Futurists use a Delphi study to highlight top risks from technology that we'll be facing by the year 2040

January 24 2024, by Charles Weir

Credit: CC0 Public Domain

Bewilderingly rapid changes are happening in the technology and reach of computer systems. There are exciting advances in artificial intelligence, in the masses of tiny interconnected devices we call the Internet of Things and in wireless connectivity.

Unfortunately, these improvements bring potential dangers as well as

benefits. To get a safe future we need to anticipate what might happen in computing and address it early. So, what do experts think will happen, and what might we do to prevent major problems?

To answer that question, Our research team from universities in Lancaster and Manchester turned to the science of looking into the future, which is called "forecasting." No one can predict the future, but we can put together forecasts: descriptions of what may happen based on current trends.

Indeed, long-term forecasts of trends in technology can prove remarkably accurate. And an excellent way to get forecasts is to combine the ideas of many different experts to find where they agree.

We consulted 12 expert "futurists" for a new research paper. These are people whose roles involves long-term forecasting on the effects of changes in computer technology by the year 2040.

Using a technique called a Delphi study, we combined the futurists' forecasts into a set of risks, along with their recommendations for addressing those risks.

Software concerns

The experts foresaw rapid progress in artificial intelligence (AI) and connected systems, leading to a much more computer-driven world than nowadays. Surprisingly, though, they expected little impact from two much hyped innovations: Blockchain, a way to record information that makes it impossible or difficult for the system to be manipulated, they suggested, is mostly irrelevant to today's problems; and Quantum computing is still at an early stage and may have little impact in the next 15 years.

The futurists highlighted three major risks associated with developments in computer software, as follows.

AI competition leading to trouble

Our experts suggested that many countries' stance on AI as an area where they want to gain a competitive, technological edge will encourage software developers to take risks in their use of AI. This, combined with AI's complexity and potential to surpass human abilities, could lead to disasters.

For example, imagine that shortcuts in testing lead to an error in the control systems of cars built after 2025, which goes unnoticed amid all the complex programming of AI. It could even be linked to a specific date, causing large numbers of cars to start behaving erratically at the same time, killing many people worldwide.

Generative AI

Generative AI may make truth impossible to determine. For years, photos and videos have been very difficult to fake, and so we expect them to be genuine. Generative AI has already radically changed this situation. We expect its ability to produce convincing fake media to improve so it will be extremely difficult to tell whether some image or video is real.

Supposing someone in a position of trust—a respected leader, or a celebrity—uses social media to show genuine content, but occasionally incorporates convincing fakes. For those following them, there is no way to determine the difference—it will be impossible to know the truth.

Invisible cyber attacks

Finally, the sheer complexity of the systems that will be built—networks of systems owned by different organizations, all depending on each other—has an unexpected consequence. It will become difficult, if not impossible, to get to the root of what causes things to go wrong.

Imagine a cyber criminal hacking an app used to control devices such as ovens or fridges, causing the devices all to switch on at once. This creates a spike in electricity demand on the grid, creating major power outages.

The power company experts will find it challenging to identify even which devices caused the spike, let alone spot that all are controlled by the same app. Cyber sabotage will become invisible, and impossible to distinguish from normal problems.

Software jujitsu

The point of such forecasts is not to sow alarm, but to allow us to start addressing the problems. Perhaps the simplest suggestion the experts suggested was a kind of software jujitsu: using software to guard and protect against itself. We can make computer programs perform their own safety audits by creating extra code that validates the programs' output—effectively, code that checks itself.

Similarly, we can insist that methods already used to ensure safe software operation continue to be applied to new technologies. And that the novelty of these systems is not used as an excuse to overlook good safety practice.

Strategic solutions

But the experts agreed that technical answers alone will not be enough.

Instead, solutions will be found in the interactions between humans and technology.

We need to build up the skills to deal with these human technology problems, and new forms of education that cross disciplines. And governments need to establish safety principles for their own AI procurement and legislate for AI safety across the sector, encouraging responsible development and deployment methods.

These forecasts give us a range of tools to address the possible problems of the future. Let us adopt those tools, to realize the exciting promise of our technological future.

Provided by The Conversation

Citation: Futurists use a Delphi study to highlight top risks from technology that we'll be facing by the year 2040 (2024, January 24) retrieved 5 May 2024 from https://techxplore.com/news/2024-01-futurists-delphi-highlight-technology-year.html