DOI:10.1145/3593005

Peter G. Neumann

Inside Risks

Computer-Related Risks and Remediation Challenges

Surveying the nontechnical issues interwoven with computer-related technologies.

THIS INSIDE RISKS column focuses on some of our computer technologies that are directly or tangentially involved in undesirable misuses, and what effective remedies might be desirable. The following enumeration is illustrative: the items are by no means comprehensive, and some cases fall into multiple categories.

▸ Uses of technology to address problems that are otherwise inherently not purely technological: for example, cryptocurrencies being used to address dissatisfaction with financial systems perceived as rigged in favor of Wall Street and banks, including money-laundering and other illegal activities used to avoid law enforcement.[a] Increases in electronic gambling (including offshore) are yet another step toward depriving addicts and others of their well-being.

▸ Uses of technology to facilitate crimes that were hitherto not technology-oriented: for example, online spear-phishing scams with ransomware and demands for cryptocurrency payments, with no real assurance of ultimate recovery in the absence of demonstrable defenses. Law enforcement seems to not have much leverage here, and offshore attacks make the problems even more difficult.

IMAGE BY ZAMUROVIC BROTHER/SHUTTERSTOCK.COM

▹ Uses of technology with well-defined legitimate purposes but poorly established or administered foundations; for example, elections that have inadequate oversight and no worthy audit trails, irrespective of whether administered in-person or using the Internet. Even the compositional trustworthiness of integrated electronic systems (voting machines, ballot scanners, vote counters) needs much more assurance from a total-system perspective, given the interfaces among the components may themselves be compromised.[b] Furthermore, abuses of social media with character assassination and disinformation—incuding Chatbots—are creating enormous problems. Misuses of digital commerce also falls into this category.

▹ Uses of technology that is not sufficiently trustworthy for its intended application needs. This is particularly relevant to high-end national security and life-critical applications, with respect to security, privacy, system and network integrity, human safety, high-probability system survivability, and more. Artificial intelligence is seen by some as a panacea, even when embedded in untrustworthy systems and networks whose compromise might in turn decrease its integrity, total-system safety, and predictability. Of course, these problems can also arise in many less-critical applications where exploits are unfortunately surprisingly easy to perpetrate—as in the ubiquity of the Internet of Almost Everything where very little assurance exists today.

▹ Uses of technology that has been compromised in favor of questionable business models: for example, targeted advertising in social media and gaming that results in widespread privacy violations, devious operation, greed, and obliviousness to the risks. Zeynep Tufekci's op-ed in *The New York Times*, "The Shameful Secret of Southwest's Failure," (Jan. 5, 2023), examines Southwest Airlines' repeated failures to upgrade their archaic computer software, which resulted in the recent total system-wide meltdown. The drive to get self-driving cars on the road quickly appears to be quite controversial, and full of dangerous behavior. Short-term optimization and failure to consider long-term risks seem to be much more important to many organizations than long-term stability. The book by Earl Boebert and James Blossom, *Deepwater Horizon: A Systems Analysis of the Macondo Disaster*, Harvard Press illustrates hasty iatrogenic technological remediations motivated by a compromised business model.

This list highlights just a few potential types of misuses of technology that remain widespread from year to year, with relatively few repercussions—a long-time topic in the ACM Risks Forum.[c] One theme that runs through the items listed here (and in previous *Communications* Inside Risks columns) is that today's technology is not trustworthy enough for many critical applications, even if it were used carefully. Some of these concerns could be addressed in the future by increasing research and development in system assurance, as suggested in the June 2022 *Communications* Inside Risks column "Total-System Trustworthiness." This would require at least better hardware and better software engineering practices, and greater oversight. Other issues reach way outside of technology, but are seriously exacerbated by the Internet, the Dark Web, rampant disinformation, a general lack of risks awareness, and other factors.

Short-term optimization and failure to consider long-term risks seem to be much more important to many organizations than long-term stability.

