Socio-Technical Systems

Brian Whitworth
New Jersey Institute of Technology, USA

INTRODUCTION

System Levels

Computer systems have long been seen as more than just mechanical systems (Boulding, 1956). They seem to be systems in a general sense (Churchman, 1979), with system elements, like a boundary, common to other systems (Whitworth & Zaic, 2003). A computer system of chips and circuits is also a software system of information exchanges. Today, the system is also the human-computer combination (Alter, 1999); for example, a plane is mechanical, its computer controls are informational, but the plane plus pilot is also a system: a human-computer system. Human-computer interaction (HCI) sees computers as more than just technology (hardware and software). Computing has reinvented itself each decade or so, from hardware in the 1950s and 1960s, to commercial information processors in the 1970s, to personal computers in the 1980s, to computers as communication tools in the 1990s. At each stage, system performance increased. This decade seems to be that of social computing, in which software serves not just people but society, and systems like e-mail, chat rooms, and bulletin boards have a social level. Human-factors research has expanded from computer usability (individual), to computer-mediated communication (largely dyads), to virtual communities (social groups). The infrastructure is technology, but the overall system is personal and social, with all that implies. Do social systems mediated by technology differ from those mediated by the natural world? The means of interaction, a computer network, is virtual, but the people involved are real. One can be as upset by an e-mail as by a letter. Online and physical communities have a different architectural base, but the social level is still people communicating with people. This suggests computer-mediated communities operate by the same principles as physical communities; that is, virtual society is still a society, and friendships cross seamlessly from face-to-face to e-mail interaction.

Table 1 suggests four computer system levels, matching the idea of an information system as hardware, software, people, and business processes (Alter, 2001). Social-technical systems arise when cognitive and social interaction is mediated by information technology rather than the natural world.

BACKGROUND

The Social-Technical Gap

The levels of Table 1 are not different systems, but overlapping views of the same system. Higher levels depend on lower levels, so lower level failure implies failure at all levels above it; for example, if the hardware fails, the software does too as does the user interface. Higher levels are more efficient ways of operating the system as well as observing it. For example, social systems can generate enormous productivity. For this to occur, system design must recognize higher system-level needs. For example, usability drops when software design contradicts users' cognitive needs.

Table 1. Information system levels

Level	Examples	Discipline
Social	Norms, culture, laws, zeitgeist, sanctions, roles	Sociology
Cognitive	Semantics, attitudes, beliefs, opinions, ideas, morals	Psychology
Information	Software programs, data, bandwidth, memory, processing	Computing
Mechanical	Hardware, computer, telephone, fax, physical space	Engineering

In physical society, architecture normally fits social norms; for example, you may not legally enter my house, and I can physically lock you out. In cyberspace, the architecture of interaction is the computer code that "makes cyberspace as it is" (Lessig, 2000). If this architecture ignores social requirements, there is a social-technical gap between what computers do and what society wants (Figure 1). This seems a major problem facing social software today (Ackerman, 2000). Value-centered computing counters this gap by making software more social (Preece, 2000).

Antisocial Interaction

Social evolution involves specialization and cooperation on a larger and larger scale (Diamond, 1998). Villages became towns, then cities and metropolitan centers. The roving bands of 40,000 years ago formed tribes, chiefdoms, nation states, and megastates like Europe and the United States. Driving this evolution are the larger synergies that larger societies allow. The Internet offers the largest society of all—global humanity—and potentially enormous synergies. To realize this social potential, software designers may need to recognize how societies generate *nonzero-sum gains* (Wright, 2001). While nonzero sum is an unpleasant term, Wright's argument that increasing the shared social pie is the key to social prosperity is strong. The logic that society can benefit everyone seems simple, yet communities have taken thousands of years to stabilize nonzero-sum benefits. Obviously, there is some resistance to social synergy.

