Technology and Regulation

special issue: security in the digital age

Risk and uncertainty in the digital ecosystem

Author(s)	Bibi van den Berg
Contact	b.van.den.berg@fgga.leidenuniv.nl
Affiliation(s)	Bibi van den Berg is Professor of Cybersecurity Governance at Leiden University, the Netherlands.
Keywords	Uncertainty; Risk; Risk management; Cyber risk management; Preparedness; Security by Design; Digital Econosystem; Cybersecurity, Cyber Resilience, Knightian Uncertainty
Published	Published: 31 Mar 2026
Citation	Bibi van den Berg, Risk and uncertainty in the digital ecosystem, Technology and Regulation, 2026, 10-27 • 10.71265/veh8cc91 • ISSN: 2666-139X

Abstract

Humans struggle with uncertainty, and risk management has been developed to tame it. It is used in many different contexts including the digital ecosystem. But is risk management suitable for addressing cybersecurity challenges? In this article, we will delve into the difference between risk and uncertainty to find the types of challenges for which risk management works well, and the types of uncertainty for which it falls short. The 'risk-uncertainty' scale will help us clarify this distinction. Next, we will zoom in on the digital domain. Cyber risk management can be brought to bear on specific cybersecurity challenges, but we must supplement it with other approaches. In this article, we will discuss two: preparedness and Security by Design.

> "It is a world of change in which we live, and a world of uncertainty. We live only by knowing *something* about the future; while the problems of life [...] arise from the fact that we know so little."[1]

1. Frank H Knight, *Risk, Uncertainty and Profit* (1921) 199, emphasis in the original.

1. Introduction

Risk and uncertainty have preoccupied human beings for many centuries, but never as much as today.[2] Until the Middle Ages, whenever humans were struck by disasters, they explained such crises by referring to divine intervention, bad luck or fate or some other power outside their own control. As Bernstein explains in *Against the gods*, this changed during the Renaissance because of a combination of different developments, the most important of which was a breakthrough in mathematics that laid the foundation for probability theory and statistics.[3]

Probability theory enabled humans to start thinking about a future in which things *might* happen, as something that involved chances rather than fates. This was a big change. When one views life as predestined or ruled by outside forces, the future is a dense fog, which at any moment may reveal unexpected challenges or lucky breaks along the way. But with the invention of probabilistic reasoning and statistics, a possibility emerged to start thinking about the future as a horizon towards which one could travel via different trajectories, as a path over which humans could exert some level of control, of influence. Risk thinking was born: the idea that we might be able to establish the likelihood of future events, and that we could engage in efforts to influence future events, either by reducing the likelihood of their materialisation, or by altering or affecting the consequences of these events.

In the centuries after we used risk thinking to increase our insulation against a wide variety of random hazards of life. We built safer houses and developed medicine to protect us from diseases. We increased food safety and developed financial safety nets such as insurance and social security plans for a rainy day. As a result, according to some scholars, objectively measured we have never been safer than we are today.[4] At the same time, interestingly enough, never before in history have we been more aware of risks, have we been more concerned about bad things happening to us, and have we been less tolerant of risk.[5] And never before in history have we been more afraid. At least part of this may be due to more knowledge and more information.[6] In contrast with previous generations, humans today have a better understanding and much more knowledge of the risks of life: of potential diseases, of financial risks, or the risks of drugs, of crime, of terrorism and wars, and of natural disasters. Moreover, risk thinking induces identifying risk, i.e. looking for things that could potentially cause harm in the future. Perhaps actively searching for risks also leads to seeing ever more of them in different domains?

In any case, over time in the past centuries risk thinking has consolidated into a structured approach to understanding and responding to risk, called risk management.[7] Today, risk management is *the* dominant paradigm for thinking about and dealing with risk.[8] Uncovering, scoping, determining, treating, monitoring and governing risks – whether it be in relation to our finances, our physical safety, our health, or be related to crime and violence, or even (geo)political tensions and wars – have become core activities in Western society. It is what preoccupies us, perhaps, more than anything else.[9]

2. Peter L Bernstein, *Against the Gods: The Remarkable Story of Risk* (John Wiley & Sons Inc 1998) 400; Ulrich Beck, 'Living in the World Risk Society' (2006) 35 Economy and society 329; Michael Power, *The Risk Management of Everything: Rethinking the Politics of Uncertainty* (Demos 2004); Deborah Lupton, *Risk* (2nd edn, Routledge 2013) vii.
3. Bernstein (n 2).
4. Steven Pinker, *Enlightenment Now: The Case for Reason, Science, Humanism and Progress* (Allen Lane - Penguin Random House UK 2018); Hans Rosling, Ola Rosling and Anna Rosling Rönnlund, *Factfulness: Ten Reasons We're Wrong about the World -- and Why Things Are Better than You Think* (First edition, Flatiron Books 2018) x; Bibi Van den Berg, 'The Need for Safety and Security' in Chrząstowski Szymon Vetere Arlene (ed), *Safety, Danger and Protection in the Family and Community: A Systemic and Attachment-Informed Approach* (Routledge 2023).
5. Lupton (n 2); Power (n 2).
6. Pat O'Malley, 'Governmentality and Risk' in Jens O Zinn (ed), *Social Theories of Risk and Uncertainty* (Blackwell 2008).
7. Terje Aven, *The Science of Risk Analysis: Foundation and Practice* (Routledge 2020) xii; Sylwia Przetacznik, 'The Evolution of Risk Management' (2022) 53 Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej w Tarnowie 95.
8. Bibi Van den Berg, Pauline Hutten and Ruth Prins, 'Security and Safety: An Integrative Perspective' in Gabriele Jacobs and others (eds), *International Security Management: New Solutions* (Springer 2019); Bibi Van den Berg, 'Dealing with Uncertainty in Cyberspace' (2024) 144 Computers & Security 1; Enrico Zio, 'The Future of Risk Assessment' (2018) 177 Reliability Engineering & System Safety 176; Lupton (n 2); Bernstein (n 2).
9. Beck (n 2); Anthony Giddens, 'Risk and Responsibility' (1999) 62 The Modern law review 1.

