner, “Weighing the Scales: The Internet’s Effect on State-Society Relations”
<http://islandia.law.yale.edu/isp/GlobalFlow/paper/Drezner.pdf>

⁶¹ V Mosco Politics and Policies in a Networked World: A Perspective from Canada”,
<http://islandia.law.yale.edu/isp/GlobalFlow/paper/Mosco.pdf>

⁶² R Cawley, “Information, Markets, Uncertainty and the Internet”
<http://islandia.law.yale.edu/isp/GlobalFlow/paper/Cawley.pdf>

⁶³ F Capra, *The Web of Life* (London: Flamingo, 1997) p287

⁶⁴ M Castells, *The Rise of the Network Society*, *supra* n55.

⁶⁵ M Castells, *The Rise of the Network Society*, *supra* n55, p 405.

⁶⁶ M Castells, *The Rise of the Network Society*, *supra* n55, p 442.

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

If one accepts Luhmann's analysis, we could make the following tentative observations. First, it would be misleading, if not inaccurate to conceive the function of law as being to create an "information security space" or "an information security commons".⁶⁷ It is society that generates an information security space. Order is constituted through complex differentiated structures and processes. Centralised institutions like law and politics constitute only a part (albeit an important one) of societal communications. Framing governance as comprising of aggregated and interdependent communications has immediate relevance for the heuristic value in the code metaphor as deployed by Lessig.⁶⁸ Lessig suggests that those who object to the new regulator fail to recognise that viewing governance or law through the metaphor of code can shed new insights on the relational dynamics between the State and society on the one hand and the interactions between law, markets, code and norms on the other.⁶⁹ This is true but there is nothing in the four modalities that foreclose attempts, which emphasises the critical role of multiple actors, and systems in the ordering activities of the social system. To be sure it is the processes of internal differentiation and structural coupling which determines the way society defines the way code is use (and not vice versa).⁷⁰ Another way of highlighting the limits in the 'code is law' thesis is that it can be seen as a static representation of the Hobbesian Leviathan in another guise.

We can briefly frame the Computer Misuse Act 1990 using the systems perspective. What we regard as being the shortcomings of the ordering role of the Act, and in turn, the limitations on the centralized system constructed by political and legal systems can be traced back to the unity of these systems and their capacity for functional differentiation. Theoretical justifications of the role of the State and the criminal law conform very much with our normative understandings of legitimacy, accountability and efficiency. These understanding reach deeply into public psyche regarding the role of political and legal systems in managing DoS attacks.⁷¹ One of the goals of governments is to reflect and be seen to address public concerns about the state of insecurity in the online environment.⁷² Criminal law theorising emphasises the critical role of the State in ordering behaviour.⁷³ The State's monopoly of the coercive machinery and deprivation of individual liberty, has long been seen as its prerogative.⁷⁴ The function of the political system can be seen as institutionalising the processes through which two public policy goals can be realised.⁷⁵ First, to reduce the threats and vulnerabilities faced by network systems and infrastructures to a manageable level. Second, to promote responsible computer use behaviour. For example, section 3 of the Computer Misuse Act 1990 defines the norms of acceptable behaviour. Individuals found to have violated the statutory code will be prosecuted in courts and subjected to penal sanctions when the legal and evidentiary burdens are discharged. This is perhaps an example of the

⁶⁷ The issue of whether the law is reflexive as argued by Teubner will not be addressed here.

⁶⁸ L Lessig, *Code: Version 2.0* (New York: Basic Books, 2006) p 5.

⁶⁹ Ibid. D Post, "What Larry Doesn't Get: Code, Law and Liberty in Cyberspace" *Stanford Law Review*, Vol 52 1439 (2000).

⁷⁰ See for example W Fisher III, *Promises To Keep: Technology, Law and The Future of Entertainment* (Stanford Law and Politics, 2004).

⁷¹ Better Regulation Commission, *Risk Responsibility and Regulation – Whose risk is it anyway?* Available at http://www.brc.gov.uk/upload/assets/www.brc.gov.uk/risk_res_reg.pdf.