If social interactions are classified by the expected outcome for the self and others (Table 2), situations where individuals gain at others' expense are antisocial. Most illegal acts, like stealing, fall into this category. The equilibrium of antisocial interaction is that all parties defect when nonzero-sum gains are lost. Antisocial acts destabilize the nonzero-sum gains of society, so to prosper, society must reduce antisocial acts. This applies equally to online society. Users see an Internet filled with pop-up ads, spam, pornography, viruses, phishing, spoofs, spyware, browser hijacks, scams, and identity theft. These can be forgiven by seeing the Internet as an uncivilized place, a stone-age culture built on space-age technology, inhabited by the "hunter-gatherers of the information age" (Meyrowitz, 1985, p. 315). This is the "dark side" of the Internet, a worldwide "tangled web" for the unwary (Power, 2000), a superhighway of misinformation, a social dystopia beyond laws where antisocial acts reign.

Figure 1. Social-technical gap

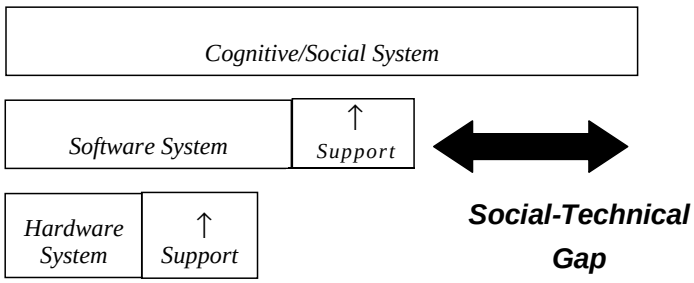


Table 2. Expected interaction outcomes

Other(s)→ Self ↓	Gain	Minor Effect	Loss
Gain	*Synergy*	*Opportunity*	*Antisocial*
Minor Effect	*Service*	*Null*	*Malice*
Loss	*Sacrifice*	*Suicide*	*Conflict*

Users are naturally wary of such a society; that is, they do not trust it. Trust has been defined as expecting that another's action will be beneficial rather than detrimental (Creed & Miles, 1996). Antisocial acts, by definition, do not create trust. Lack of trust reduces interaction, especially if there is a less risky alternative. For example, while electronic commerce is a billion-dollar industry, it has consistently performed below expectations, though in online trade sellers reduce costs and buyers gain choice at a lower price. E-commerce benefits both customers and companies, so why is it not the majority of trade? Every day millions of customers who want to buy things browse thousands of Web sites for products and services, yet the majority purchase from brick-and-mortar, not online, sources (Salam, Rao, & Pegels, 2003). If online society does not prevent antisocial acts, users will not trust it, and if they do not trust it, they will use it less.

In the tragedy of the commons, acts that benefit individuals harm the social group, whose loss affects the individuals in it (Poundstone, 1992). If farmers graze a common grass area, a valuable common resource is destroyed (from overgrazing), yet if one farmer does not graze, another will. The tragedy occurs if individual economics drives the group to destroy a useful common resource. Most animal species are barely able to cross this individual-gain barrier to social synergy. Only insect colonies compare to humans in size, but each community is one genetic family, allowing selection for cooperative behavior (Ridley, 1996). Humanity has created social benefits without genetic selection. How did we cross the zero-sum barrier? The answer seems to be our ability to develop social systems.

If the commons farmers form a village, it makes no sense for the village to destroy its own resource. If the village social system, of norms, rules, and sanctions, can stop individuals from overgrazing, the village keeps its commons and the benefits thereof. If only the village chief grazes the commons, there is an inherent instability between individual and community gain. However, if the commons is shared, say by a grazing roster, both village and members benefit. As society has evolved, bigger communities have produced more but also shared more. Social systems that spread social benefits fairly seem to stabilize nonzero-sum benefits better than those in which society's benefits accrue only to a few. The social concept of fairness seems to reconcile the conflict between private benefit and public good.