The advent of digital technologies has led to the emergence of a whole new realm of risks and risk-related concerns. Risk management thus has also become a cornerstone activity for organisations and governments in relation to the digital ecosystem in the past decades. 'Cyber risk management' or 'digital risk management' is now a well-established branch of the tree of enterprise risk management,[10] and is also a *sine qua non* for (inter)national security for many governments and the international arena.[11]

At the same time, the convergence of risk management and the digital domain also has its critics. According to some, risk management has been uncritically adopted to realms in which its effects are suboptimal, or at least unproven.[12] According to others, digital ecosystems have specific characteristics that make them unsuitable for effectively responding to risk using traditional risk management methods.[13] Meanwhile, decision makers still consider (cyber) risk management the gold standard to ensure the security of their organisations,[14] auditors still check companies' digital security maturity using cyber risk management frameworks and standards,[15] and (EU) regulators all push for more 'risk-based' legislation in the field of digital technologies.[16] [17]

How do we reconcile the opposing views on cyber risk management? In this article, we delve into the strengths and weaknesses of cyber risk management and risk-based regulation, to establish under which conditions these approaches have merit, and where their limits lie. At the end of the article, suggestions will be made for additional tools that could be used to resolve some of the risk- and uncertainty-related challenges in relation to networked, digital technologies.

2. Stepping back: risk and uncertainties

The notion of risk is closely related to that of uncertainty. Sometimes, the two terms are used interchangeably. This is understandable, because both pertain to events that may happen in the future, but need not necessarily do so. Risky or uncertain events are events of which we do not know when, if ever, they will take place. Both involve future-oriented thinking.

10. Alan Calder and Steve Watkins, *IT Governance: An International Guide to Data Security and ISO27001/SO27002* (5th edn, KoganPage 2015); Nist, 'Managing Information Security Risk (Special Publication 800-39)' (NIST (National Institute of Standards and Technology) 2011); Jan Meszaros and Alena Buchalcevova, 'Introducing OSSF: A Framework for Online Service Cybersecurity Risk Management' (2017) 65 Computers & Security 300.
11. Zachary A Collier and others, 'Cybersecurity Standards: Managing Risk and Creating Resilience' (2014) 47 Computer 70; Lee A Bygrave, 'Security by Design: Aspirations and Realities in a Regulatory Context' (2022) 8 Oslo law review 126; OECD, 'Digital Security Risk Management for Economic and Social Prosperity' (Organization for Economic Co-operation and Development (OECD) 2015) https://www.oecd.org/en/publications/digital-security-risk-management-for-economic-and-social-prosperity_97892642454 71-en.html; OECD, 'Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security' (OECD Legal Instruments 2024) OECD/LEGAL/0312 https://legalinstruments.oecd.org/public/doc/116/116.en.pdf accessed 9 May 2024; A Mouco, BL Ruddell and S Ginsburg, 'Resilience to High Consequence Cascading Failures of Critical Infrastructure Networks' (The Sam Houston State University Institute for Homeland Security 2023) https://doi.org/10.17605/OSF.IO/5R2H6.
12. Power (n 2); Douglas W Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It* (2nd edn, Wiley 2020).
13. Myriam Dunn Cavelty and Jennifer Giroux, 'The Good, the Bad, and the Sometimes Ugly: Complexity as Both Threat and Opportunity in the Vital Systems Security Discourse' in Emilian Kavalski (ed), *World politics at the edge of chaos: Reflections on complexity and global life* (SUNY Press 2013); Deirdre K Mulligan and Fred B Schneider, 'Doctrine for Cybersecurity' (2011) 140 Daedalus 70; Van den Berg, 'Dealing with Uncertainty in Cyberspace' (n 8).
14. C Brumfield, *Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework* (John Wiley & Sons 2021); S Moyo, *Executive's Guide to Cyber Risk: Securing the Future Today* (John Wiley & Sons 2022); Przetacznik (n 7).
15. Georg Disterer, 'ISO/IEC 27000, 27001 and 27002 for Information Security Management' (2013) 04 Journal of Information Security 92; Calder and Watkins (n 10); Gregory J Touhill and C Joseph Touhill, *Cybersecurity for Executives: A Practical Guide* (John Wiley & Sons 2014); Sergeja Slapničar, Micheal Axelsen and Marc Eulerich, 'Cyber Risk Management: An Illusion of a Risk-Based Approach' [2025] Journal of management control http://dx.doi.org/10.1007/s00187-025-00401-z.
16. European Commission, 'The EU's Cybersecurity Strategy for the Digital Decade' (High Representative of the European Union for Foreign Affairs and Security Policy 2020) JOIN(2020) 18 final https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:52020JC0018 accessed 9 May 2024; Bygrave (n 11).
17. Examples of 'risk-based regulation' in the EU include the General Data Protection Regulation (GDPR) and the AI Act.

However, the terms risk and uncertainty do not overlap entirely.[18] For one, risks have a ring of calculability in them,[19] of an ability to establish the likelihood with which particular events will materialise in the future. For uncertainties such quantification is fundamentally impossible.[20] In the next section, we will delve more deeply into the intricacies of why this is the case. Second, to establish the size of risks, i.e. to calculate the likelihood of their materialisation and the impact such materialisation may have, we use the past. We look at similar events in the past to understand impacts and to establish how often a certain event may occur again in the future. As we will see below, this method cannot be used successfully for uncertainties. Finally, one element of risk-thinking is that we as humans can exert (some form of) influence over them: we can come up with interventions to reduce the likelihood of their materialisation, or we can come up with measures to reduce their impact, or both. This by no means entails that we can 'solve' all risks, but the term risk *management* reveals that there is an underlying belief in the manageability of such future events. Sometimes perhaps our abilities to influence risky future events may be marginal, but there is always at least something we can try to do to address them. For uncertainties, it is questionable whether this is the case. Let us delve deeper into the distinction between uncertainties and risks now.

