Risks of Computer-Related Technology

Dr. Peter G. Neumann, Principal Scientist, Computer Science Laboratory
SRI International, Menlo Park, California 94025-3494 USA
e-mail: Neumann@CSL.SRI.com Web: http://www.csl.sri.com/neumann

Working notes for ISODARCO, Trento, 9 August 2002

Abstract: This talk will address computer-related risks involving (among other topics) individual well-being and world stability, reliability, safety, security, and privacy, and what can be done to combat those risks. In many cases, much greater proactive effort is needed to reduce the risks. In some cases (as the computer observes in the movie War Games), "The only winning strategy is not to play." We will consider risks in defense (including proposed missile defense systems), aviation, space, control systems, communications systems, finance, health care, information systems generally, etc. For extensive background, seethe handout http://www.csl.sri.com/neumann/illustrative.html, and see www.risks.org

In light of the long-standing risks of system malfunctions as well as malicious or accidental system misuse, and impelled by the newly increased awareness of threats of terrorism, it seems natural for us to consider computer-related technologies and their relationships with social, political, economic, and environmental issues. The problems to be considered include system security, system reliability, human safety, system survivability, application integrity, privacy, and many other considerations.

In that almost everything we do is becoming dependent on computer technologies, for better or for worse, that means we need to covera lot of ground to understand what is at stake. Of greatest concern hereis that we focus on the big picture, without getting lost in the details.

There are numerous dimensions we could consider in what is actuallya highly multidimensional problem. Very briefly, some of the dimensionalalternatives that come to mind include

* Internationalism vs isolationism
* Multilateralism vs unilateralism
* Rule by agreement vs rule by force
* Partnerships vs nationalism
* Deregulation vs regulation
* Level economic playing fields vs corporation-dominated globalization
* Free markets vs controlled markets (including international cartels)
* Development of alternative energy sources vs dependence on fossilfuels

However, there are four other sets of alternatives that will be of particular concern to us here:

* Understanding the risks of the misuse of technology vs ignoring them
* More technology vs less technology for addressing social problems
* Open information vs secrecy
* Privacy vs surveillance
  [Unfortunately, the last two of these dimensions present some nasty conflicts with each other.]

Most of these dimensions are considered rather simplistically as black-and-white alternatives, sometimes between different ideologiesor between good and evil. Each of these seeming dichotomies is infact itself a broad range of options. In reality, things are generally notpurely black or white, and we must recognize many shades of gray. Attemptsto see everything from one extreme or another are likely to break down, andseem to reflect a serious lack of common sense. Typically, there areno easy answers. I frequently quote Albert Einstein, who said in conversation (although nowhere that I know of in any of his writings) that "Everything should be made as simple as possible, but no simpler." As a society,we tend to try to make things too simple.

So, let's consider how these four dimensions might apply to technology,and in particular to information technology?

[Understanding the risks of the misuse of technology vs ignoringthem]
[More technology vs less technology for particular problems]
[Open information vs secrecy]
[Privacy vs surveillance]

* Computer-communication technology. For many applications, weneed reliable, secure, highly available systems. For many critical applications, what we need is strength in depth. Whatwe have in practice is weakness in depth. Information systems and networksare riddled with vulnerabilities and weak links. Furthermore, the mass-marketmarketplace has failed miserably in producing robust systems, although itis wonderful at producing more fancy features. We should never assumethat the systems we depend on are invulnerable, or that the people who use andoperate them are infallible. We must learn to design systems much moredefensively

* The Internet. The Internet has opened up enormous new opportunities,for third-world development, world-wide commerce, education, rapidinformation flow, etc. However, the Internet has very little realresistance to coordinated attacks (although what we have seen thus far ismore or less child's play), and the systems attached to it tend to be highly vulnerable. Trojan horses, Viruses, worms, denial of serviceattacks, and

so on represent real threats -- primarily because of the absenceof robust system and network architectures. The beauty of the Internetis that it is truly international. However, the future of the Internetis seriously threatened by its lack of enlightened management, governmentdesires at control, corporate greed, and many other factors. VariousInternet task forces attempt to steer the technological evolution. TheInternet Corporation for Assigned Names and Numbers has a fairly narrowcharter, but even that has caused enormous controversy. A new organizationcalled People For Internet Responsibility (pfir.org) is attemptingto encourage more democratic and representative approaches that will ensurethat the Internet is truly for everyone, and not ruined by corporateinterests, purveyors of electronic junk mail (spam), swindlers, and soon, while at the same time not overly constrained by regulation.