LEGITIMATE INTERACTION: A SOCIAL REQUIREMENT

The fact that social systems of law and justice are primarily about reducing unfairness in society (Rawls, 2001) is necessary because in society, one person's failure can cause another's loss, and one person's contribution can be another's gain, for example, in software piracy. One way to reduce antisocial acts is to make people accountable for the effects of their acts not just on themselves but also on others. Without such accountability, perceptions of unfairness arise, for example, when people take benefits others earned, or pay no price for harming others. Unfairness is not just the unequal distribution of outcomes, but the failure to distribute outcomes according to action contributions. Studies suggest people react strongly to unfairness, tend to avoid unfair situations (Adams, 1965), and even prefer fairness to personal benefit (Lind & Tyler, 1988). This natural justice perception seems to underlie our ability to form positive societies. Progress in legitimate rights seems to correlate with social wealth, as does social corruption with community poverty (Eigen, 2003). Perhaps people in fair societies contribute more work, ideas, and research because others do not steal it, or self-regulate more, which reduces security costs. Either way, accountability (or justice) seems a requirement for social prosperity.

The social goal has been defined as legitimate interaction that is fair to individuals and beneficial to the social group (Whitworth & deMoor, 2003). Legitimacy is a complex social concept. Fairness alone does not define it as conflict can also be fair. A duel is a fair fight, but duels are still outlawed as being against society. Legitimate interaction includes public-good benefits as well as individual fairness. In sociology, the term legitimate applies to governments that are justified to their people, not coerced (Barker, 1990). It can mean having the sanction of law, but legitimacy is more than legality. Mill (1859/1995, p. 1) talks of the "limits of power that can be legitimately exercised by society over the individual." Jefferson wrote, "… the mass of

mankind has not been born with saddles on their backs, nor a favored few booted and spurred, ready to ride them legitimately…" (Somerville & Santoni, 1963, p. 246). Fukuyama (1992) argues that legitimate communities prosper, while those that ignore it do so at their peril. These statements have no meaning if legitimacy and legality are the same, as then no law-setting government could act illegitimately.

The social requirement of legitimacy complements that of security. Security ensures a system is used as intended, while legitimacy defines that intent. Whether a user is who he or she says (authentication) is a security issue. What rights he or she should have (authority) is a legitimacy issue. In generating trust and business, no amount of security can compensate for a lack of legitimacy. Dictatorships have powerful security forces, but their citizens distrust them, reducing social synergy. In prosperous modern societies, security is directed by legitimacy, and legitimacy depends on security.

Online Legitimacy

Physical society uses various means to prevent antisocial acts from destabilizing social benefits, including the following.

1. **Ethics:** Supports right acts by religion or custom
2. **Barriers:** Fences, doors, or locks to prevent unfair acts
3. **Revenge:** Individuals "pay back" those that cheat
4. **Norms:** Community laws, sanctions, and police

All have also been tried in cyberspace, with varying degrees of success.

Arguably the best means to legitimate interaction is to have moral, ethical people, who choose not to cheat. But while most agree altruism is good and selfishness bad, we often do not practice what we preach (Ridley, 1996). Will online society make people more ethical than physical society?

Barriers, like a locked door, can prevent unfairness, but any barrier raised can be overcome. Online security is a continual battle between those who create and those who cross barriers. Also, barriers can reduce as well as increase fairness. Do we really want a cyber society built on the model of medieval fortresses?

A third way to legitimate interaction is through revenge: to repay actions in kind, or cheat the cheaters (Boyd, 1992). In Axelrod's (1984) prisoner's dilemma tournament, the most successful program was TIT-FOR-TAT, which began cooperating, then copied whatever the other did. If people who are cheated today will take revenge tomorrow, cheating may not be worth it, but do we want cyber society run under a vigilante justice system?

