Computer Outages*

Jayati Ghosh

It is a truth that should now be universally acknowledged that, everywhere in the world, our lives are driven by computers – or more specifically, by the workings of Information and Communication Technology (ICT) and therefore the internet. And our dependence on them is not just temporary or partial: it is continuous and overwhelming. It is not just people who actively use computers – whether on desktops or laptops or tablets or mobile telephones – whose lives are driven by them and by internet access. Increasingly, (and certainly in urban areas) almost all forms of transport, most forms of financial transaction, many forms of quotidian work and interaction, are reliant on the underlying operations of computer systems. As "the internet of things" quietly becomes more and more significant, the very gadgets that people use on a regular basis function on the basis of information collected, computed and transmitted in ways that are typically not even known to or grasped by the user.

All this has created new forms of dependency and vulnerability, which we do not fully recognise. The usual concerns that many people have about this domination of "smart" machines all around us relate to privacy, monitoring and surveillance, and of course the ever-present possibility of cyber fraud. These are certainly valid concerns. But the implications of a simple failure of a computer system – and outage or downtime – are somehow seen as less dire, probably because most people believe that such temporary collapses can be speedily rectified and dealt with, and that most computer systems have enough back up to resolve the ensuing problems quickly and relatively smoothly, without major disruption.

But now it seems that such a belief in the fundamental resilience (if such a word can be used) and reliability of systems based in cyberspace are not justified and could even be touchingly naïve. The latest example of the fragility of these systems has come with the collapse of the computer system of British Airways on 27 May 2017, which unleashed a complete shutdown of flights for a full day followed by huge numbers of cancellations, delays, chaos and confusion for several days thereafter.

According to British Airways, the computer system broke down because of a "power failure" – but surely that raises many more questions than it answers. How could an international airline company as large and established as British Airways not have a system of uninterrupted power supply, which is something even private individuals seek to ensure when they are dealing with data? Surely it would have had multiple servers in different locations? What about adequate back up, including on the "cloud", which must be the most obvious item on any computer system checklist? And was there no system in place to deal with such emergency contingencies to minimise their adverse effects?

If none of this was apparently in place for British Airways, people would be justified in feeling concerned about many other computers systems that are assumed to have adequate protection, back up and contingency planning. What about banks, for example, and credit card companies that have apparently experienced various nightmarish hacks and other cyber threats that are intentionally played down by the media to prevent panic? What about military systems, which are increasingly reliant

on software and computer programmes, and which we do not lose sleep over because we assume that sufficient precautions have been taken to cover all possible contingencies, even unexpected ones?

In fact, what has just happened at British Airways is not entirely unusual at all. In August 2016, a power breakdown at Delta Airlines mission control in Atlanta, Georgia in the US, caused massive disruptions, fight cancellations and delays. Apparently the switchgear that routes and distributes power failed – but significantly, in that case as well, the backup systems did not work, either because they were not properly in place or because some network operations that should have turned automatically to back up did not do so. The computer system was restored in six hours, although of course the knock on effect of the disruption continued for several days, because of the tightness of the prior flight schedules.

Sometimes the problem stems from issues at data companies to whom specific tasks are outsourced. Earlier this year, services at Britain's National Health Service were disrupted for several days because of a power outage incident at Capita data centre, which also affected various other companies that used them to provide online assistance and other computer services.

Not all computer breakdowns are as damaging and disruptive; this clearly depends on the service being offered. The collapse of Amazon Web Services in early March this year involved a power breakdown for eleven hours, which meant not just major slowdowns but complete unavailability of more than a hundred large online retailers and major websites like Amazon, Netflix, Reddit and others. While this clearly caused significant losses, this may not have been as dramatic and disastrous. But the very simplicity of the cause of the problem makes one pause: apparently the entire breakdown was caused by a typo! An employee engaged in routine maintenance to remove some of the smaller subsystem servers for billing incorrectly entered one wrong command, which brought down a large number of servers. That one human error could not be immediately corrected, and then the servers that had been brought down then took much longer to be recovered than anyone had anticipated. (Indeed, it seems that some of these servers have still not been recovered…)

Simple human errors have been responsible for other breakdowns as well, so far with less adverse impact. The internet start-up GitLab, which is a repository manager, was doing very well until it had a minor power outage that temporarily slowed down the system. While trying to fix the system, a system administrator accidentally typed the command to delete the primary database. Meanwhile the power outage had meant that the last back up was already six hours old – so some data was irretrievably lost, which for a repository is really bad news.

In these last examples, the point to note is not how bad the impact was (the final effect may not have been so terrible after all) but how minor and simple was the error that caused it. It underlines how ridiculously easy it apparently is to make entire systems come crashing down with just a minor and only too human mistake. It makes nonsense of the idea that these systems are meant to reduce the risk associated with the need for human intervention. In addition, obviously, the backup systems that would ensure that such things never cause any real impact, are simply not in place.

This may well be because maintaining such thorough and comprehensive backups that promise completely smooth and seamless transition when one system has failed, is expensive and would reduce profitability. And in these days of cost cutting, such expensive features that may never have to be used often seem to CEOs as unnecessary luxuries that companies can do without. Similarly, governments engaged in fiscal austerity are more inclined to cut corners in these crucial areas, especially if the probability of such a “black swan” event is rather low.

But that is all the more reason for all of us to be more worried than we are about our present state of vulnerability. It seems that attacks by cyber terrorists and hackers, or manipulation of data by bad guys, are not the only sources of possible collapse of the vast networks of computer systems that increasingly run our lives. It could just be some computer operative pressing the wrong key in a hurry – or on a bad hair day – that messes everything up.

* **This article was originally published in the Frontline Print edition: June 23, 2017.**