2.1 Subways and coconuts

To clarify the distinction between uncertainty and risk in more detail, as a first step we will build on an article called *Forecasting and uncertainty in the economic and business world* by Makridakis, Hogarth and Gaba.[21] In this article the authors discuss two different types of uncertainty which they label 'subway uncertainties' and 'coconut uncertainties'. To explain the former, Makridakis *et al.* say, let us assume that a person always travels to work on the subway, and that this person would start to keep a record of how long it takes them to reach their workplace every day. Over time, these records will reveal some variations in travel times, for example because they sometimes have to wait a little longer for a train to arrive, or because it may take just slightly longer to get to the subway station.[22] However, as long as no big disturbances occur, the variation in travel times will in all likelihood be small. There is uncertainty involved with every time this person travels to work and back; after all, there is no guarantee in advance that the travel time will be completed in exactly the same amount of time. But if one were to plot the variations in the recorded travel times in a graph, a Bell curve, or normal distribution, would be the result. Based on observations of past travel times, over time, statistical predictions could be made of how long the journey would take on each given day, and these predictions would be quite accurate, at least so long as no big changes occur in the pattern.

Note that the class of subway uncertainties has three characteristics. First, with subway uncertainties the future resembles the past; there are minor variations in outcomes only, which over time, as we gather more data, increases our ability to predict future events with a measure of accuracy. Second, subway uncertainties are 'simple', or bounded, in the sense that there is a limited set of variables at play in generating certain outcomes. Third, subway uncertainties occur in (reasonably) predictable patterns, at least so long as no great disturbances occur.[23]

Contrast this with the other kind of uncertainties, which Makridakis *et al.* call 'coconut uncertainties'. This term refers to a fictional story of a man who travels to a tropical island on a trip with his family.[24] Before he left, he tried to think through and mitigate all the potential things that could go wrong on the trip. Yet tragically, on vacation he is hit on the head by a coconut falling from a tree, and he dies. How unlucky can a person be? Coconut uncertainties are "rare event[s] with critical consequences".[25] Because such events

18. K Francis Park and Zur Shapira, 'Risk and Uncertainty', *The Palgrave Encyclopedia of Strategic Management* (Palgrave Macmillan UK 2017).
19. Anette Mikes, 'From Counting Risk to Making Risk Count: Boundary-Work in Risk Management' (2011) 36 Accounting, organizations and society 226.
20. Knight (n 1).
21. Spyros Makridakis, Robin M Hogarth and Anil Gaba, 'Forecasting and Uncertainty in the Economic and Business World' (2009) 25 International journal of forecasting 794.
22. Makridakis, Hogarth and Gaba (n 21) 802.
23. Obviously, these three characteristics are closely related and strengthen one another: because there are fewer variables, there are also fewer variations, and because of both the chance of disturbances in the pattern is reduced. Similarly, because there are few variables, patterns can be discerned and hence the future resembles the past. Etcetera.
24. Spyros Makridakis, Robin M Hogarth and Anil Gaba, *Dance with Chance* (Oneworld 2009).
25. Makridakis, Hogarth and Gaba (n 21) 803.

are rare, we do not expect them – or oftentimes do not even consider them a possibility. However, while it is highly unlikely that a person is killed by a coconut falling on their head, at the same time the class of rare events is actually vast. Highly unlikely events occur all the time. Earthquakes, terrorist attacks, financial crises and chemical spills all are examples of coconut uncertainties: although rare, all of these events can strike at any point in time with destructive consequences. When they do, they surprise us, because we tend to overlook the possibility of their occurrence in everyday life. As Maktridakis *et al*. explain, therefore, this type of uncertainty "defies all attempts at measurement."[26] They "remain totally and utterly unpredictable."[27]

In contrast with subway uncertainties, coconut uncertainties lack patterns, are far from simple, and are the result of the interplay between a large set of different variables. Coconut events are so rare that we cannot model them. We lack the data to make predictions on them, and if we would try to plot them into a graph, the result would be a scatter pattern: such events may happen randomly, with no discernible order. Oftentimes their occurrence depends on an unlikely conjunction of a range of different factors. This means that the complexity of predicting them, even remotely adequately, becomes too big. Too many factors are involved in their materialisation, each of which itself usually also has all sorts of dependencies.

What sets subway uncertainties and coconut uncertainties apart is the fact that while subway uncertainties have some degree of uncertainty in them, they are also quite predictable and can be modelled. Coconut uncertainties, by contrast, are so rare and unique that they cannot be modelled, and it is even very difficult to envision them.

2.2 A priori, statistical and Knightian uncertainties

The separation of uncertainties into subway and coconut uncertainties overlooks one more type of uncertainty – one that is actually crucial to our understanding of the strengths and weaknesses of risk management. To shed light on this, we will look at the work of the 20th century economist Frank Knight, who makes a distinction between three types of uncertainty.[28] According to Knight, 'a priori uncertainties' are those uncertainties for which we can make solid predictions using probability theory. He calls them 'a priori' uncertainties, because the distribution of potential outcomes in the future is known, either in principle or in actual fact.[29] What sets a piori uncertainties apart is that we know in advance all potential outcomes, and the set of potential outcomes is finite. Because of this, we can precisely calculate the future odds of each particular outcome. Throwing dice is an example in case. We know that dice have six sides, so the likelihood of throwing the number 3 is always 1 in 6, that is if the dice has no imperfections. After all, there are only 6 potential outcomes in this example, and with each time the dice are thrown, one of these outcomes materialises. As Jarvis explains, "[w]hat is unique about a priori probability for Knight, [...] is that it speaks to a defined classification of instances. The risk outcomes are known and there is no possibility of deviation from these save for nefarious activity in terms of rigging the dice."[30]