A fourth way for society to support legitimate interaction is by norms and laws. If laws oppose antisocial acts, why not apply laws online? This approach is popular, but old means may fail in new system environments (Whitworth & deMoor, 2003). Laws assume a physical-world architecture so may not easily transfer to virtual worlds that work differently from the physical world (Burk, 2001). Legal processes may suffice for physical change, but while laws can take years to pass, the Internet can change in a month. New cases, like cookies, can arise faster than laws can be formed, like weeds growing faster than they are culled. Also, the programmers who define cyberspace can bypass any law. The Internet, once thought innately ungovernable, could easily become a system of perfect regulation and control (Lessig, 1999) as once software is written, issues of law may have already been decided. Finally, laws are limited by jurisdiction, as attempts to legislate telemarketers illustrate. U.S. law applies to U.S. soil, but cyberspace does not exist inside America. The many laws of many nations do not apply to a global Internet. For these reasons, the long arm of the law struggles to reach into cyberspace. The case is still out, but many are pessimistic. Traditional law seems too physical, too slow, too impotent, and too restricted for the challenge of a global information society.

FUTURE TRENDS

That the social needs of online society are not yet met suggests two things. First, Internet growth may be just beginning, and second, meeting social needs is the way to achieve that growth. Perhaps we are only seeing the start of a major human social evolu-

tion. We may be no more able to envisage a global information society than people in the middle ages could conceive today's global trade system. The differences are not just technical, like ships and airplanes, but also social, differences in how we interact. Traders today send millions of dollars to foreigners they have never seen for goods they have not touched to arrive at unknown times. Past traders would have seen that as mere folly, but today's market economy has social as well as technical support:

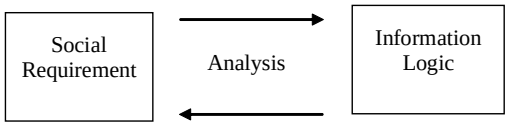
To participate in a market economy, to be willing to ship goods to distant destinations and to invest in projects that will come to fruition or pay dividends only in the future, requires confidence, the confidence that ownership is secure and payment dependable…knowing that if the other reneges, the state will step in… (Mandelbaum, 2002, p. 272)

Social benefits require the influence of social entities, like the state. Individual parties in an interaction are biased to their own benefit. Only a community can embody legitimate rules above individuals, yet these must be manifested as well as conceived. The concept of the state assumes physical boundaries that do not exist in cyberspace. For online society to flourish, the gap between social right and software might must be closed, but stretching physical law into cyberspace is problematic (Samuelson, 2003). Physical laws operate after the fact for practical reasons: To punish unfairness, it must first occur. Yet in cyberspace, we write the code that defines all interaction. It is as if we could write the laws of physics in the physical world. Hence, a new possibility arises. Why not focus on the solution (legitimacy) rather than the problem (unfairness)? Why let antisocial acts like spam develop, then try ineffectually to punish them when we can design for social fairness in the first place? When societies move from punishing unfairness to encouraging legitimacy, it is a major advance, from the laws of Moses or Hammurabai to visionary statements of social opportunity like the French Declaration of Human Rights or the United States constitution. Cyberspace is a chance to apply several thousand years of social learning to the global electronic village; designing social software in a social vacuum may condemn us to relearn the social lessons of physical history in cyberspace.

In physical society, it was the push for distributed ownership that created social rights; the original pursuers of rights were British elite seeking property rights from their King: "It was the protection of property that gave birth, historically, to political rights" (Mandelbaum, 2002, p. 271). Over time, the right to own was extended to all citizens, as giving today's freedoms proved profitable. Ownership as a concept can be applied online. Twenty years ago, issues of "Who owns the material entered in a group communication space?" (Hiltz & Turoff, 1993, p. 505) were raised. If information objects can be owned, a social property-rights framework can be applied to information systems (Rose, 2001). Analysing who owns what can translate social statements into IS specifications and vice versa (Whitworth & deMoor, 2003; Figure 2).

