The Unsustainable Fragility of the Digital, and What to Do About It

Luciano Floridi[1]

Saturday, 27th of May 2017. An IT meltdown plunged into chaos British Airways' flights at Heathrow and Gatwick airports. More than 75,000 passengers, including your philosopher, were grounded, during the busy May Bank Holiday weekend. Apparently, the cause was a mere inadvertent cutting of power, followed by an unauthorised and incorrect restoration. It took three days to get back to normal. Discomfort and damage to passengers were incalculable. Costs were significant: £58 million in compensation. The loss of reputation was serious, especially in a highly competitive environment, with limited margins, such as that of airlines. The system crashed again on the 2nd of August, this time only temporarily.

Sunday, 28th of May 2017. First assessment of the damage caused by WannaCry. The malware hit Microsoft Windows systems, encrypting infected computer files and then asking for a ransom to decrypt them. This time your philosopher was safe, probably because he uses Apple systems. It is estimated that, at that date, WannaCry had already infected more than 230,000 computers (they will soon become 300,000) in 150 countries. It was one of the largest computer infections of all time. Among the affected organisations were Deutsche Bahn, FedEx, Telefónica, Renault, the Russian Ministry of Interior, and many others. In England, the National Health System (NHS) was forced to cancel appointments and send patients home. For a few days, we went back to paper and pen. Luckily, there were no casualties.

Two disasters. But also two good examples of how fragile the digital is, how wide and risky our dependence on it is becoming, and how systemic the problems caused by digital failures can be.

Fragility is not necessarily a bad feature all the time. It can also be a positive, even precious, quality, if, for example, we are talking about the delicacy of a crystal vase. But it becomes a problem when it denotes the unreliability of a system, and the more so the more we depend on it. So when the system in question is that digital sofa on which

✉ Luciano Floridi
luciano.floridi@oii.ox.ac.uk

[1] Oxford Internet Institute, University of Oxford, 1 St Giles, Oxford OX1 3JS, UK

our information society is increasingly couchpotatoing, we should really worry about it. We live in increasingly complex environments, which work only thanks to digital technologies. We fight complexity with even more complexity. Suffice it to think that, in 2025, 70% of the world's population will be urbanised. Cities may not become very smart very soon, but they are growing really fast and certainly becoming reliant on the digital to work, safely and securely.

Digital fragility is a serious issue. The question is whether anything can be done to make the digital less fragile and more reliable. Resignation is not a strategy. On the contrary, much can and should be done to strengthen the digital and ensure that the damage is at least limited, if not entirely avoided, whenever the "digital sofa" collapses under our bottoms. It is not too early to act on the fragility of the digital, and not just for individuals, but also for companies and institutions. Because the cost of doing nothing is now unsustainable.

Let's start with a classic solution: if the system collapses, there should be a backup that kicks in. It is called resilience through redundancy. Add one leg to the sofa, to use the previous analogy. Or make sure that there is at least one spare wheel, like in my old Vespa. The trouble with British Airways was to cut costs so radically that when the spare wheel was needed, it was not there. Unfortunately, just like in my new Vespa. In the case of personal systems, individuals have long had the experience of making a full and updated backup. If your computer is blocked by a malware, it is tedious, but you can format and reinstall a clean copy. If only it were so simple for the whole information society and the analogue world.

Another solution is "reflexivity". In digital systems, everything is zero and one: the operating system, the programs managed by the operating system, and the data manipulated by the programs. This is so obvious today that we take it for granted. Yet, it is quite amazing if you think of it for a moment. It is as if the driving system, the engine and the petrol of the car were all made of the same interchangeable substance. Or as if bottles and glasses were made of solid ice, and you could use them to pour and drink water. Thanks to such reflexivity, the digital is able to work with itself, on itself, for itself. WannaCry infected so many computers because too many did not have the necessary updates to block it, forgetting that reflexivity does indeed make the digital so fragile, since malware too is made of zeros and one, but it is also what allows the digital to defend itself, with an antivirus for example. The future will increasingly need the positive feature of digital reflexivity, without which we will not be able to protect the software of our driverless cars, for example. The next malware might be called WannaDrive and force us to walk. More generally, one solution to cope with the fragility of the digital is more digital, not less. The way forward is to have software that monitors, repairs, and improves other software.

And talking about cars, there is always a third, old-fashioned solution: insurance. According to a Financial Times article,[1] the cyber insurance market grew significantly after WannaCry. Unfortunately, we often shut the stable door after the horse has bolted. Today, the cyber insurance sector has a value of about $3 to $4 billion a year but, according to Allianz, it could easily reach $20 billion in 2025, becoming one of the fastest-growing segments in the insurance industry.

[1] https://www.ft.com/content/25bf97e8-3a27-11e7-821a-6027b8a20f23

Finally, we should not underestimate the usefulness of fragility itself. We constantly use it to our own advantage in the artefacts we build, by introducing fuses, valves, safety glasses, emergency break glasses, and lifesaving devices of all kinds. If something goes wrong, the system degrades in a calculated and limited way, and we know where and how to intervene. We should do the same thing with the digital. Accidentally, that is what happened with WannaCry. It is unclear why, but the malware had a peculiar feature: before infecting a computer, it checked whether a dark website had been registered. Following a negative response—the site did not exist—the malware infected the files. So a young British researcher registered the website. The result was surprising: the malware, finding that the URL had been registered, stopped infecting new computers. In other words, the creation of the website played the role of a kill switch. Similar measures involve the creation of so-called honeypots, virtual baits that provide apparently legitimate data, such as a website, that are safely isolated and monitored to detect and block attackers.

WannaCry caused huge economic losses. According to one estimate, they could reach up to $4 billion.[2] But in another sense, we got lucky. There were no human tragedies. Yet the alarm should be loud and clear. It is time that we all accept our responsibilities and act on them.

First, the organisations. For example, the National Security Agency was aware of the vulnerability in Windows that was exploited by WannaCry. They should have warned everyone as early as possible, and not kept it secret, in order to exploit it as a possible cyber weapon in the future. They launched the alarm too late, after the information had been stolen. How many other vulnerabilities are the spooks still hiding from us?

Then there are companies like Microsoft, which will have to become more accountable as the first line of defence. It is not acceptable to abandon old operating systems as no longer supported or patchable; because these are still used anywhere in digital environments and of course a chain is only as robust as its weakest ring.

And finally, there is ourselves, the users. We need to be more responsible because, just like in health care, a small percentage of unvaccinated people is at risk of endangering a whole population.

The digital can take care of itself, but like in all systemic contexts, the solutions work only if everyone collaborates. No matter how robust the other legs of the couch may be, if one is fragile, we will always end up getting hurt. And it will be just our fault.

[2] http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/