⁷² S Brenner and J Schwerha IV "Transnational Evidence-Gathering and Local Prosecution of International Cybercrime" (2002) 20 *John Marshall Journal of Computer and Information Law* 347.

⁷³ A Ogus, *Regulation – Legal Form and Economic Theory* (Oxford: OUP, 1994), R Baldwin C Scott and C Hood, *A Reader on Regulation* (Oxford: OUP, 1998)

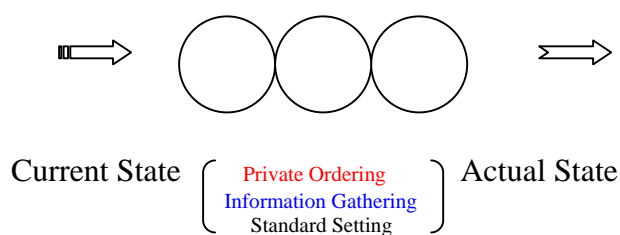
⁷⁴ See A Ashworth (citation needed) M Brake and C Hale, *Public Order and Private Lives: The Politics of Law and Order*. London: Routledge, 1992), J Braithwaite (1999) 'A Future Where Punishment Is Marginalised: Realistic or Utopian?', *UCLA Law Review* 46(4): 1727–50

⁷⁵ AP Simester and GR Sullivan, *Criminal Law: Theory and Doctrine* (Oxford: Hart, 2000) pp 1-17.

The term computer integrity is used to denote those activities that compromise the integrity of computer and network systems: see in particular I Walden, "Computer Crime" in C Reed and J Angel (ed) *Computer Law* (Oxford: OUP, 5th ed, 2003) pp 295-296.

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

coupling of political, legal and psyche systems. Functional differentiation can also be seen in the role of the legal system in defining when behaviour comes within the classification of legal/illegal acts. The key idea of functionally differentiated autopoietic systems like the legal system, and in particular the criminal law is that they are operationally closed in the sense that what constitutes a legal or illegal act is a matter to be resolved by the law. Functional differentiation is a double-edged sword. On the one hand, society is the legal environment and looks to law to transform communications into meanings that individuals and organisations can process. It is also the courts that determine the legal and evidentiary rules in the light of the amendment to section 3 of the Computer Misuse Act 1990. There is now no requirement for prosecution to show that the DoS attack caused an ‘unauthorised modification’ of the contents of the victim’s computer. With respect to the *actus reus* it is no longer necessary for the D to make an unauthorised modification to the contents of any computer. D will now be liable where he does an unauthorised act in relation to any computer whether requisite *mens rea* is present or not. The juridical process can be said to transform the “political” communication into recognisable rules and norms so that the evidence can be interpreted through the legal code. The legal system structures and defines the applicable principles, the definitional reach and the content of the legislation. The creation of an environment that provides a context for the legal system is critical to asserting the symbolic value of the criminal law and the importance the State attaches to order and security. The process of structural coupling ensures that the legal and political systems do not operate in isolation. Structural coupling allows the law to re-code political and by proxy societal concerns into its structures and processes. On the other hand, the legal system does not “communicate” or interact *with* its environment. This is an important constraint on the legal system. Law does not involve itself with enforcement – unless and when the DoS attacker has been apprehended. New and information communication technologies have also meant that there is a “time lag” that now determines law’s ability to respond to the problems posed by information security threats. A systems perspective suggest that knowledge is not static or given but is constantly being reproduced and created through interactions. Legal and political systems are not synchronised with the pace with which other entities and systems self-organise and self-reproduce. Or for that matter communications from DoS attackers that reject rules, norms and values established by the legal and political systems.



