DOI:10.1145/2700366

Peter G. Neumann

# Inside Risks
# Far-Sighted Thinking about Deleterious Computer-Related Events

*Considerably more anticipation is needed for what might seriously go wrong.*

Several previous *Communications* Inside Risks columns (particularly October 2012 and February 2013) have pursued the needs for more long-term planning—particularly to augment or indeed counter some of the short-term optimization that ignores the importance of developing and operating meaningfully trustworthy systems that are accompanied by proactive preventive maintenance. This column revisits that theme and takes a view of some specific risks. It suggests that advanced planning for certain major disasters relating to security, cryptography, safety, reliability, and other critical system requirements is well worth consideration. The essential roles of preventive maintenance are also essential.

## Crises, Disasters, and Catastrophes

There is a wide range of negative events that must be considered. Some tend to occur now and then from which some sort of incomplete recovery may be possible—even ones that involve acts that cannot themselves be undone such as deaths; furthermore so-called recovery from major hurricanes, earthquakes, and tsunamis does not result in the same physical state as before. Such events are generally considered to be crises or disasters. Other events may occur that are totally surprising and truly devastating (for example, the comet activity that is believed to have caused a sudden end of the dinosaurs).

In this column, I consider some events relating to computer-related systems whose likelihood might be thought possible but perhaps seemingly remote, and whose consequences might be very far-reaching and in extreme cases without possible recoverability. Such events are generally thought of as catastrophes or perhaps cataclysms. The primary thrust here is to anticipate the most serious potential events and consider what responses might be needed—in advance.

## Cryptography

This column is inspired in part by a meeting that was held in San Francisco in October 2014. The CataCrypt meeting specifically considered Risks of Catastrophic Events Related to Cryptography and its Possible Applications. *Catastrophic* was perhaps an overly dramatic adjective, in that it has an air of finality and even total nonrecoverability. Nevertheless, that meeting had at least two consensus conclusions, each of which should be quite familiar to readers who have followed many of the previous Inside Risks columns.

First, it is clear that sound cryptography is essential for many applications (SSL, SSH, key distribution and handling, financial transactions, protecting sensitive information, and much more). However, it seems altogether possible that some major deleterious events could undermine our most widely used cryptographic algorithms and their implementations. For example, future events might cause the complete collapse of public-key cryptography, such as the advance of algorithms for factoring large integers and for solving discrete-log equations, as well as significant advances in quantum computing. Furthermore, some government-defined cryptography standards (for example, AES) are generally considered to be adequately strong enough for the foreseeable future—but not forever. Others (for example, the most widely used elliptic-curve standard) could themselves already have been compromised in some generally unknown way, which could conceivably be why several major system developers prefer an alternative standard. Recent attacks involving compromisible random-number generators and hash functions provide further warning signs.

As a consequence of such possibilities, *it would be very appropriate to anticipate new alternatives and strategies for what might be possible in order to recover from such events*. In such a situation, planning now for remediation is well worth considering. Indeed, understanding that nothing is perfect or likely to remain viable forever, various carefully thought-through successive alternatives (Plan B, Plan C, and so forth) would be desirable. You might think that we already have some potential alternatives with respect to the putative demise of public-key cryptography. For example, theoretical bases for elliptic-curve cryptography have led to some established standards and their implementations, and more refined knowledge about lattice-based cryptography is emerging—although they may be impractical for all but the most critical uses. However, the infrastructure for such a progression might not be ready for widespread adoption in time in the absence of further planning. Newer technologies typically take many years to be fully supported. For example, encrypted email has been very slow to become easily usable—including sharing secret keys in a secret-key system, checking their validity, and not embedding them in readable computer memory. Although some stronger implementations are now emerging, they may be further retarded by some nontechnical (for example, policy) factors relating to desired surveillance (as I will discuss later in this column). Also, some systems are still using single DES, which has now been shown to be susceptible to highly distributed exhaustive cracking attacks—albeit one key at a time.

**Essentially every system architect, program-language and compiler developer, and programmer is a potential generator of flaws and risks.**

Second, it is clear—even to cryptographers—that even the best cryptography cannot by itself provide total-system solutions for trustworthiness, particularly considering how vulnerable most of our hardware-software systems and networks are today. Furthermore, the U.S. government and other nations are desirous of being able to monitor potentially all computer, network, and other communications, and seek to have special access paths available for surveillance purposes (for example, backdoors, frontdoors, and hopefully exploitable hidden vulnerabilities). The likelihood those access paths could be compromised by other parties (or misused by trusted insiders) seems much too great. Readers of past Inside Risks columns realize almost every computer-related system and network in existence is likely to have security flaws, exploitable vulnerabilities and risks of insider misuse. Essentially every system architect, program-language and compiler developer, and programmer is a potential generator of flaws and risks.

Recent penetrations, breaches, and hacking suggest that the problems are becoming increasingly worse. Key management by a single user or among multiple users sharing information could also be subverted, as a result of system security flaws, vulnerabilities, and other weaknesses. Even worse, almost all information has now been digitized, and is available either on the searchable Internet or on the unsearchable Dark Net.