Future social-software designers may face questions of what should be done, not what can be done. There seems no reason why software should not support what society believes. If society believes people should be free, our Hotmail avatars should belong to us. If society gives a right not to communicate (Warren & Brandeis, 1890), we should be able to refuse spam (Whitworth & Whitworth, 2004). If society supports privacy, we should be able to remove personal data from online lists. If society gives creators rights to the fruits of their labors (Locke, 1963), we should be able to sign and own electronic items. If society believes in democracy, online bulletin boards should be able to elect their leaders. Such suggestions do not mean the mechanization of online interaction: Social rights do not work that way. Society grants people privacy, but does not force them to be private. Likewise, owning a bulletin-board item means you may delete it, not that you must delete it. Software support for social rights would allocate rights to act, not automate right acts, giving choice to people to not to program code.

Figure 2. Social-requirements analysis



CONCLUSION

The core Internet architecture was designed over 30 years ago to engineering requirements existing when a global electronic society was not even envisaged. It seems due for an overhaul to meet the social needs of virtual society. Architecture, whether physical or electronic, affects everything, and social systems require precisely such general changes. The marriage of society and technology needs respect on both sides. To close the social-technical gap, technologists cannot stand on the sidelines: They must help. System designers must recognize accepted social concepts, like freedom, privacy, and democracy, that is, specify social requirements as they do technical ones. Translating social requirements into technical specifications is a daunting task, but the alternative is an antisocial cyber society that is not a nice place to be. If human society is to expand into cyberspace, with all the benefits that implies, technology must support social requirements. The new user of social-technical software is society, and the user requirement of society is legitimate interaction.

REFERENCES

Ackerman, M. S. (2000). The intellectual challenge of CSCW: The gap between social requirements and technical feasibility. *Human Computer Interaction, 15*, 179-203.

Adams, J. S. (1965). Inequity in social exchange. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 2, pp. 267-299). New York: Academic Press.

Alberts, B., Bray, D., Lewis, J., Raff, M., Roberts, K., & Watson, J.D. (1994). *Molecular biology of the cell.* New York: Garland Publishing, Inc.

Alter, S. (1999). A general, yet useful theory of information systems. *Communications of the AIS, 1*, 13-60.

Alter, S. (2001). Which life cycle: Work system, information system, or software? *Communications of the AIS, 7*(17), 1-52.

Axelrod, R. (1984). *The evolution of cooperation.* New York: Basic Books.

Barker, R. (1990). *Political legitimacy and the state.* Oxford, UK: Oxford University Press.

Boulding, K. E. (1956). General systems theory: The skeleton of a science. *Management Science, 2*(3), 197-208.

Boyd, R. (1992). The evolution of reciprocity when conditions vary. In A. H. Harcourt & F. B. M. de Waal (Eds.), *Coalitions and alliances in humans and other animals* (473-492). Oxford, UK: Oxford University Press.

Burk, D. L. (2001). Copyrightable functions and patentable speech. *Communications of the ACM, 44*(2), 69-75.

Chung, L., Nixon, B. A., Yu, E., & Mylopoulos, J. (1999). *Non-functional requirements in software engineering.* Boston, MA: Kluwer Academic.

Churchman, C. W. (1979). *The systems approach.* New York: Dell Publishing.

Creed, W. E., & Miles, R. E. (1996). Trust in organizations: A conceptual framework linking organizational forms, managerial philosophies, and the opportunity costs of control. In R. M. Kramer, M. Roderick, & T. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 16-38). London: Sage.

Diamond, J. (1998). *Guns, germs and steel.* London: Vintage.

Eigen, P. (2003). *Transparency international corruption perceptions index 2003* [Speech]. London: Foreign Press Association. Retrieved from http://www.transparency.org/cpi/2003/cpi2003.pe_statement_en.html

Fukuyama, F. (1992). *The end of history and the last man.* New York: Avon Books Inc.

Goodwin, N. C. (1987, March). Functionality and usability. *Communications of the ACM,* 229-233.

Hiltz, S. R., & Turoff, M. (1993). *The network nation: Human communication via computer* (Rev. ed.). Cambridge, MA: MIT Press.