The ability of the legal and political system’s to respond to the perturbations caused by DoS is limited by this time lag. First, the system’s current state is defined by its structures and interacting components which are necessary to maintain its identity and autonomy. Perturbations from the environment lead to the system assessing its operations with a view to reaching its desired state. Second, the desired state is reached through the evolution of its internal dynamics. These features explain the somewhat functional-problem solving capabilities of legal and political systems and underscore the view that the perception of a “right answer” may conceal a more complex social reality. Accordingly, if order cannot be

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

found through the activities of law or politics, the market or organisations may provide a possible venue for responding to the perturbations.⁷⁶

4. Policy Implications

We can integrate Luhmann's view of society as a system of communications into the broader governance debates.⁷⁷ Questions about designing optimal regulatory infrastructures, the constitutional dimensions of regulation in cyberspace, or the role of software in private ordering have been the subject of governance debates in the age of post modernity.⁷⁸ Issues about the reactive nature of law or the problems associated with securing compliance reflect an ongoing concern about the role of law and the State in ordering society. Information and communication technologies now connect political, legal, economic sub-systems at different levels of intensity.⁷⁹ We can identify four features that define governance in the age of globalisation: mobility, interactivity, flexibility and relational structures. Communications in Luhmann's social system can be seen as integrative with recursive and self-organising attributes that reflect complex internally and functionally differentiated component parts. This is not to say that there is now no role for political and legal systems. The point here is that these systems have their constraints and the systems cannot be used mechanistically – social actors are not cogs in the political and legal machinery.⁸⁰ It is instructive to observe the way Luhmann portrays the various entities and sub-systems as having the capacity to self-organise, adapt and utilize resources of the components to interact with others whilst retaining their identity and codes. It may be that we need to resist the intuitive appeal of legal liability rules, for example, in imposing liability on ISPs and software program manufacturers. Legal regulations may produce additional negative externalities – the regulation space must now accommodate the social and innovation aspects of new technologies.⁸¹ Assuming that we can target the intermediary, where botnets are used, we have the additional complications posed by jurisdiction and different laws governing liability. Additionally, even if these problems are overcome, as Coase reminds, parties will invariably find alternative instruments to avoid or minimize exposure to legal liability.

Luhmann's conception of society as an interdependent network of autonomous entities and systems is not dissimilar to peer-to-peer networks.⁸² Benkler observes that:⁸³
“We live in a technological context in which a tremendous amount of excess capacity of the basic building blocks of our information and communication infrastructure is widely deployed. The widely distributed and topologically diverse deployment of these resources makes them ideally suited for building redundant, survivable backup systems for our basic information and communications infrastructure. Harnessing this excess capacity to create such a survivable infrastructure will likely be done most effectively, not through improving the ability to price these resources, but through improving the conditions for social sharing and exchange of the excess capacity users own. If we invest our policy efforts in hardening our systems to attack instead of rendering them survivable, if we ignore in our institutional design choices the effects on price-based markets and enterprise organization, we will lose a

⁷⁶ See for example, the emerging security flaws identified in the Apple iPhone and the information gathering processes of White Hat hackers.

⁷⁷ See RAW Rhodes, “The New Governance: Governing Without Government.” (1996) Political Studies XLIV: 652–67.

⁷⁸ See as an example the collection of essays in K Ladeur (eds), *Public Governance in the Age of Globalization* (Aldershot: Ashgate, 2004).

⁷⁹ AL Barabasi, *Linked: The New Science of Networks* (Cambridge, MA: Perseus, 2002), WR Ashby, *An Introduction to Cybernetics* (London: Chapman & Hill, 1956)

⁸⁰ J Zittrain, “The Generative Internet” Harvard Law Review, Vol. 119, p 1974, May 2006.

⁸¹ J Zittrain, “A History of Online Gatekeeping”, Harvard Journal of Law and Technology, Vol. 19, No. 2, p 253, 2006.

