Aameen Patel *Highways England traffic controller*

Rt Hon. Liz Row MP *Foreign Secretary*

Jan Sikorski *Deputy Director at the Civil Contingencies Secretariat (CCS)*

Rt Hon. Harold Stuart MP *Defence Secretary*

Sir Jon Whewell *Cabinet Secretary*

PREFACE TO THE PAPERBACK EDITION

The hardback edition of this book was published in a different, more comfortable, pre-Covid-19 world. The global crisis through which we have all been living since that time has changed many things – some of them, in all probability, permanently. But there is one thing that it hasn't changed at all. The frenetic efforts of governments, businesses and communities to address the challenge of the virus have done nothing to resolve – have, if anything, further obscured – challenges that are only a little further off.

Although this is entirely understandable, and perhaps temporarily inevitable, it exposes us (with crushing irony) to the very same danger that has afflicted the whole world in the face of the coronavirus: the danger of being under-prepared for an event whose colossal impact is ignored because the likelihood of it happening today

or tomorrow is low. Once again, both the world's leaders and the world's populations are focussing on the present. Once again, we are paying far too little heed to building resilience against the threats of the future.

This book is about one of the most obvious, but also one of the most neglected, future threats: the threat of network collapse. It presents strong reasons for believing that we need, now, to guard against this threat, and to do so in a way that is flexible, formidable and foolproof.

Much of the book is just as applicable to the world's past lack of preparedness for Covid-19 as it is to the world's current lack of preparedness for network collapse. A large part of the analysis is devoted to explaining why we all (governments, businesses, media, people at large) find it so difficult to consider small probability, large impact threats with the seriousness they deserve – until they actually arrive on the scene, at which point we spend so much time and effort attending to the current catastrophe that we run the serious risk of ignoring the next threat along the line.

So part of the point of the book is to urge that we should learn the lessons of history in the right way. Instead of assuming that the next crisis will be substantially the same as the last one, or that we have now 'had' crises, we should assume instead that a series of crises (each, in themselves, unlikely but serious in their impacts) will come at us – generally from unanticipated directions.

We should assume that our defences against them, however well-constructed, will sometimes prove inadequate, because we cannot expect to construct adequate defences against unanticipated causes.

None of this, however, should make us pessimistic, let alone despairing. On the contrary, the moral of this book is that if we take appropriate steps to prepare ourselves for dealing with crises that have occurred despite our best defences against them, then we can in fact get through them with reasonable aplomb. The art of crisis management is to have means to hand of mitigating the problems we cannot prevent, and of being well prepared to deploy those mitigations in the face of disconcerting circumstances. There is no rule book, no text book, no recipe that will provide all of the answers in advance. Life as we know it in peacetime cannot be preserved, unaffected in wartime. But we can get through most kinds of war without too many dead at the end, if we know how to make do and mend, and if we have had the foresight to furnish ourselves with the rudimentary means of doing so.

It is in this spirit that I hope the recommendations made in this book for the construction of analogue fallbacks to handle digital crises will be read and understood. They are, I believe, a necessary feature of any resilient society in a modern age hugely dependent on a network of networks. But they are also a paradigm for the sort of preparation that humanity at large, and each country's

government in particular, should make for dealing with events that we hope not to witness, may never witness, and yet which need to be recognised as possibilities rather than dismissed as fantasies.

Oliver Letwin
October 2020

PROLOGUE

Midnight, Thursday 31 December 2037

Aameen Patel may have been the first person to notice. Everyone else in Integrated Traffic Control at Highways England's Swindon HQ was either snoozing or drinking coffee in the lounge area. But Aameen had arrived at 23:45 for the midnight to 06:00 shift, and had just turned on his screen. He cursed silently when it went blank. With all this advanced technology, why couldn't they make sure computers worked on New Year's Eve?

He obviously couldn't report the fault using the normal Skype-view on his blank terminal, so he reached for his i16 to call the IT people. He was so focused on trying to remember the number that he didn't at first take in that the signal-indicator wasn't showing any bars.