This overall situation could turn out to be a disaster for computer system companies (who might now be less trusted than before by their would-be customers), or even a catastrophe in the long run (for example, if attackers wind up with a perpetual advantage over defenders because of the fundamental inadequacy of information security). As a consequence, *it is essential that systems with much greater trustworthiness be available for critical uses—and especially in support of trustworthy embeddings of cryptography and critical applications*.

## Trustworthy Systems, Networks, and Applications

Both of the preceding italicized conclusions are highly relevant more generally—to computer system security, reliability, safety, and many other properties, irrespective of cryptography. Events that could compromise the future of an entire nation might well involve computer-related subversion or accidental breakdown of critical national infrastructures, one nation's loss of faith in its own ability to develop and maintain sufficiently secure systems, loss of domestic marketplace presence as a result of other nations' unwillingness to acquire and use inferior (potentially compromisible) products, serious loss of technological expertise, and many other scenarios. The situation is further complicated by many other diverse nontechnological factors—both causes and effects—for example, involving politics, personal needs, governmental regulation or the lack thereof, the inherently international nature of the situation, diplomacy, reputations of nations, institutions and individuals, many issues relating to economics, consequences of poor planning, moral/working conditions, education, and much more.

We consider here a few examples in which the absence of sufficient trustworthiness might result in various kinds of disaster. In each case, differences in scope and negative impacts are important considerations. In some cases, an adverse event may be targeted at specific people or data sources. In other cases, the result may have much more global consequences.

**Ubiquitous surveillance**, especially when there is already insufficient trustworthiness and privacy in the systems and networks being surveilled. Planning for a world in which the desires for meaningfully trustworthy systems have been compromised by ubiquitous surveillance creates an almost impossible conflict. The belief that having backdoors and even systemic flaws in systems to be used by intelligence and law-enforcement operatives without those vulnerabilities not being exploited by others seems totally fatuous.[2] As a consequence, the likelihood of having systems that can adequately enforce security, privacy, and many other requirements for trustworthiness seem to have almost totally disappeared. The result of that reality suggests that many routine activities that depend on the existence of trustworthy systems will themselves be untrustworthy—human safety in our daily lives, financial transactions, and much more.

There is very little room in the middle for an acceptable balance of the needs for security and the needs for surveillance. A likely lack of accountability and oversight could seriously undermine both of these two needs.

Privacy and anonymity are also being seriously challenged. Privacy requires much more than secure systems to store information, because many of the privacy violations are external to those systems. But a total privacy meltdown seems to be emerging, where there will be almost no expectation of meaningful privacy. Furthermore, vulnerable systems combined with surveillance results in potential compromises of anonymity. A recent conclusion that 81% of users of a sampling of anonymizing Tor network users can be de-anonymized by analysis of router information[1,a] should not be surprising, although it seems to result from an external vulnerability rather than an actual flaw in Tor. Furthermore, the ability to derive accurate and relatively complete analyses from communication metadata and digital footprints must be rather startling to those who previously thought their actions were secure, when their information is widely accessible to governments, providers of systems, ISPs, advertisers, criminals, approximately two million people in the U.S. relating to healthcare data, and many others.

## A Broader Scope

Although the foregoing discussion specifically focuses primarily on computer-related risks, the conclusions are clearly relevant to much broader problems confronting the world today, where long-term planning is essential but is typically deprecated. For example, each of the following areas is often considered to be decoupled from computer-communication technologies, but actually is often heavily dependent on those technologies. In addition, many of these areas are interdependent on one another.

**Privacy requires much more than secure systems to store information, because many of the privacy violations are external to those systems.**

- *Critical national infrastructures* are currently vulnerable, and in many cases attached directly or indirectly to the Internet (which potentially implies many other risks). *Telecommunications providers* seem to be eager to eliminate landlines wherever possible. You might think that we already have Plan B (mobile phones) and Plan C, such as Skype or encrypted voice-over-IP. However, such alternatives might assume the Internet has not been compromised, that widespread security flaws in malware-susceptible mobile devices might have been overcome, and that bugs or even potential backdoors might not exist in Skype itself. Furthermore, taking out a few cell towers or satellites or chunks of the Internet could be highly problematic. *Water supplies* are already in crisis in some areas because of recent droughts, and warning signs abound. Canadians recall the experience in Quebec Province in the winter of 1996–1997 when power distribution towers froze and collapsed, resulting in the absence of power and water for many people for almost a month. Several recent hurricanes are also reminders that we might learn more about preparing for and responding to such emergencies. *Power generation and distribution* are monitored and controlled by computer systems are potentially vulnerable. For example, NSA Director Admiral Michael Rogers recently stated that China and "probably one or two other" countries have the capacity to shut down the nation's power grid and other critical infrastructures through a cyberattack.[b] Clearly, more far-sighted planning is needed regarding such events, including understanding the trade-offs involved in promoting, developing, and maintaining efficient alternative sources.
- *Preservation and distribution of clean water supplies* clearly require extensive planning and oversight in the face of severe water shortages and

[a] Roger Dingledine's blog item and an attached comment by Sambuddho, both of which qualify the 81% number as being based on a small sample. See https://blog.torproject.org/blog/traffic-correlation-using-netflows.