Contrast this with the second type of uncertainties, which Knight calls 'statistical uncertainties'. In the case of statistical uncertainties, the distribution of potential outcomes in the future is not known, but we may learn about this distribution through empirical observations using inductive reasoning.[31] While such empirical observations may help us get a more solid understanding of the distribution over time, we will never be able to predict the future precisely, because the number of observations needed to reach that point is infinite – we may, as a matter of principle, always encounter an observation that does not align with our previous ones. Hence the term 'statistical uncertainty': making predictions for future events of this type involves estimation and an error bar. Subway uncertainties are statistical uncertainties: with each time the person makes the trip to work and back, (s)he may gather more data on the duration of the trip. So long

26. Makridakis, Hogarth and Gaba (n 24) 217.
27. Makridakis, Hogarth and Gaba (n 24) 223.
28. Knight (n 1).
29. Mikes (n 19).
30. Darryl SL Jarvis, 'Theorising Risk and Uncertainty in International Relations: The Contributions of Frank Knight' (2011) 25 International relations 296, 304.
31. David M Townsend, Richard A Hunt and Judy Rady, 'Chance, Probability, and Uncertainty at the Edge of Human Reasoning: What Is Knightian Uncertainty?' (2024) 18 Strategic entrepreneurship journal 451.

as no major disturbances appear in the pattern, the accuracy of this person's statistical predictions will grow over time. However, there will always be a degree of uncertainty in each specific trip because of the occurrence of minor variations.

Finally, the third category that Knight distinguishes has come to be known as 'Knightian uncertainty' in later works.[32] [33] We encountered this kind of uncertainty above under the banner of coconut uncertainties. For this type of uncertainty, there is "*no solid basis of any kind* for classifying instances", according to Knight.[34] This type of uncertainty is unmeasurable in principle, because "distributions are nonexistent".[35] As Townsend *et al*. explain, "the events in question are too dissimilar and, therefore, cannot be grouped into the same probability set as other events".[36] [37] As we have seen, this type of uncertainty often catches us by surprise, because we did not even consider it as an option – it is that rare and unusual. Nassim Taleb's 'black swans'[38] are Knightian uncertainties: they are outliers, events with a big impact that are so unusual that we find it hard, if not impossible, to envision them, so that they surprise us when they materialise. What characterises black swans, Taleb points out, is that we tend to use hindsight bias to explain that we *could* have actually seen this surprise coming.

Note that while we may not be able to calculate such future events, they still play a large role in our imaginations of the future, and we tend to worry over them quite a bit. Governments seek to take measures to prevent terrorist attacks, individuals seek to protect themselves against high costs for cancer treatment through health insurance, and organisations take protective measures against cyber attacks by state actors, despite the fact that they do not know when, if ever, these events will take place in their context, and these risks cannot be quantified in any way. The possibility of these events is sufficient for us to have concerns over them.

2.3 A desire for perfect predictability through quantification

Which of these types of uncertainties do we call 'risks'? And which of these types of uncertainties are, and can be, managed through risk management? Let us begin with the former. Framed within the division by Makridakis *et al*., subway uncertainties are risks, but coconut uncertainties are not. Subway uncertainties are quantifiable and we have sufficient data to make (reasonably) adequate predictions about them. For coconut uncertainties we lack such data, and coconut events are so rare that we lack the methods to do mathematics on them.

When we plot the difference between risks and uncertainties onto the division made by Knight, then risk refers to *both* a priori and statistical uncertainties, while Knightian uncertainty refers to 'real' uncertainty. Knight's division reveals something important: the term 'risk' may sometimes refer to future events for which we know the distribution, and which we can predict well. Take, for instance, the tossing of a coin. Each time we toss a coin, the outcome will be heads or tails. While we do not know in advance which outcome will materialise with each toss, we can calculate the probability of each outcome precisely, at least when the coin is perfect. But as we have seen, the term 'risk' may also be used for subway uncertainties: for future events of which we have an understanding of the distribution based on observations of past events that are similar, but not perfect knowledge. For such uncertainties we can use statistics and the more data we have from the past, and the more the past resembles the future, the better we can make predictions for that future.

---

32. Mikes (n 19); Jarvis (n 30); Townsend, Hunt and Rady (n 31).
33. Knight himself calls this type of uncertainty 'estimates', because in business contexts decision makers often tend to take courses of action under this type of uncertainty, using guesswork and subjective assumptions as their main guidance. However, the term 'estimate' can be confusing when used in other contexts of this type of uncertainty, especially when speaking of *non-intentional* unique occurrences with critical consequences, such as the Great Depression (1929-1934) or the invention of the internet.
34. Knight (n 1) 221, emphasis in the original.
35. Mikes (n 19) 242.
36. Townsend, Hunt and Rady (n 31) 457.
37. For Knight, who was an economist, interestingly, most business decisions regarding the future involve this type of uncertainty, and so does most human conduct. See page 226 of *Risk, Uncertainty and Profit*.
38. Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (Penguin Books 2008).

Note because a priori and statistical uncertainties are lumped together into the single term 'risk', this category brings together two quite different phenomena. First, risk refers to events and patterns that we can predict precisely and numerically, on the basis of established facts. Second, risk refers to estimations of the likelihood that events will occur, based on past experiences, which we may predict with some measure of likelihood yet that may also involve quite a significant measure of uncertainty. Tossing a coin involves a definitively measurable uncertainty, whereas predicting a storm has a much greater degree of uncertainty, even though we know from past experiences how storms develop, have large data sets with weather events in specific locations, and understand the scientific principles of how storms develop and follow a trajectory. Predicting a storm is a statistical uncertainty, because we use empirical data from the past to predict the future, but the error bar of getting such a prediction right is huge, since there are many variables involved and the variations between the past and the future may be big as well.