It was at this point, he later remembered, that the

that the billions spent on defending key networks may actually fail to preserve normal operation under attack conditions.' Of course, in any rational world, the minister would go on to explain that this was merely an inevitable fact, since no defence, however elaborate, well planned and well funded, can possibly be perfect. But the media circus that surrounds governments and large businesses is not rational; it sweeps people and arguments along in a great tide of emotion, and the losers are people who have long, rational answers to short, irrational questions. Senior figures in any government are well aware of this and are therefore naturally reluctant to indulge in speculation about failed defences and fallback options.

The way out of this bind is for governments to seize the initiative at times when there is no crisis and not even any whiff of crises to come. By proactively announcing that fallback options are being added to investment in defence, and by describing this as a 'second-line of protection for the economy and society', ministers can protect themselves against lurid accusations of defeatism and panic, and can instead (accurately) represent the recognition of the possibility that the first (defensive) line of protection may fail as a strength rather than a weakness of their approach. By acting in this way, they can also create sufficient public understanding of fallback options to avoid damaging and inaccurate media stories later about 'secret plans to deal with expected network failure': plans

that are announced cannot be secret, and what is not secret is not much of a story.

From probability to scenario analysis

Once a 'red' team has been established to look at fallback options to cover failure while the 'green' team works on improving network defences to prevent failure, the 'red' team needs to adopt a method of working that is wholly different from the way the 'green' team works.

When you are designing and building defences to protect modern networks, you need to start with probability analysis – because you can't afford to protect the networks against every conceivable form of attack, and it therefore makes sense to protect them against the most likely forms of attack. Of course, the 'green' team needs to be conscious of all the points about misleading statistics that were made in earlier chapters of this book; but the fact remains that statistics – and the assessment of probability that statistics make possible – are an invaluable part of the 'green' team's equipment.

By contrast, the 'red' team, which is designing fallback options to be used if there is network failure, should *totally avoid any reference to statistics and probabilities.* It should focus remorselessly on worst-case scenarios, without worrying in the least about how likely these are to occur. This ought to be obvious – but it will seem

quite counter-intuitive in any established bureaucracy, because established bureaucracies are used not only to cost–benefit analysis of the sort that is so destructive of fallback-option planning but also to the allied pursuit of probability analysis. It becomes a habit in any well-trained bureaucracy to consider probabilities before taking action. But the 'red' team has to overcome this habit. It has to recognize that the whole point of fallback-option planning is to quit worrying about how likely it is that network failure of any particular kind will occur for any particular reason, and to concentrate instead on how to make society and the economy capable of carrying on in a half-way reasonable fashion if and when network failure does occur. So probabilities don't matter to the 'red' team doing the work on fallback options. What should matter to this team is only the ability of the state and society to handle serious persistent network failure in a reasonably robust way.

Another way of putting this is that the 'red' team doing the fallback-option planning needs to use scenario analysis instead of probability analysis.

It is worth emphasizing this point, because serious scenario analysis is unusual in any government, and involves habits of mind that are not frequently found outside the military. It is fairly straightforward to slap down on a piece of paper a broad scenario, and then proceed without much further analysis to construct a fallback option that

will apply in the event that this scenario becomes real. But serious scenario analysis involves much more than this. It means working through the ramifications and consequences of the scenario – understanding the full range of what is likely to go wrong if modern convergent networks fail. And this includes not just administrative issues but also the human dimension – the effects on people who are living through the network failure. In other words, it means constructing stories like the story told in this book, and then thinking through how to enable people to live through such stories in a way that gives the story a different and better ending. That is a work of imagination which will not come naturally to any bureaucracy that is attuned to considering systems and statistics rather than stories and human consequences.

The value of trial and error

This need for the 'red' team to step outside the normal, bureaucratic mind-set when analysing scenarios is closely allied to another unusual requirement for successful fallback-option planning: a willingness to proceed on the basis of trial and error.

Because fallback options are by definition not the way we go about our business most of the time in our ordinary lives, they can't be refined through the experience gained from daily use, in the way that is now usual