

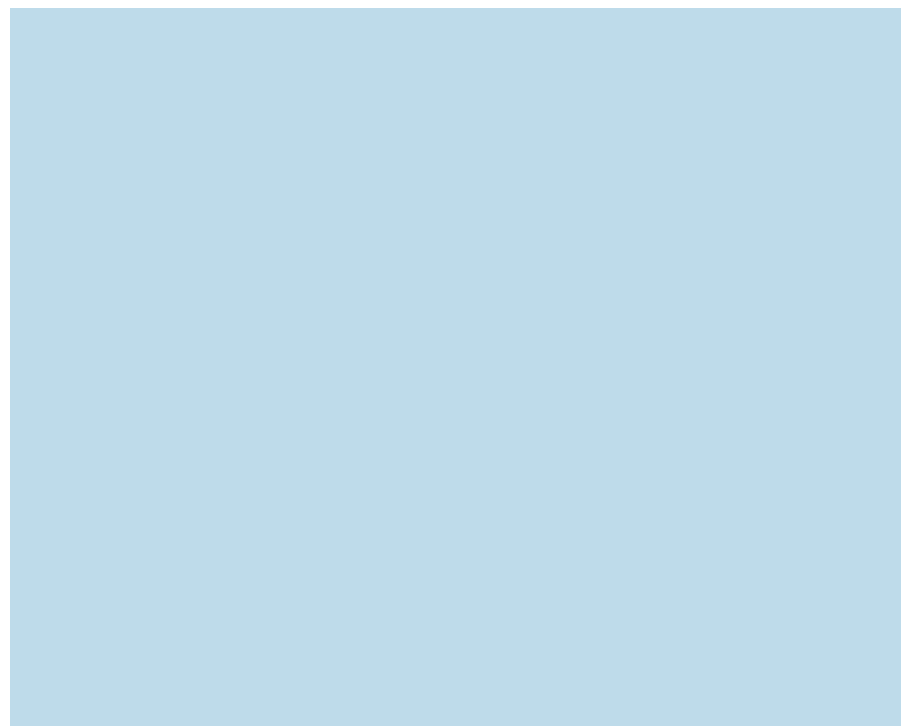
Inside Risks

A Holistic View of Future Risks

Almost everything is somehow interrelated with everything else—and that should not surprise us.

THIS COLUMN CONSIDERS SOME challenges for the future, reflecting on what we might have learned by now—and what we systemically might need to do differently. Previous Inside Risks columns have suggested that some fundamental changes are urgently needed relating to computer system trustworthiness.^a Similar conclusions would also seem to apply to natural and human issues (for example, biological pandemics, climate change, decaying infrastructures, social inequality), and—more generally—being respectful of science and evident realities. To a first approximation here, I suggest almost everything is potentially interconnected with almost everything else. Thus, we need moral, ethical, and science-based approaches that respect the interrelations.

Some commonalities across different disciplines, consequent risks, and what might need improvement are considered here. In particular, the novel coronavirus (COVID-19) has given us an opportunity to reconsider many issues relating to human health, economic well-being (of individuals, academia, and businesses), domestic and international travel, all group activities (cultural, athletic, and so forth), and long-term survival of our planet in



the face of natural and technological crises. However, there are also some useful lessons that might be learned from computer viruses, malware, and inadequate system integrity, some of which are relevant to the other problems—such as computer modeling and retrospective analysis of disasters, supply-chain integrity, and protecting whistle-blowers.

A quote from Jane Goodall in an interview in April 2016 seems more broadly relevant here than in its original context: “If we carry on with business as usual, we’re going to destroy

ourselves.” The same is true of my quote from the early crypto wars regarding export controls: “Pandora’s Cat Is Out of the Barn, and the Genie Won’t Go Back in the Closet.” We are apparently reaching a crossroads at which we must reconsider potentially everything, and especially how it affects the future.

Priorities Among Competing Goals
Human civilization does not tend to agree among issues such as *fairness, equality, safety, security, privacy, and self-determination* (for example). With

^a For example, see “How Might We Increase System Trustworthiness?” *Communications* (Oct. 2019); <http://www.csl.sri.com/neumann/cacm247.pdf>

COVID-19, economical well-being, health care, climate change, and other issues (some of which are considered here), if we cannot agree on the basic goals, we will never reach whatever they might have been—especially if the goals appear to compete with each other.