* Our national and international critical infrastructures are riddledwith vulnerabilities, including those relating to security, reliability,system survivability, and human safety. This is true of telecommunications, electric power, water supplies, gas and oil distribution, transportation, and even government continuity. For example, see the reportof the U.S. President's Commission on Critical Infrastructure Protection,under Bill Clinton, which concluded that essentially everything is vulnerableto external and internal attacks and indeed to falling apart onits own even without attacks. Many of these risks have been known formany years, although very little has been done in the past.

* Privacy, secrecy, surveillance, monitoring, oversight, and who watchesthe watchers? Privacy problems are enormous, and widely ignored. The average person believes he or she has nothing to hide, so why is privacy important? The answers to that include identity theft,false information, monitoring, harassment, blackmail, targetted personal attacks,and many other problems. Independent oversight is absolutely essential. Anderson has become the poster child for mismanagement and lack of independent auditing at Enron, Waste Management, even more recently AOL-TimeWarner. The situation is much worse in computers. Even where independentaudit trails exist, they may be tampered with, or destroyed, or bypassed altogether. Although there are often opportunities toreconstruct audit data that has been deleted, there are also serious problemswith trying to rely on digital evidence, since the integrity of the evidentiaryprocess may be in doubt. If you have to rely on the integrityof a computer system to protect your information you are already in trouble,because security problems and privacy violations also involve peoplewho have access to or can penetrate databases. If you have to relyon people who are untrustworthy, all bets are off.

* Openness. There is a big debate within various communities asto whether secrecy can increase security. In a few cases, perhapsit can. But

assuming that you can avoid exploitation of serious securityflaws by pretending they do not exist is sheer folly. Besides,in the absence of knowledge about how vulnerable you are, you are unlikely totake remediative measures. Nevertheless, you would prefer thatyour adversaries do not know more than you do. This is a reallynasty problem. The debates over open-source versus closed-source proprietarysoftware are also important. Note that open-source software is by itselfnot the answer either. But hiding behind flawed proprietary softwareleads to the institutionalization of security by obscurity, which is inherentlya bad idea.

* The election process. One example that is not generally recognizedas particularly critical is our election process, which in a senseputs many of the previously discussed technological problems such as reliability, security, and privacy into a single context. Many warningshave been given over the past decades, but they have largely fallen ondeaf ears. The Florida experience is really just the tip of a huge iceberg. Registration: Tens of thousands of voters were disenfranchisedby bogus felony lists in Florida; up to 4 million votes were lost in2000, according to the Caltech/MIT study. There are huge risksin the integrity of your vote, the counting process, and the accountability ofthe entire process. Punched cards are clearly problematic. But all-electronic systems are enormously risky: in all of today's systems, thereis no real assurance that your vote as cast is counted correctly, and typicallyno accountability in case of an obvious fraud. The softwareis almost always proprietary, with the professed belief that this makes it moresecure. There are huge opportunities for fraud. In that true democracydepends critically on the integrity of the election process, the oldquote is highly relevant: "It's not who votes that counts, it's who countsthe votes."

The Illustrative Risks document on my Web site gives pages and pagesof cases involving computer-based failures in defense, space, aviation,other transportation, power, medical systems, control systems, the environment, finance, telecommunications, elections, law enforcement, and perhapsmost frustratingly, information security and privacy. My Web sitealso has
If you can't remember the
Web site, just search for Neumann at http://www.google.com.

Here are just a few examples from ILLUSTRATIVE RISKS and www.risks.org:

Commercial aviation problems.
Lauda Air 767 thrust reversal, Northwest Airlines flight 255 warning system not powered up, British Midland 737 wrong engine(right) shut off [right was wrong], Aeromexico crash near LAX pilotand controller errors, four Airbus A320 crashes, Air New Zealand

known wrong course data not fixed. The Russian plane recentlytold to
go up by the automated collision avoidance system, and to descendby
the Swiss air-traffic controller.
Military problems enormous, many not widely reported. Yorktowndead in
the water for almost three hours on application divide-by-zero.
Patriot clock drift. Vincennes Aegis. Black Hawkfriendly fire.
Handley-Page Victor aircraft tailplane flutter: (1) wind-tunnel model
error in wing stiffness and flutter, (2) rsonsance test erroneouslyfitted
to aerodynamic equations, (3) low-speed flight tests incorrectly
extrapolated ==> tailplane broke off in first flight test.
Control systems increasingly in trains, cars, ships, appliances, etc.
Muni metro door program: three failed door closings shut downentire Muni.
Numerous train wrecks due to human error, some hardware and softwareproblems
Exxon Valdez, Puget Sound Ferry system 1980s dock crashes, modernized
but the computerized Issaquah ferries were cut back to manualcontrols!
Medical applications: Therac 25 (Nancy Leveson's article and book).
Heart-monitor line plugged into power supply in Seattle Children's
Hospital, killing a 4-year-old girl 1986, similar case 7 yearslater
in Chicago. EMI on pacemakers and magnets acting on defibrillators.
London Ambulance Service fiasco. Healthcare databasesand hospital
control. Remote computer-controlled surgical operations. Smart cards for
personal medical profiles. Medical database privacy issuesin general.
The Y2K problem.