2.4 The risk-uncertainty scale

The term 'risk' thus actually describes a *range* of calculable events in the future, some of which we can calculate precisely, and others not so precisely, or actually pretty sloppily. The entire range is called risks, however. This is problematic, because by using a single word to capture this variety the qualitatively different nature of a priori and statistical uncertainties is hidden. All risks are treated in the same way: as calculable, full stop. As a matter of fact, oftentimes when speaking of risks two assumptions come into play. First, that having a store of data enables us to calculate risks *precisely*; and second, that risks are straightforward or '*simple*' uncertainties, with few variables and minor variations only. Or to phrase it differently: when speaking of risks we often assume they are 'a priori subway uncertainties' – calculable with exact probabilities. In our way of speaking of risk, the optimistic promise of calculability, which stems from a priori uncertainties, is transferred onto statistical or subway uncertainties, with a silent promise that 'if only we have more time and more data in the future' such uncertainties will be calculable with exactly the same certitude as knowing the outcome of rolling the dice or tossing a coin.

To make matters worse, especially in our everyday speech we tend to add coconut uncertainties, or Knightian uncertainties, into the mix as well when speaking of risks. Rare events that we cannot predict, such as terrorist attacks, earthquakes, chemical spills or large-scale internet outages, are then pulled into the domain of risks and treated as maybe a more complex but definitely a manageable type of future event. Here, too, the idea of calculability lures us into believing that if we gather enough data we might, someday, just be able to do the maths on coconut uncertainties – and with that calculation get more control over them, tame them somehow.

The figure below summarises what I will call the *risk-uncertainty scale*.

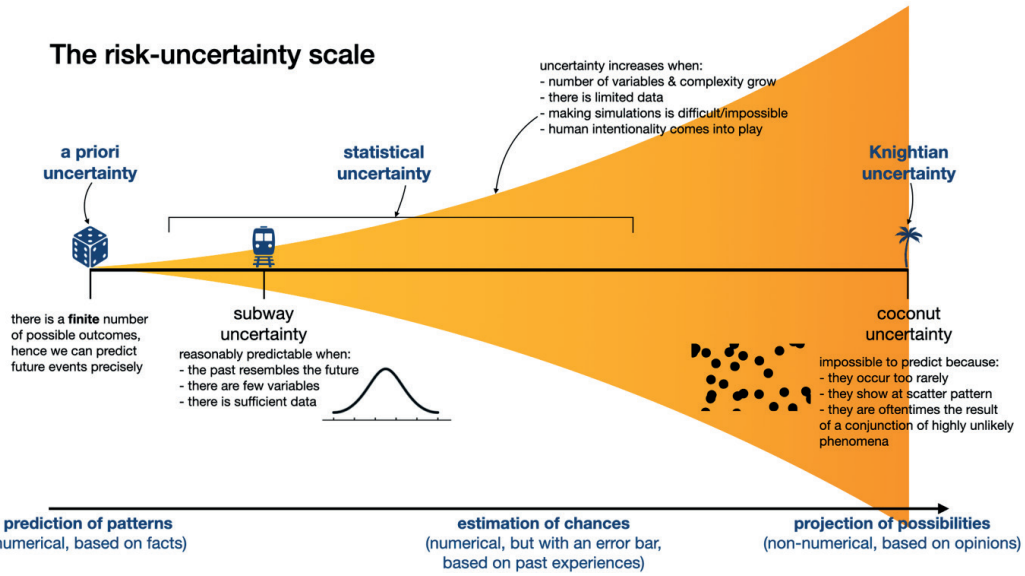

Figure 1: The risk-uncertainty scale

Where a future event falls on the scale, is determined by four elements. First, there is the issue of *complexity*. The 'simpler' the event, the more to the left it falls in the model. 'Simple' events oftentimes occur on a limited scale, there is a limited number of relevant variables in play, and there are limited connections with e.g. other systems. The complexity of these kinds of events is conceivable to us; we can foresee the potential outcomes at play. All the way to the left we find events with a finite number of variables and outcomes. These can be predicted precisely using probability theory. Next are subway uncertainties: uncertainties that display a regular pattern with minor variations, and that have few variables. Towards the middle the complexity increases: the scale of and impact of events increases,[39] we can no longer foresee all potential consequences,[40] there is a large number of variables, and increasing interconnectedness and dynamism vis-à-vis other events and systems.[41] Beyond a certain point, which is impossible to pinpoint exactly, the complexity is such that we cannot make adequate predictions anymore.

Second, there is the issue of *data*, both in terms of availability and in terms of quality. For statistical uncertainties the rule is: the more data that is available, and the higher the quality of the data, the more accurate our predictions of the future will be – so long as the future resembles the past. Generally, data availability and data quality are at least loosely correlated with complexity. This means that in the figure, the further to the right the event falls, the fewer (good) data is usually available. Without a large volume of high-quality data, calculating uncertainty becomes difficult, if not outright impossible.[42]

Third, making predictions for the future is solidified using *simulations* and other forms of modelling. In simulations we can play with variables and discover the different outcomes this will lead to, and – most importantly, this play is risk-free. Because we engage in scenario-thinking in a virtual environment, disastrous outcomes will not lead to actual harm. The better the simulations that we can run, the more solid our ability to predict future events. In the figure, events that can be modelled or simulated well fall on the left side of the scale, whereas events for which the use of modelling or simulations is more complicated or even outright impossible are on the right-hand side.

Finally, the role of human *intentionality* cannot be underestimated. In 1937 John Maynard Keynes wrote that the "prospect of a European war is uncertain, or the price of copper and the rate of interest twenty years hence, or the obsolescence of a new invention, or the position of private wealth owners in the social system in 1970. About these matters there is no scientific basis on which to form any calculable probability whatsoever. We simply do not know."[43] One of the key reasons why we do not know these things is because of the role of human agency. The choices that individuals or collectives may make in all these examples will have an impact on the outcomes of events in the future. Whenever the wilful decisions of individuals or groups of people are involved in the events we seek to predict, this complicates predictions, and in many cases pushes such uncertainties into the domain of Knightian uncertainties. Hence, on the left side of the figure we find events in which human intentionality plays no role or only a very limited role. The further we move to the right, the more relevant the role of intentionality often is.