Gaps in education that address all of the issues mentioned here are also a serious concern. Math scores appear to be down in many countries, and younger employees do not seem to know how to make change when paid in cash. English and other language scores are down, and many people—not just younger students—cannot write or speak in intelligible sentences. Also, colloquial speech often can result in potentially serious ambiguities. Books may also cause trouble, as reading abilities seem to be diminishing and respected classic books are being banned for being subversive. (See Ray Bradbury's book *Fahrenheit 451* and subsequent movies.) Unfortunately, the notion of socioeconomic equality in educational and employment opportunities is politically challenged—although technology might offer some help, if it were easy to master and were used more wisely.

In addition, education of technology (in the U.S., at least) seems to have lost the incentives to consider systems in the large, instead stress-

[a] See Paul Krugman, "Blockchains, What Are They Good For?," *The New York Times* (Dec. 2, 2022).

[b] See the June 2021 *Communications* Inside Risks column "The Risks of Election Believability (or Lack Thereof)," which is a plea for designing, deploying, and overseeing systems with higher assurance—as a matter of good practice, but also to combat those who believe well-administered past elections have been rigged, and that future elections can also be compromised.

[c] See http://www.risks.org

ing programming languages that are too easy to misuse and that have inherent failings. For example, Bruce Debruhl has nicely amplified the lack of system-orientation in U.S. colleges and university curricula.[d] Even the so-called memory-safe languages (such as Java and Rust) can be badly misused, and allow elements that are not memory safe to be invoked. An interesting discussion of technology education and its relation to public interest, with various short-term and long-term potential remediations seems to be of considerable interest.[e]

Conclusion

Recent years have been a period in which certain computer-related technologies are being relied upon, with relatively little reflection on their short- and long-term effects. It is also an era in which other issues relying on those technologies also became challenged by extreme views that ignored the nuances relating to those issues, and that disregard sound science. The COVID-19 pandemic seems to have considerably changed our views of the future. The ChatBot craze is riddled with problems.[f] However, personal, institutional, and governmental integrity has become challenged, where many nontechnical issues are tightly interwoven with technology and must also be understood—for example, as part of the threat models and business models, as well as development practice and oversight. We need considerably more attention to total-system and application assurance in our educational efforts and in responsible system developments.

The ChatBot craze is riddled with problems.

Today's technology is not trustworthy enough for many critical applications.

Ideally, we also might need to include humanistic approaches to the uses of technology, such as espoused by Norbert Wiener in 1950,[g] Joseph Weizenbaum, Don Norman, and others. Uses of technology should benefit people, not just corporations. At present, technological advances seem to be an end in themselves, much more likely to increase disparities rather than to diminish them—for example, between the rich and the poor; advanced and struggling nations; economic well-being and abject poverty; and so on. Furthermore, computer technology might be considered potentially dangerous if it is without meaningful assurances that it can satisfy humanitarian needs, or even that it can provide assurances that its dual uses for evil can be manageable. However, in today's world that would seem very difficult to achieve.

Some of the problems noted here are actually very complex and multifaceted. Serious future-facing steps might require approaches transcending the technology, such as legal constraints on uses of technology primarily anti-humanitarian, as well as steps toward less disparity in education, jobs, and pay scales, and a cultural shift that issues considered here tend to require significant nontechnological remediation as well as proactive realizations of the limits of technology. However, beware of oversimplification!

[d] See *ACM Risks Forum 33*, 56; http://www.risks.org

[e] See https://bit.ly/3UXXR9n

[f] For example, see El-Mahdi et al. On the Impossible Security of Very Large Foundation Models; https://bit.ly/3L6tpVT

[g] See Norbert Wiener, *Human Use of Human Beings* (1950).

Peter G. Neumann (neumann@csl.sri.com) is Chief Scientist in the SRI International Computer Science Lab and creator/moderator of the ACM Risks Forum.

He is very grateful to his long-standing Inside Risks oversight group (whose patience helped significantly in developing this column) and to Prashanth Mundkur for his incisive comments.