More and more systems are CRITICAL (e.g., SAFETY CRITICAL, SURVIVABILITY CRITICAL, etc.) as we increasingly computerize. And many newrisks, such as what will be introduced by voice-activated speech-understanding systems, subject to native dialects, foreign accents, malicious impersonators, bystanders. We need to learn more from experiences of ourselvesand others.

My Web site is full of material on how we could dramatically improvethe situation. However, I strongly believe that no solutions arelikely to work in the long run unless they are based on uncompromised human-oriented democratic principles. Everything we do is becoming interrelated, internationally. This is very obvious when we consider the WorldWide Web, the Internet, television, radio, and other media, whereby almost everyonein the civilized world is interconnected one way or another, almost instantaneously.

Perhaps ironically, cartoonists seem to be doing a good job of bringing reality to the public. For example, here's a quote from GeorgeOrwell that appeared in "The Boondocks" comic strip in the Sunday comics pagesof the *San Francisco Chronicle*, 30 Jan 2002:

"If liberty means anything at all, it means the
right to tell people what they do not want to hear."

Roles of Technology

We have a tendency to try to solve problems with inappropriate approaches. There are significant risks in attempting to use technological approachesto solve social problems, and similarly risks to using social/legal/economic solutions to solve technological problems. Beware of uses oftechnology that only appear to improve things.

Examples:

* Attempts to prevent terrorism through national missile defense, national identity cards, face scanning, and bombing caves. National IdentityCards may be seen as merely an extension of drivers' licenses, but thereare serious risks in the associated databases and infrastructures: identity theft, false arrests, untrustworthy insiders, and so on. Besides,such a card would probably not have prevented the September 11 terrorists, especially those who were masquerading as others but had what lookedlike legitimate identities. Face scanning generally gives huge falsepositive rates, and at the moment includes only a few dozen faces. Biometric authentication does have a place in hypercritically sensitive applications, but seems questionable in general. In general, we have the problemof putting a safe-like lock on the front door and leaving a side dooropen. But beware of putting too much faith in these technologies. Manyof the threats can bypass them.

* Attempts to control electronic borders such as telephones, faxes, television, radio, and the Internet: Singapore, China, Taliban, jammingof the Voice of America, etc.

* Attempts at censorship, for example, by attempting to reject certaintypes of information such as pornography through simple-minded filtering. Even sillier, the German federal and state governments have recently agreedto ban pornography worldwide except between 11pm and 6am in their timezone.

* Attempts to prevent viruses through filters instead of designing systems correctly to prevent them.

* Attempts to control spamming often overzealously block important e-mail.

* Technology can do wonders for the entire world, but only if we canget away from crass commercial greed. The commercial marketplacewill not solve all our problems. We cannot dominate and control the world,nor can we be completely isolationist.

* We must look at the global implications of everything we do. World economics. The world environment. Combatting world povertyand hunger. We

pay lip-service to better education, but education also seems to be suffering from lowest-common-denominatorism, increasingly emphasingthe regurgitation of factoids -- including misinformation gleaned fromthe Internet. Creative thinking seems to be deprecated.

* Optimizations based on narrow sets of assumptions (what might seemgood for me personally? or for my family? or for my company? or for my country) produce wildly differing results from optimizations based on realistic assessment of long-range and often not just national implications.

- Enron is an extreme example of optimizing from the perspectiveof a few individuals rather than from the perspective of the employeesand stock holders, or even more broadly from the perspective ofthe good of the nation and the world!

- Fossil-fuel is another example. Policies based on theassumption that oil is the most important commodity in the world are radicallydifferent from human-oriented policies, policies based on alternativeenergy sources and conservation or moderation. To a manwith a hammer, everything looks like a nail. To an investor inoil, everthing looks like a dollar bill. To anyone interested in long-termsurvival of the planet and the species, conservation looks like a no-brainer.