[b] CNN.com (Nov. 21, 2014); http://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/.

lack of sanitation in some areas of the world, and the presence of endemic diseases where no such supplies currently exist. Computer models that relate to droughts and their effects on agriculture are not encouraging.

- Understanding the importance of proactive *maintenance of physical infrastructures* such as roadways, bridges, railway track beds, tunnels, gas mains, oil pipelines, and much more is also necessary. From a reliability perspective, many power lines and fiber-optic telecommunication lines are located close to railroad and highway rights of way, which suggests that maintenance of bridges and tunnels is particularly closely related to continuity of power, and indeed the Internet.
- *Global warming and climate change* are linked with decreasing water availability, flooding, rising ocean temperatures, loss of crops and fishery welfare. Computer modeling consistently shows incontrovertible evidence about extrapolations into the future, and isolates some of the causes. Additional computer-related connections include micro-controlling energy consumption (including cooling) for data centers, and relocating server complexes into at-risk areas—the New York Stock Exchange's computers must be nearby, because so much high-frequency trading is affected by speed-of-light latency issues. Moving data centers would be vastly complex, in that it would require many brokerage firms to move their operations as well.
- *Safe and available world food production* needs serious planning, including consideration of sustainable agriculture, avoidance of use of pesticides in crops and antibiotics in grain feeds, and more. This issue is of course strongly coupled with climate change.
- *Pervasive health care* (especially including preventive care and effective alternative treatments) is important to all nations. The connections with information technologies are pervasive, including the safety, reliability, security and privacy of healthcare information systems and implanted devices. Note that a catastrophic event for a healthcare provider could be having its entire collection of records harvested, through insider misuse or system penetrations. The aggregate of mandated penalties could easily result in bankruptcy of the provider. Also, class-action suits against manufacturers of compromised implanted devices, test equipment, and other related components (for example, remotely accessible over the Internet or controlled by a mobile device) could have similar consequences.

**The biggest realization here may be that many of these problem areas are closely interrelated, sometimes in mysterious and poorly understood ways.**

- *Electronic voting systems* and *compromises to the democratic process* present an illustrative area that requires total-system awareness. Unauditable proprietary systems are subject to numerous security, integrity, and privacy issues. However, nontechnological issues are also full of risks, with fraud, manipulation, unlimited political contributions, gerrymandering, cronyism, and so on. Perhaps this area will eventually become a poster child for accountability, despite being highly politicized. However, remediation and restoration of trust would be difficult. Eliminating unaccountable all-electronic systems might result in going back to paper ballots but procedural irregularities remain as nontechnological problems.
- *Dramatic economic changes* can result from all of the preceding concerns. Some of these potential changes seem to be widely ignored.

The biggest realization here may be that many of these problem areas are closely interrelated, sometimes in mysterious and poorly understood ways, and that the interrelations and potential disasters are very difficult to address without visionary total-system long-term planning.

## Conclusion

Thomas Friedman[3] has written about the metaphor of *stampeding black elephants*, combining the black swan (an unlikely unexpected event with enormous ramifications) and the elephant in the room (a problem visible to everyone as being likely to result in black swans that no one wants to address). Friedman's article is concerned with the holistic preservation of our planet's environment, and is not explicitly computer related. However, that metaphor actually encapsulates many of the issues discussed in this column, and deserves mention here. Friedman's discussion of renewed interest in the economic and national security implications is totally relevant here—and especially soundly based long-term economic arguments that would justify the needs for greater long-term planning. That may be precisely what is needed to encourage pursuit of the content of this column.

In summary, without being a predictor of doom, this column suggests we need to pay more attention to the possibilities of potentially harmful computer-related disasters, and at least have some possible alternatives in the case of serious emergencies. The principles of fault-tolerant computing need to be generalized to disaster-tolerant planning, and more attention paid to stampeding black elephants.

### References

1. Anderson, M. 81% of users can be de-anonymised by analysing router traffic, research indicates. *The Stack*; http://thestack.com/chakravarty-tor-traffic-analysis-141114.
2. Bellovin, S.M., Blaze, M., Diffie, W., Landau, S., Neumann, P.G., and Rexford, J. Risking communications security: Potential hazards of the Protect America Act. *IEEE Security and Privacy 6*, 1 (Jan.–Feb. 2008), 24–33.
3. Friedman, T.L. Stampeding black elephants: Protected land and parks are not just zoos. They're life support systems. *The New York Times* Sunday Review (Nov. 23, 2014), 1, 9.

**Peter G. Neumann** (neumann@csl.sri.com) is Senior Principal Scientist in the Computer Science Lab at SRI International, and moderator of the ACM Risks Forum.

I am grateful to members of the Catacrypt steering committee and the ACM Committee on Computers and Public Policy, whose thoughtful feedback greatly improved this column.