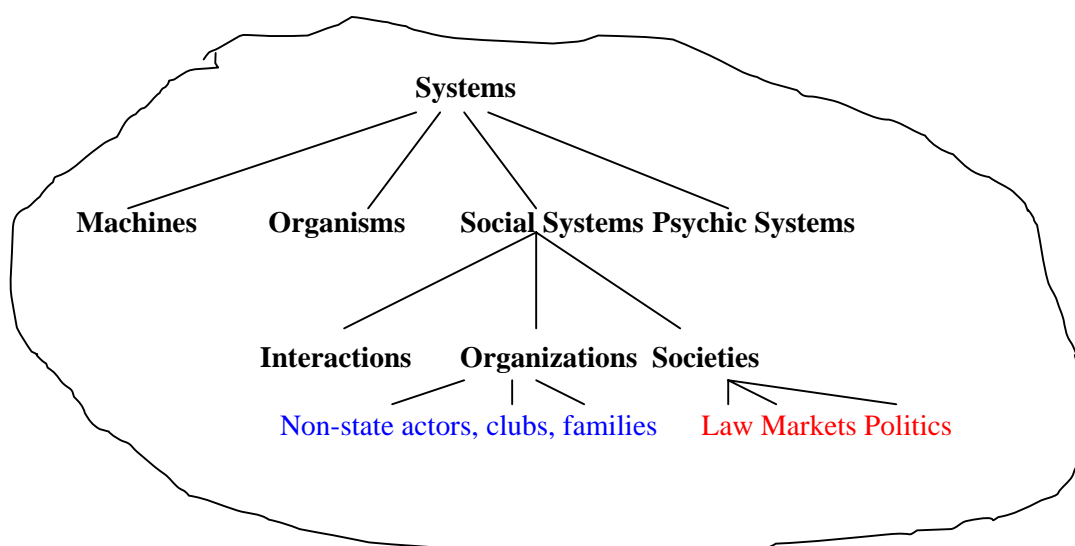
⁸² Y Benkler, “Peer Production of Survivable Critical Infrastructures” in F Paris 73, 74

⁸³ Ibid p 75

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

significant opportunity to improve the survivability of our information systems at relatively low cost and with minimal bureaucratic intervention.”

Like Benkler we can imagine the governance challenge in terms of how best we can integrate functionally differentiated systems that now include mobile actors, which make available portals for resources and open up new forms of interaction and organisation which bridge time and space.



Information security is not merely a public law problem. It is true that the State will continue to be a primary actor in this context.⁸⁴ It is however not the sole actor in the policymaking and decision making process. Globalisation and the Internet has merely expanded the policymaking and decision making process to include a wider range of actors in the public sphere.⁸⁵ Governance in the Internet is now transforming into a mediated concept embracing horizontal interactions and norm compliant systems, which focus on harnessing common interests and values. These developments now alter the orthodox dynamics through which information security risks have been traditionally conceived. Managing risks and uncertainty therefore need not be conceived in terms of the command and control hierarchy but more in terms of evolving polycentric and distributed networks. There is some evidence that the actors in the social system are leveraging information resources and developing internally differentiated structures. Increasingly, communications in the form of exchanges involving standard setting protocols, codes of practice, compliance and self-regulatory procedures being used to complement legal and political objectives. Non-state actors like ENISA, the ITU, CERT, ISPs and security service providers are now attempting to respond to the perturbations of their respective environments. Some of these perturbations may be due to the constraints faced by the legal system, others correspond to the increasing trend in using legal regulations

⁸⁴ See Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services.

⁸⁵ C Scott, “Regulation in the age of governance: the rise of the post-regulatory state”, in J Jordana and D D Levi-Faur (eds) *The Politics of Regulation* (Cheltenham: Edward Elgar, 2004) p145, 157-161

Draft Paper v.2: The Computer Misuse Act 1990 and Denial of Service Attacks: The Risk Society, Reflexivity and the Tragedy of the Security Commons