The Importance of Fundamental Principles

Numerous principles for computer system security and integrity have been known for many years, and occasionally practiced seriously. Some corresponding principles might be considered more broadly in the combined context of risks in engineering computer-related systems, but also in natural systems.

Albert Einstein wrote “It can scarcely be denied that the supreme goal of all theory is to make the irreducible basic elements as simple and as few as possible without having to surrender the adequate representation of a single datum of experience.”^b This is often paraphrased as “Everything should be made as simple as possible, *but no simpler*.” Although the longer statement could be thought of as applicable to trying to explain things as they are (for example, the universe), the simplified version (“should be made”) is also fundamental to the development of new computer systems, as well as in planning proactively for potential catastrophes and collapsing infrastructures.

This *principle*, together with principles relating to transparency, accountability, and scientific integrity, suggest dealing openly and appropriately with risks, while being respectful of science and reality throughout. For example, we tend to make huge mistakes by stressing short-term gains (particularly financial), while ignoring the long-term risks (including everything else). Unfortunately, the gains are unevenly distributed, as the rich get richer, and the poor tend to get poorer and suffer much more.

The principles relating to completeness are particularly critical to com-

puter system design, implementation, applications, and human interfaces, but also regarding responses to pandemics, climate change, and the planet’s environment—along with their implications for human health and well-being, and resource exhaustion of rare elements.

A closely related principle of *pervasive holism* invokes a big-picture view of the Einstein principle, in which everything is potentially in scope unless explicitly ruled out—for example, for reasons of impossibility, feasibility, or perhaps for mistaken decisions about costs, when the long-term overall benefits would dramatically outweigh the short-term savings. Pervasive holism represents the ability to consider all relevant factors, and the ensuing risks. It is relevant broadly across many disciplines. For example, it is essential in the design of computer-communication systems. It encourages systems to be designed to compensate for a wide range of threats and adversities, including some that might not be anticipated *a priori*. Similarly, climate change is causatively linked with extreme weather conditions, melting glaciers, more disastrous fires, human activities, fossil fuels, changes in agriculture, and—with nasty feedback—greater demands for air conditioning and refrigerants such as hydrofluorocarbons that are making the problems worse. On the positive side, atmospheric and sea changes have been observed during the pandemic shutdown (with reduced fuel consumption and much less travel), reinforcing arguments that alternatives to fossil fuels are urgently needed (especially as they are becoming

Numerous principles for computer system security and integrity have been known for many years, and occasionally practiced seriously.

increasingly economical and competitive).

Many nations have clearly realized that careful application of scientific analysis is always desirable, but it can be misused or misapplied. In confronting pandemics, massive immunization programs must be preceded by extensive testing, without which they can have serious consequences (including organ failures, deaths, iatrogenic effects, and in some cases allergic reactions such as anaphylaxis). In pharmaceuticals, some effects are disingenuously called ‘side-effects’—whereas in many cases these effects are well known to have occurred (and are often extensively enumerated in the labeling). However, the effects of deforestation, pesticides, toxic environments (water, air, polluted oceans), non-recyclable garbage, overuse of antibiotics, and so on should by now all be well recognized as long-term risks.

In today’s novel coronavirus and its ongoing mutations, a holistic approach requires anticipating human physical and mental health factors, and their interactions with economic factors and social equality (all persons are supposedly created equal, but usually not treated accordingly—but what about other creatures?), along with future implications, globally rather than just locally. It also requires understanding potential long-term damage—for example, effects on heart, brain, and other organs are still unknown. Fully anticipating the consequences of insurance policies that would not allow existing preconditions is also a major issue, in light of the huge numbers of COVID-19 infections worldwide. Equality in almost everything is desirable, especially in education when home schooling is impossible, broadband access is spotty or nonexistent, and the lack of ubiquitous Internet-accessible devices is a show-stopper for many children. Equal opportunity to vote is also critical, but is being badly abused. Furthermore, spreading disinformation and other forms of disruption can be especially damaging in all of the preceding cases. So, many of these issues are actually interrelated. As one further example of the extent of interrelationships and inter-

^b See <https://quoteinvestigator.com/2011/05/13/einstein-simple/>

locking dependencies, the realization that arctic glacial melting is releasing methane and possibly ancient viruses from earlier pandemics is also relevant.