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

Lessig, L. (2000). Cyberspace's constitution. *Lecture given at the American Academy, Berlin, Germany.* Retrieved from http://cyber.law.harvard.edu/works/lessig/AmAcd1.pdf

Lind, E. A., & Tyler, T. R. (1988). *The social psychology of procedural justice.* New York: Plenum Press.

Locke, J. (1963). An essay concerning the true original extent and end of civil government. In J. Somerville & R. E. Santoni (Eds.), *Social and political philosophy: Readings from Plato to Ghandi* (chap. 5, section 27, pp. 169-204). New York: Anchor Books.

Mandelbaum, M. (2002). *The ideas that conquered the world.* New York: Public Affairs.

Meyrowitz, J. (1985). *No sense of place: The impact of electronic media on social behavior.* New York: Oxford University Press.

Mill, J. S. (1955). *On liberty.* Chicago: The Great Books Foundation. (Reprinted from 1859)

Poundstone, W. (1992). *Prisoner's dilemma.* New York: Doubleday, Anchor.

Power, R. (2000). *Tangled web: Tales of digital crime from the shadows of cyberspace.* Indianapolis, IN: QUE Corporation.

Preece, J. (2000). *Online communities: Designing usability, supporting sociability.* Chichester, UK: John Wiley & Sons.

Rawls, J. (2001). *Justice as fairness.* Cambridge, MA: Harvard University Press.

Ridley, M. (1996). *The origins of virtue: Human instincts and the evolution of cooperation.* New York: Penguin.

Rose, E. (2001, March). Balancing Internet marketing needs with consumer concerns: A property rights framework. *Computers and Society,* 17-21.

Salam, A. F., Rao, H. R., & Pegels, C. C. (2003). Consumer-perceived risk in e-commerce transactions. *CACM, 46*(12), 325-331.

Samuelson, P. (2003). Unsolicited communications as trespass. *Communications of the ACM, 46*(10), 15-20.

Sanders, M. S., & McCormick, E. J. (1993). *Human factors in engineering and design.* New York: McGraw-Hill.

Somerville, J., & Santoni, R. E. (1963). *Social and political philosophy: Readings from Plato to Ghandi.* New York: Anchor Books.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220.

Whitworth, B., & deMoor, A. (2003). Legitimate by design: Towards trusted virtual community environments. *Behaviour & Information Technology, 22*(1), 31-51.

Whitworth, B., & Whitworth, E. (2004, October). Reducing spam by closing the social-technical gap. *IEEE Computer,* 38-45.

Whitworth, B., & Zaic, M. (2003). The WOSP model: Balanced information system design and evaluation. *Communications of the Association for Information Systems, 12,* 258-282.

Wright, R. (2001). *Nonzero: The logic of human destiny.* New York: Vintage Books.

KEY TERMS

Avatar: An information object that represents a person in cyberspace, whether a Hotmail text ID or a graphical multimedia image in an online multiplayer game.

Information System: A general system that may include hardware, software, people, and business or community structures and processes (Alter, 1999, 2001), vs. a social-technical system, which must include all four levels.

Nonzero Sum: In zero-sum interaction, one party gains at another's expense so the parties compete. Negative acts that harm others but benefit the actor give an "equilibrium" point at which everyone defects and everyone loses (Poundstone, 1992). In contrast, in nonzero-sum interaction, parties co-

operate to increase the shared resource pie, so they gain more than they could have working alone: It is a win-win situation. The synergistic benefits of society seem based on nonzero-sum gains (Wright, 2001).

Social System: Physical society is not just mechanics nor is it just information, as without people information has no meaning. Yet it is also more than people. Countries with people of similar nature and abilities, like North and South Korea, or East and West Germany, performed differently as societies. As people come and go, we say the society continues. Jewish individuals of 2,000 years ago have died just as the Romans of that time, yet we say the Jews survived while the Romans did not. What survived was not buildings, information, or people, but a manner of interaction: their social system. A social system is a general form of human interaction that persists despite changes in individuals, communications, or architecture (Whitworth & deMoor, 2003) based on persistent common cognitions regarding ethics, social structures, roles, and norms.