2.5 Risk management

What are the implications of the conflation of a priori, statistical and Knightian uncertainties into the singular notion of risk for risk management? Where does risk management fall on the risk-uncertainty scale? And what can risk management deliver for the digital ecosystem and other domains?

Risk management can be defined as the activity of seeking to set "the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues."[44] Stories of the origins of risk management diverge. It appears that risk thinking blossomed into a structured approach in different

39. Jens Rasmussen, 'Risk Management in a Dynamic Society: A Modelling Problem' (1997) 27 Safety science 183.
40. Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Basic Books 1984) x.
41. Terje Aven and Marja Ylönen, 'A Risk Interpretation of Sociotechnical Safety Perspectives' (2018) 175 Reliability Engineering & System Safety 13.
42. Slapničar, Axelsen and Eulerich (n 15).
43. John Maynard Keynes, 'General Theory of Employment' (1937) 51 The Quarterly Journal of Economics 209, 214.
44. Heinz-Peter Berg, 'Risk Management: Procedures, Methods and Experiences' (2010) 1 Reliability: Theory & Application 79, 81.

realms, most notably in finance,[45] in public health,[46] and in safety science, for instance in relation to the nuclear industry[47] and the automotive and airline industries.[48] As we have seen above, risk management is also the go-to for many organisations when dealing with their digital risks or cybersecurity. By now, it may be clear that the underlying worldview of risk management is an attempt to gain a sense of control with respect to uncertainty by making future events predictable, by anticipating such events and treating them accordingly.

Risk management is a process that consists of several steps: establishing the risk environment, identifying the risks, measuring and analysing them, prioritising and comparing the risks, treating the risks, evaluating whether the treatments are effective and risks are adequately managed, and continuously monitoring and reporting on the risks.[49] What risk management has become most well-known for is the quantification of risks. Oftentimes, this is done by multiplying the probability that an event will occur in the future and the consequences this may lead to, i.e. the harm or the impact it will have.[50] The advantage to taking this approach is that risks are translated into numbers, which facilitates a more objective discussion on their importance.[51] Numbers make risks comparable, and consequently it becomes possible to make choices on which risks deserve priority over others, which need to be addressed first, and which can be delayed until later or even ignored entirely. As Aven and Ylönen say, through risk management "decision makers are provided with a rational approach for controlling the risk. By meeting some probabilistic limits or criteria, the remaining risk is found to be tolerable or even negligible."[52] Against a backdrop of limited resources and limited time the quantification of risks is a valuable asset.

2.6 Risk management works well here...

It is not surprising, therefore, that risk management has gained tremendous popularity in the past decades. Flying is safe because of solid risk management, and we can build mega structures such as skyscrapers and bridges over deep ravines because of good risk management. Note that these activities involve subway uncertainties: there are uncertainties involved, but these uncertainties are well understood, and for these activities the future resembles the past. We have plenty of experience from the past that we can build on: there is a store of data on misses and near misses that we have learnt from. For aviation, for instance, there is the Aviation Safety Network, a publicly available, international database in which all incidents and near misses worldwide for airplanes with over 12 passengers have been stored since 1919.[53] For building, our experience is even richer. We have been building since the earliest settlements of civilization, and we know what works and what does not. Moreover, in aviation and in construction we use simulations to test things before we put new ideas to use in practice. We train pilots in the risk-free environment of a simulator and any change made to an airplane is tested virtually extensively before it is added to real planes. Similarly, big buildings are exposed to a variety of variables simulating weather events, tremors and earthquakes in virtual

45. Mikes (n 19); Georges Dionne, 'Risk Management: History, Definition, and Critique' (2013) 16 Risk Management and Insurance Review 147.
46. John Wreathall and Christopher P Nemeth, 'Assessing Risk: The Role of Probabilistic Risk Assessment (PRA) in Patient Safety Improvement' (2004) 13 Quality and Safety in Healthcare 206.
47. Aven and Ylönen (n 41).
48. James Reason, *Managing the Risks of Organizational Accidents* (Ashgate 1997) 1; Sidney Dekker, *Foundations of Safety Science: A Century of Understanding Accidents and Disasters* (Routledge 2019); Elisabeth Paté-Cornell, 'Finding and Fixing Systems Weaknesses: Probabilistic Methods and Applications of Engineering Risk Analysis' (2002) 22 Risk analysis: an official publication of the Society for Risk Analysis 319; Bibi Van den Berg, Ruth Prins and Sanneke Kuipers, 'Assessing Contemporary Crises: Aligning Safety Science and Security Studies' (2020) Oxford Research Enclopedia of Politics http://dx.doi.org/10.1093/acrefore/9780190228637.013.1733.
49. Berg (n 44).
50. David Strachan-Morris, 'Threat and Risk: What Is the Difference and Why Does It Matter?' (2012) 27 Intelligence & National Security 172; Carl L Pritchard, *Risk Management: Concepts and Guidance* (2nd edn, ESI International 2001).
51. Some authors point out that perception should be factored into conversations about risk to make them truly 'objective'. See, for instance, Elke U Weber, '"Risk as Feelings" and "Perception Matters": Psychological Contributions on Risk, Risk-Taking, and Risk Management' in Howard Kunreuther, Robert J Meyer and O Michel-Kerjan Erwann (eds) (University of Pennsylvania Press 2019); Sven Ove Hansson, 'Seven Myths of Risk' (2005) 7 Risk Management: An International Journal 7; Paul Slovic, Baruch Fischhoff and Sarah Lichtenstein, 'Facts and Fears: Understanding Perceived Risk', *Societal Risk Assessment* (Springer US 1980); Paul Slovic, 'Perception of Risk' (1987) 236 Science 280; Paul Slovic, *The Feeling of Risk* (Earthscan/Taylor & Francis 2010) 1.
52. Aven and Ylönen (n 41) 15.
53. See 'Aviation Safety Network Database' https://aviation-safety.net/database, accessed on 6 November 2025.

environments before a single brick is laid. Finally, note that while airplanes and megastructures appear to be complex things, they are in fact not so complex at all: the number of variables that need to be taken into consideration for an airplane to stay up in the sky, and for a building to stay upright in relation to different geophysical and human factors is, in fact, limited.