Principles involving controllability, adaptability, and predictability require better understanding of the importance of *a priori* requirements, as well as the vagaries of models, designs, development, implementation, and situational awareness in real time. These are vital in computer system development. In pandemics, these principles should help reduce the uncertainties of taking different approaches to limiting propagation of contagion, severity of cases, duration of disruption, extent of acquired immunities, and above all a willingness to accept reality and scientific knowledge.

A caveat is needed here: The preceding principles can be used effectively by people who deeply understand the fields in which they are working—and who also have a willingness to work well with colleagues with a better understanding of other areas. In the absence of such knowledge and willingness, the principles are likely to be very poorly misapplied. Humility is a virtue in this regard.

Legal and Ethical Principles

In the social and economic arena, there is a similar need for close attention to the core legal principles driving privacy, antitrust, labor rights, environmental damage, and so on. There is a small but growing group of legal scholars who are revisiting our legal foundations, in an overarching framework they call an approach to ‘law and political economy’, somewhat in reaction to the very influential ‘law and economics’ approach that originated from the University of Chicago.^c

Adherence to ethical principles is of course also likely to contribute to human integrity, as well as to transparency, accountability, and reality.

Models, Predictions, and Planning

Creating realistic models for computational or other problems considered here is always an art form. A selected model may itself be fundamentally di-

Adherence to ethical principles is of course also likely to contribute to human integrity, as well as to transparency, accountability, and reality.

vergent from reality. Assumptions made may be speculative, or in some cases intentionally biased to enable the model to justify preconceived goals. (With statistics, anything can be ‘proven’.) Furthermore, static models are unable to adapt to changing events, so the model must be adaptable to evolving realities and the emergence of better knowledge. This is true of pandemics, climate change, as well as computer system behavioral modeling.

Having well-designed models that provide transparency, respect reality, and are mathematically sound is very important—in order to be able to reason sensibly. However, because models inherently represent abstractions of reality, reasoning about models typically introduces discrepancies between the models and reality. Predicting the future based on erroneous models and erroneous logic is not a path to success. Similar remarks apply to statistical analysis of inherently multidimensional problems. These issues have clearly been raised in predicting the progress of pandemics, climate change, and the trustworthiness of computer systems (for example). Although this is a particularly fundamental area, it deserves much more study. However, when evidence clearly demonstrates poor results, it is time to reassess failed remediations.

Testing and Verifying

Testing finds problems, but cannot find the absence of problems. Verification can find some of the problems, but many others are beyond routine analysis—such as side channels, hardware attacks, and other things that might not be included in threat mod-

Calendar of Events

VOLUTPAT ORNARE ARCU

Donec sit amet neque nec odio pharetra semper. Suspendisse dictum ligula eu diam. Pellentesque convallis porttitor eros. Nunc placerat accumsan ante. Etiam scelerisque nisl non ligula. Quisque vitae lacus. Pellentesque in augue. Integer laoreet nisl nec ipsum. Ut massa orci molestie quis, blandit et cursus et lorem. Donec congue massa quis metus.

DONEC EU MAGNA

Nunc aliquet ante eget lectus. Vestibulum scelerisque dignissim nisi. Phasellus id elit suspendisse aliquet. Aenean semper, magna quis interdum sagittis, arcu odio tincidunt lacus, non tristique diam arcu sed nibh. Vestibulum non eros vitae dolor dignissim volutpat.

Suspendisse elementum, felis vel hendrerit congue, neque urna consectetur nisl, ac vehicula nisi leo id arcu. Aenean aliquam. Sed suscipit. Quisque semper justo sed leo. Aenean porta, diam non pellentesque pulvinar, ipsum orci ultrices dui, in elementum velit mauris sit amet dolor.

PELLENTESQUE ERAT

Vitae dui semper fermentum. Fusce pede mauris, rutrum at, ullamcorper porta, ultrices ac, felis. Integer nunc enim, bibendum quis, ullamcorper nec, dictum sed, lorem. Morbi lacinia felis vitae massa. Nam tortor magna posuere, adipiscing ac, tincidunt eu, lectus. Nulla tortor nisi, sodales non, luctus non, posuere at, ante. Suspendisse adipiscing sem mollis mi. Duis lobortis commodo orci.