System: A system must exist within a world and cannot exist if its world is undefined: No world means no system. Existence is a property a system derives from the world around it. The nature of a system is the nature of the world that contains it; for example, a physical world, a world of ideas, and a social world may contain physical systems, idea systems, and social systems, respectively. A system that exists still needs an identity to define what is a system and what is not a system. A system indistinguishable from its world is not a system; for example, a crystal of sugar that dissolves in water still has existence as sugar, but is no longer a separate macroscopic system. The point separating system from nonsystem is the system boundary. Existence and identity seem two basic requirements of any system.

System Elements: An advanced system has a boundary, an internal structure, environment effectors, and receptors (Whitworth & Zaic, 2003). Simple biological systems (cells) formed a cell-wall boundary and organelles for internal cell functions (Alberts et al., 1994). Simple cells like Giardia developed flagella to effect movement, and protozoa developed light-sensitive receptors. We ourselves, though more complex, still have a boundary (skin), an internal structure of organs, muscle effectors, and sense receptors. Computer systems have the same elements: a physical-case boundary, an internal architecture, printer and screen effectors, and keyboard and mouse receptors. These elements apply at different levels; for example, software systems have memory boundaries, internal program structures, specialized input analysers, and specialized output driver units.

System Environment: In a changing world, changes outside a system may cause changes within it, and changes within may cause changes without. A system's environment is that part of a world that can change the system or be affected by it. What succeeds in the system-environment interaction depends on the environment. In Darwinian evolution, the environment defines system performance. Three things seem relevant: opportunities, threats, and the rates by which these change. In an opportunistic environment, right action can give great benefit. In a risky environment, wrong action can give great loss. In a dynamic environment, risk and opportunity change quickly, giving turbulence (sudden risk) or luck (sudden opportunity). An environment can be of any combination, for example, opportunistic, risky, and dynamic.

System Levels: Is the physical world the only real world? Are physical systems the only possible systems? The term information system suggests otherwise. Philosophers propose idea systems in logical worlds. Sociologists propose social systems. Psychologists propose cognitive mental models. Software designers propose data entity relationship models quite apart from hardware. Software cannot exist without a hardware system of chips and circuits, but the software world of data records and files is not equivalent to the hardware world. It is a different system level. Initially, computer problems were mainly hardware problems, like overheating. Solving these led to software problems, like infinite loops. Informational requirements began to drive chip development, for example, network and database protocol needs. HCI added cognitive requirements to the mix. Usability demands are now part of engineering-requirements analysis (Sanders & McCormick, 1993) because Web sites fail if people reject them (Goodwin, 1987). Finally, a computer-mediated community can also be seen as a social

system. An information system can be conceived on four levels: mechanical, informational, cognitive, and social. Each emerges from the previous, not in some mystical way, but as a different framing of the same thing. For example, information derives from mechanics, human cognitions from information, and society from a sum of human cognitions (Whitworth & Zaic, 2003). If all levels derive from hardware, why not just use that perspective? Describing modern computers by chip and line events is possible but inefficient, like describing World War II in terms of atoms and electrons. As higher levels come into play, systems become more complex but also offer higher performance efficiencies.

System Performance: A traditional information system's performance is its functionality, but functions people cannot use do not add performance. If system performance is how successfully a system interacts with its environment, usability can join nonfunctional IS requirements, like security and reliability, as part of system performance. The four advanced system elements (boundary, internal structure, effectors, and receptors) can maximize opportunity or minimize risk in a system environment. A multidimensional approach to system performance, as suggested by Chung, Nixon, Yu, and Mylopoulos (1999), suggests eight general system goals applicable to modern software: functionality, usability, reliability, flexibility, security, extendibility, connectivity, and confidentiality (Whitworth & Zaic, 2003).