In sum, risk management works well for airplane safety and building mega structures because these activities fall on the left side of the risk-uncertainty scale.

2.7 ...but risk management runs into troubles here...

As we have seen in our discussion on the risk-uncertainty scale, the further one moves to the right, however, the lower the degree of calculability – until beyond the point where quantification is no longer possible. When subway uncertainties become too complex, when there is limited data and/or data quality is low,[54] when simulations and modelling are difficult or impossible, and when intentionality plays a role in affecting (the trajectory towards) future events, risk management runs into trouble. It does not work well for Knightian or coconut uncertainties, because those cannot be predicted.

A few examples show how this works. When trying to respond to the risk of terrorist attacks, governments and organisations tend to look to the past to increase protections. They will, for instance, place large boulders in front of the entrance to buildings that may be a potential target to prevent an attacker from driving a vehicle into the facade. But terrorist activities, we have seen, cannot be predicted because we lack data, and modelling them would result in a scatter pattern. Moreover, it is far too complicated to know in advance where terrorists may strike – there are simply too many potential targets and too many ways in which attackers could operate. And most importantly, terrorists aim to sow fear by striking in an unexpected place at an unexpected moment in an unexpected way. They will go out of their way to surprise. Taking measures to prevent one type of attack, therefore, will entail that a terrorist may find other ways and means to attack. Risk management does not help in combatting this type of uncertainty.

Unfortunately, even when no intentionality is involved, risk management holds limited value for coconut uncertainties. Think of financial crises or earthquakes. For these types of incidents, we have data about past events, but the data is never rich enough to be able to say, with any degree of certainty, when or where the next crisis will hit. There are simply too many variables, and there is too much complexity and interdependency to be able to predict them.[55] We know that earthquakes and financial crises occur, but risk management falls short in helping us prevent them or in effectively and efficiently reducing their impact.

2.8 A desire to for control

What these examples show is that risk management works for a priori uncertainties and for straightforward or 'simple' subway or statistical uncertainties. It falls short for any form of statistical uncertainty that is more complicated than that, let alone for Knightian or coconut uncertainties. Basically, it cannot help us manage uncertainties from approximately the middle of the risk-uncertainty scale onwards towards the right side.

However, as we have seen, in our current understanding of risk we conflate a priori, statistical uncertainties and Knightian or coconut uncertainties all into a single concept. And that concept is then taken up in risk management practices with the ambition of identifying, quantifying and treating *any future event that we label as a risk*, thus gaining (a level of) control over all challenges we may face. This is problematic because it overlooks (1) the qualitatively different nature of the events we are seeking to treat, and (2) the fact that there is a fundamental impossibility to control coconut uncertainties or Knightian uncertainties in the first place, due to their complexity and rarity. Risk management may thus lead to an illusion of control for problems for which no such control is feasible.

54. Also see Aven (n 7) 3.
55. Aven (n 7).

3. Managing cyber risk?

The next question is: what does this mean for risks in relation to the digital ecosystem? Can cyber risks be managed using risk management methods and practices? Where do cybersecurity challenges fall on the risk-uncertainty scale?

3.1 Risk management runs into trouble here...

When we look at the risks that organisations run in relation to the digital ecosystem, it is obvious that we are looking at a relatively new environment that is very much in flux, and where a high degree of interconnectedness is one of the defining characteristics. When applying the four criteria for successful risk management which we discussed above to the digital environment the challenges for this approach are significant. Already in 1997, the former CEO of Google, Eric Schmidt, called the digital ecosystem "the first thing that humanity has built that humanity doesn't understand,"[56] and the complexity of the internet in those days pales in comparison with today. Large numbers of new pages, platforms, apps, clouds, devices and domains are added to this system of systems[57] daily, introducing new code, new protocols and unfortunately also, oftentimes, new vulnerabilities. Keeping the pace with the possible exploits for this dynamically changing ecosystem had led to an imbalance between attackers and defenders in cyberspace according to some researchers,[58] since defenders need to keep track of every potential vulnerability in their systems, whereas attackers only need to find a single weakness they can abuse.[59] Others even label this an arms race,[60] especially when nation states are involved. Automated vulnerability detection[61] and automated patching[62] are often mentioned as steps to solve these challenges, but the complexity of the digital ecosystem is such that large numbers of uncertainties will remain.

The second condition for risk management to work well is the availability of large volumes of high-quality data. This, too, is a challenge in relation to the digital ecosystem, first and foremost because we lack the (historical) data of e.g. 100+ years of flying or thousands of years of construction. As a matter of fact, only very few useful datasets are available for instance for research in this domain.[63] In this dynamically developing context, moreover, the challenges constantly change, which makes gathering sufficient data for proper predictions challenging. Just when we start getting a handle on a particular type of risk, new risks emerge or a new version of a well-known risk pops up, which weakens our level of control over it. Moreover, in contrast with, for instance, the aviation industry, information sharing on attacks or incidents is not common, at least not on a very large scale.[64] Obstacles to sharing information may include concerns over reputational damage, intellectual property leaks and data quality as well as weak trust relationships.[65]