to increase corporate and business compliance, and the information gathering role of feedback loops from the market with regard to information security products and services.⁸⁶ Standard setting is a much under emphasised aspect of governance. In contrast to the coercive and reactive machinery of the law, standard setting provides an invaluable instrument through which a variety of social actors can internalize Internet security practices and norms.⁸⁷ It is flexible and can enable organisations to integrate the standards that correspond with their respective needs.⁸⁸ The ISO/IEC 27002: 2005 is a code of practice published by the International Organisation for Standardization.⁸⁹ The information security standard sets out the key information security principles and guidelines, the processes for risk assessment and management relating to access controls, human resources security, physical and geographical security, incident reporting, compliance organisation and asset management.⁹⁰ ISO/IEC 27001 can be used in conjunction with 27002.⁹¹ These standardization protocols enable organisations to implement risk management practices and undertake audits.⁹² Increasingly non-State actors are participating in the information security governance process. For example, the International Telecommunications Union (ITU) has been at the forefront of promoting transparency in the standardization process.⁹³ Communications relating to security standards in telecommunication networks are now made available to organisations. Following the second phase of the World Summit on the Information Society (WSIS) in Tunis in 2005, the ITU acts as moderator of the WSIS Action Line C5 on building trust and security in the use of information and communication technologies.⁹⁴ The European Telecommunications Standards Institute (ETSI) is another independent, non-profit organization, which continues to contribute to the creation of a culture of information security by developing telecommunications standards for technologies, which include telecommunications, broadcasting, intelligent transportation and medical electronics. The European Network and Information Security Agency, is another agency, which has directed its efforts in preventing, addressing and responding to information security issues.⁹⁵ Finally, the Convention on Cybercrime of the Council of Europe now makes available a binding international instrument on this particular subject. This Convention provides a guideline, which countries can use to develop national legislation against Cybercrime and as a framework for international cooperation.⁹⁶ All these developments underscore the need for a research agenda that focuses on how national and international organisations, companies and other entities, now process, adapt and evolve structures that reflect the complex information security landscape. The early indications are that these new systems are providing avenues for structural coupling and sharing of knowledge and expertise.⁹⁷

⁸⁶ A Google search for “information security products” revealed over 29 million hits.

⁸⁷ N Luhmann, “Differentiation of Society” *Canadian Journal of Sociology* (1977) 2(1) pp 29-53, N Luhmann, “Systems as Difference” *Organization* (2006) 13 p 37

⁸⁸ <http://www.iso.org/iso/en/ISOOnline.frontpage>

⁸⁹ This standard was previously known as ISO/IEC 17799.

⁹⁰ <http://www.iso.org/iso/en/aboutiso/introduction/index.html>

⁹¹ http://en.wikipedia.org/wiki/ISO/IEC_27001

⁹² <http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf>

⁹³ <http://www.itu.int/osg/csd/>

⁹⁴ See WSIS Action Line C5 and the Partnerships for Global Cybersecurity initiative can be found at www.itu.int/pgc/, ITU Plenipotentiary Resolution 130: “Strengthening the role of ITU in building confidence and security in the use of information and communication technologies” (Antalya, 2006)

<http://www.itu.int/osg/spu/cybersecurity/pgc/2007/docs/security-related-extracts-pp-06.pdf>

<http://www.itu.int/cybersecurity/>

⁹⁵ http://www.enisa.europa.eu/tmra/h_home.html

⁹⁶ <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG>

⁹⁷ See ETSI, 2nd Security Workshop: Future Security 16-17 January 2007 - Sophia-Antipolis, France Workshop Report

http://portal.etsi.org/securityworkshop/Presentations07/ETSI_2nd_Security_Workshop_Report.pdf

VI. Conclusion

Three observations can now be offered. First, viewing society as a complex aggregate of systems that exhibit characteristics of operational closure and open cognitive processes is particularly relevant as States now find that power is decentralised and distributed. Second, as individuals can now belong in different subsystems (organisations) it becomes incumbent to discover the resource potential that subsists in these multifaceted relationships. Third, Luhmann's reference to systems exhibiting functionally differentiated structures is central to the project of re-thinking issues about identifying and sustaining functional equivalents. For example, private ordering can be achieved through the organisation and structures of each sub system. Luhmann's focus on communications and use of systems perspectives provides us with one avenue through which we can understand the complexities of social systems and the processes and structures for transforming chaos into order. It is not possible to understand the complexities of information security governance through the juridical or centralized hierarchical frameworks. This paper has proposed an alternative perspective that aims to deepen our understanding of why it is that we are now witnessing the emergence of cooperative and heterarchical behaviour in society in the wake of growing information security threats. Luhmann's thesis is by no means comprehensive or beyond criticism. This paper has not delved into the shortcomings in his methodology. It has instead attempted to understand, why despite our best endeavors, the law appears to be ill equipped in the face of growing online threats. Luhmann provides us with some insights. By viewing society as being constituted by communications, we may perhaps temper our expectations of what "answers" law can give, or for that matter, what politics and economics can deliver. Luhmann reminds that managing complexity is not only an interactive process but it is also an evolutionary one.