ODIO SED TORTOR

Interdum mollis. Maecenas lobortis, tellus sed mollis nonummy, sapien ante aliquet tellus, et sagittis lacus dolor eu sem. Quisque ut turpis nec risus molestie scelerisque. Nulla placerat. Curabitur sollicitudin quam ut risus.

Mauris aliquet, felis imperdiet adipiscing imperdiet, purus dolor sollicitudin felis, vel convallis ligula lorem scelerisque lorem. Nunc pellentesque. Cras nec lacus. Aenean suscipit sem a orci.

^c See https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547312

AD TK

els. Thus, even a combination of both may not be enough, which applies to computer algorithms, protocols, software, and hardware, but also to some of the other areas considered here. For example, biological testing and applications of artificial intelligence and deep learning need to have a sounder basis that could eliminate vastly too many false positives and false negatives, as well as other forms of unrealistic results.

Formal methods are increasingly being applied to software hypervisors (for example, CertiKOS, seL4, and the Green Hills Integrity Multivisor) and to hardware (for example, CHERI, Centaur). Formal modeling of biological pathways, techniques to stimulate immunities, effects of climate change, short- versus long-term consequences, and many other possible approaches could be considered using formal analysis. Of particular interest might be formal analysis of requirements, models, and analysis techniques in other areas considered here.

System and Supply-Chain Integrity

The availability and integrity of delivered computer-related systems and medical supplies clearly present enormous problems, which are likely to be exacerbated in times of crisis. Over recent years, the implementation of many entities has increasingly been outsourced and off-shored, including computer hardware fabrication, just-in-time delivery of automobile parts, hospital health-care necessities, and even food. It should be obvious that our computer systems, medical supplies, and other resources may be inadequately protected from supply-chain disruptions, tampering, and even fraud.

The effects of monopolized industrial sectors are notable here. The concentration of industrial production of various types in a few very large players (most prominently and visibly in the tech sector, but it is pervasive across the board with hidden monopolies galore, for example, in pharmaceuticals and health-care management).^d It effectively creates fewer but far more consequential points of failure. In addition, due to the lack of alternatives, product quality

suffers when market power is abused, due to the lack of alternatives.^e

Principles of robust and resilient system design, both industrial and computer related, suggest that having many distributed and roughly commensurate producers or protocol participants is preferable to highly centralized structures. The latter might be superficially more efficient, but could mask dramatic failure modes. This notion also shows up in ecology, where diverse and vibrant farm ecosystems are typically more resilient than crop monocultures. Furthermore, concentrated economical power embodied by monopolies is easily converted into political power, leading to contribution-favoring legislation and rising economic inequality.

The advantages of having diverse and widely dispersed (but well coordinated and carefully monitored) actors seem to be preferable in improving distributed computer-system resiliency, economies of industrial organizations, approaches to pandemics, and thriving ecosystems.

System Integrity

Overall system integrity is also an issue. For example, election integrity is dependent not just on voting machines and paper ballots. It also depends on the trustworthiness of registration databases, tabulation and auditing processes, as well as (for example) the avoidance or tolerance of distorting effects such as gerrymandering, selective disenfranchisement, and rampant use of disinformation. Some efforts require effective national leadership, and in some cases extensive international cooperation.

Protecting Protectors and Truth of Information

Reporting of systemic flaws newly found by white-hat hackers has generally become carefully managed in order to avoid flagrant misuse; however, the market for zero-day flaws remains lucrative. Whistle-blowers have often subsequently been victims of character assassinations, particularly those that are fabricated to distract from

^d See <https://prospect.org/health/hidden-monopolies-raise-drug-prices/>

^e See <https://prospect.org/power/monopoly-misrepresentation-and-malpractice-3m-ear-plugs/>

Willingness to accept and respond to reality is fundamental to avoiding risks.

would-be exposure of misdeeds. Also, numerous medical experts who have dealt with legitimate scientific evidence regarding COVID-19 have been treated as illegitimate purveyors of fake information, as if they had been whistle-blowers spreading false accusations. The same is true of climate change, which requires careful consideration of the underlying science. Conspiracy theories continue to appear. The principles of transparency and accountability are particularly important in these contexts.