- Long-term research versus short-term profits (as two extrememotivations, with many intermediate approaches). We have becometremendously short-sighted regarding long-term research, which is absolutelyessential for the future of the planet. By failing to adequatelysupport essential research, we are eating our own seed corn. Thereare a few outstanding examples of far-sighted research that has paid off enormously-- computer systems, telecommunications, lasers, biotechnology, andincreasingly speech recognition and understanding (which is emergingas a huge money saver for the telephone industry). But in the computerfield, and particularly in mass-market software, much of the mostimportant research in robust systems has been ignored in favor of market-drivenfeatures. Of course, we are very gifted when it comes to glitzyentertainment and fancy features. Mass market software is good atproducing dancing pigs on your screen. We produce television sets and othervisual media with amazing picture definition, but the content is often lowest-common denominator. But when it comes to critical systemsthat must function correctly, securely, reliably, all of the time, the recordis amazingly bad.

* As a society, we have seem to have evolved into a mentality of anything goes as long as you can get away with in. This seem applicableto corporations as well as individuals. It seriously affects theenvironment and the long-term future of civilization.

* We evidently don't learn much from history. To come back toEnron, *The New Yorker* had an article by James Surowiecki in January 2002 on an Enron-like scam from 1861, the Central Pacific Railroad, where Leland Stanford and his partners set up a contracting subsidiary and scammedthe government for at least $50 million in overcharges. Of course,all of the documents magically disappeared.

* We are in general very bad at reacting in advance to warning signs, although we seem to do fairly well at building new doors after thehorse is out of the barn. However, given that our critical infrastructuresand our computer-communication technologies are so riddled with vulnerabilities,we need to be much more proactive. Unfortunately, the biggest impedimentseems to be that we have never had the electronic equivalent of a Pearl Harboror September 11, and therefore have not been compelled to do enough toprotect our infrastructures. This is a characteristic problem for security. Unless you have been burned, there is little incentive for proactive action.

We must learn to invest more in the global long-term future, ratherthan just responding to perceived local short-term needs. Long-termvision is essential. Almost everything we do is increasingly interrelatedwith almost everything else -- economic policies, energy policies, technology policies. We should always look at the big picture, rather than just optimizingin the small. And along the way, we need much greater altruism.

* Open democratic institutions are clearly our best hope -- for nation states and for technology policy such as ensuring that the Internetevolves constructively. It seems evident that world terrorism is nurturedby almost everything else. However, democracies can be easily corrupted,and influenced by intense lobbying. The Enron case might be an exampleof what might be called sweet-and-sour pork barrels.

With respect to terrorism, one of my favorite mixed metaphors is applicable here: we are facing a new era in which Pandora's cat is out of thebarn and the genie won't go back in the closet.

U.S Supreme Court Justice Brandeis long ago remarked that governmentsteach by example. A relevant motto in our actions might be "Assumethat others will do as you do, not as you say." So let me conclude by suggestingthat, as individuals and as nations, we need to consistently set examplesthat have deep commitments to international human rights and human well-being,as well as to economically sound environmental policies. Technologyhas a significant role to play -- if it is used wisely. However, itoften further escalates the problems it tries to solve, and sometimes even createsnew problems. For example, there is a serious risk of increasingthe already huge gap between the haves and the have-nots, because technology often benefits only the haves. It also creates a spy-vs-spy spiralwhere the

attackers have a much greater advantage than the defenders. Thisis certainly true of short-sighted security measures that do not lookat the world as a system in the large. Solutions ultimately requirepervasive attention to international affairs, rather than just purely domestic considerations.

BIO: Peter G. Neumann (Neumann@CSL.sri.com, http://www.csl.sri.com/neumann) has doctorates from Harvard and Darmstadt. After 10 years atBell Labs in Murray Hill, New Jersey, in the 1960s, he has been in SRI's ComputerScience Lab since September 1971. He is concerned with computer systemsand networks, security, reliability, survivability, safety, and many risks-related issues such as voting-system integrity, crypto policy,social implications, and human needs including privacy. He moderatesthe ACM Risks Forum, edits CACM's monthly Inside Risks column, chairs the ACM Committeeon Computers and Public Policy, co-chairs the ACM Advisory Committee on Security and Privacy, co-founded People For Internet Responsibility(PFIR, http://www.PFIR.org), and co-founded the Union for Representative International Internet Cooperation and Analysis (URIICA, http://www.URIICA.org). His book, Computer-Related Risks, isin its fourth printing. He is a Fellow of the ACM, IEEE, and AAAS, and is alsoan SRI Fellow. He is the 2002 recipient of the National Computer SystemSecurity Award. He is a member of the U.S. General Accounting Office Executive Council on Information Management and Technology, and the NationalScience Foundation Computer Information Science and Engineering Advisory Board. He has taught at Stanford, U.C. Berkeley, and the University of Maryland.