Privacy and Related Concerns

Respecting personal privacy is a ubiquitous challenge in every computer-related activity, particularly in the presence of overreaches in widespread surveillance, the desire for cryptographic backdoors for law enforcement, and detailed statistical reporting. In addition, addressing rampant disinformation and hate speech, as well as attacks on whistle-blowers, are in conflict while trying to protect free speech. Some of these and other issues are particularly relevant to pandemics (for example, with the need for intensive monitoring and large-scale fine-grained contact tracing)—as well as almost everything involving big data.

What Is Missing from This Conceptual Big-Picture View?

The discussion here may seem somewhat disconnected, and the desire for holistic approaches overly ambitious. However, it is becoming ever clearer that the topics considered here are interrelated in ways that are sometimes not obvious. For example, man-made disruptions of nature seem to be bit-

ing back at us in various ways, including climate change, health, eco-balance, pollution, and animal-human crossovers of pandemics. This column is merely a high-level attempt to find commonality in what may once have appeared to be disparate subjects. Putting all the pieces together with adequate foresight presents major challenges. Everything along the way needs precise definitions, descriptions, specifications, and logical thought, including the dependencies among the constituent elements. Well-defined realistic abstractions are important, along with well-defined refinements that can be used to determine overall consistency and predictable results. Only then can rational conclusions be reached that have any bearing on reality.

The sense of composing the pieces with predictable assurance is conceptually understood in theory with respect to computer systems, although not often observed in practice. A goal here would be to mirror such approaches with respect to other areas, such as biological processes, pandemic spreading, environmental problems, and other socioeconomic issues, to give them a more scientific and logical basis. Understanding the legal foundations of markets and social interactions is also a basic part of what needs to be included in the holistic view, along with the technological, engineering, and other scientific principles. Identifying any common abstractions and their potential interactions could be very helpful.

In the opposite direction, what might computer technology learn from the ongoing natural-world problems noted here? For example, our system models and risk models for trustworthy computer systems generally fail to consider the risks holistically—for example, neglecting those that are external to the technology. Predicting any consequences on the basis of questionable models is also a major risk, especially if the results superficially seem generally believable—and what one might like to believe. Thus, we need to learn more from each other.

Conclusion

Willingness to accept and respond to reality is fundamental to avoiding risks.

The unknown unknowns are always risky, but can be minimized somewhat by proactively seeking to identify the potential risks, and reflecting on Murphy's Law—rather than ignoring the emergence of certain presumed rare disasters that have been emerging much more often, which deserve *a priori* attention (rather than relying on case-by-case *a posteriori* remediation).

This clearly applies to infrastructures, supply chains, and medical preparedness, among other topics considered here—or further topics that could have been included here but were not even mentioned, with the unfortunate consequence of making the discussion *too simple*, in conflict with the Einstein principle.

As has been frequently noted, but which is nevertheless highly relevant here, We Are All In This Together, and Almost Everything Is Increasingly Becoming Interrelated—for better or for worse. Isolated defensive actions have very limited value; your own actions can affect others. Retrogressive governmental actions are counterproductive. Biological viruses and computer risks can both propagate globally with amazing rapidity. In any event, you must protect yourself, while also respecting the well-being of others. Wearing a mask and isolating yourself are akin to being intensely security-aware with respect to computer viruses and phishing attacks, having backups to defend against ransomware attacks, and being cognizant of reality.

Ultimately, more altruistic foresight could help to avoid all sorts of undesirable events, such as pandemics, climate change, environmental disasters, global extinction of species, disparities in education and economic well-being, and unnecessary losses of human life—as well as crossover combinations of these (for example, as varied as the Deepwater Horizon fiasco, deforestation of the Amazon, the demise of honey bees, and wars). And yet, this brief summary is only a beginning. ▣

Peter G. Neumann (neumann@csl.sri.com) is Chief Scientist of the SRI International Computer Science Lab, and has moderated the ACM Risks Forum since its beginning in 1985. He is grateful to Prashanth Mundkur and Tom Van Vleck for helping considerably enrich the holistic perspective in this column.

Copyright held by author.