56. Cited in Peter W Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know (R)* (Oxford University Press 2014) 26.
57. Herbert Lin and Amy Zegart, *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Institution Press 2019); Zio (n 8).
58. Ali Abbas and others, 'Guardians of the Galaxy: Protecting Space Systems from Cyber Threats (Dagstuhl Seminar 25101)' (Schloss Dagstuhl - Leibniz-Zentrum für Informatik 2025) http://dx.doi.org/10.4230/DAGREP.15.3.1; Quan Hong and others, 'Active Defense Research: A New Perspective Integrating Traps and Vulnerabilities', (*2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Sanya, China, December 2024; Farzan Kolini and others, 'Exploring Incentives and Challenges for Cybersecurity Intelligence Sharing (CIS) across Organizations: A Systematic Review' (2022) 50 Communications of the Association for Information Systems 86.
59. Erik Hollnagel, 'Managing for Security' in Gabriele Jacobs and others (eds), *International Security Management: New Solutions to Complexity* (Springer International Publishing 2021); Jerome H Saltzer and M Frans Kaashoek, 'Principles of Computer System Design: An Introduction' in Jerome H Saltzer and M Frans Kaashoek (eds), *Information security* (Morgan Kaufmann 2009).
60. Jarno Limnéll, 'The Cyber Arms Race Is Accelerating – What Are the Consequences?' (2016) 1 Journal of cyber policy 50; Anthony Craig and Brandon Valeriano, 'Conceptualising Cyber Arms Races',(*2016 8th International Conference on Cyber Conflict (CyCon)*, Tallinn, May2016).
61. Michael E Whitman and Herbert J Mattord, *Principles of Information Security* (4th edn, Cengage learning 2012).
62. Abbas and others (n 58).
63. Frank Cremer and others, 'Cyber Risk and Cybersecurity: A Systematic Review of Data Availability' (2022) 47 The Geneva Papers on Risk and Insurance Issues and Practice 698.
64. Elaine M Sedenberg and James X Dempsey, 'Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs' (2018) https://arxiv.org/abs/1805.12266.
65. Kolini and others (n 58).

Note also that information is proprietary, especially for cybersecurity companies, and this inhibits these organisations' inclinations to share information. Finally, sometimes there are legal or regulatory restrictions that inhibit information sharing, for instance in relation to privacy and personally identifiable information.[66] Taken together, we may conclude there are significant obstacles regarding the creation of large-scale, high-quality data sets for cyber risk management.

Third, there is the importance of modelling and simulations. Here, too, the challenges are significant, and this is mostly due to the amount of variables that may be relevant to any innovation in, or in relation to, the digital environment, and the potential impacts changes to code may have across interconnected domains. In simulations and models we oftentimes reduce the complexity of reality in order to productively, for instance, test a limited set of variables under a variety of conditions.[67] In a flight simulator, the model captures precisely those elements that one would want to test: it enables pilots to train a wide variety of situations they might encounter in real airplanes without putting them in an actual airplane. For software testing we also use contained environments, in which complexity is reduced to see how they withstand, for instance, different types of attacks. However, this is qualitatively different from using a flight simulator, because once software is released 'into the wild', predicting how it will interact with other code, and match with devices, platforms and clouds entails so many variables that realistic modelling is not feasible. Moreover, when simulating attacks on systems, networks and code, we use known attack methods and focus on known attack vectors. If, in the future, new attack methods and vectors may be discovered, these will not have been discovered in simulations prior to launch.

Last, there is the element of intentionality. Many cybersecurity challenges, though not all, involve human intentionality: they are the result of human beings that wilfully go out of their way to exploit vulnerabilities. Attacks on data, networks and systems come in many shapes and guises, ranging from acts of cybercrime to cyber espionage, and from offensive cyber operations to disinformation.[68] The impact of cybersecurity challenges may be minor, as is the case for instance when schoolkids attempt to steal exams from the school server, but also more severe, as is the case for instance when a large firm comes to a grinding halt as a consequence of a ransomware attack or when systems are harmed through the use of malware. The impact becomes even more significant in the case of deliberate supply chain attacks,[69] or when cascading effects emerge,[70] or when malware 'goes rogue' and affects parties (far) beyond the original target.[71] The harm that may be done is also varied, ranging from financial gain to reputational damage, from gaining intel to sowing discord, and from hampering activities to damaging privacy. Moreover, the range of actors that abuse the vulnerabilities of and in the digital ecosystem to harm others is also varied and each may do more or less damage in their own ways.[72] In all cases, however, when wilful attacks are instigated in or against the digital ecosystem, it is hard, if not outright impossible, to predict them for all the reasons we have discussed above.

66. ibid.
67. Cf. Heiner Müller-Merbach, 'The Role of Modeling' in Ulrich Derigs (ed), *Optimization and operations research – volume I* (EOLSS Publications 2009).
68. Van den Berg, Prins and Kuipers (n 48); B Van den Berg, 'Digitale Veiligheid: Een Inleiding' in B Van den Berg and others (eds), *Handboek Digitale Veiligheid* (Springer 2026).
69. Kim Zetter, 'The Untold Story of the Boldest Supply-Chain Hack Ever' *Wired* (2023) https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/ accessed 16 July 2025; Byung-Gak Son and others, 'The Dark Side of Supply Chain Digitalisation: Supplier-Perceived Digital Capability Asymmetry, Buyer Opportunism and Governance' (2021) 41 International journal of operations & production management 1220; ENISA, 'Identifying Emerging Cyber Security Threats and Challenges for 2030' (ENISA (European Union Agency for Cybersecurity) 2023) https://www.enisa.europa.eu/sites/default/files/publications/ENISA accessed 7 March 2025.
70. Alexander Cedergren and Jonas Johansson, 'Cascading Effects: What Are They, and How Do They Affect Society?' (University of Lund 2017); Mouco, Ruddell and Ginsburg (n 11); Chris C Demchak, 'Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)' (2012) 14 Journal of Comparative Policy Analysis: Research and Practice 254.
71. Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' *Wired* (22 August 2018) https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Bibi Van den Berg and Sanneke Kuipers, 'Vulnerabilities and Cyberspace: A New Kind of Crises', in Oxford Research Encyclopedia of Crisis Analysis (Oxford University Press 2022) http://dx.doi.org/10.1093/acrefore/9780190228637.013.1604.
72. Mark De Bruijne and others, 'Towards a New Cyber Threat Actor Typology: A Hybrid Method for the NCSC Cyber Security Assessment' (Nationaal Cyber Security Centrum 2017) https://www.wodc.nl/binaries/2740_Volledige_Tekst_tcm28-273243.pdf.

3.2 ...but risk management has value here

Based on this analysis, one would think that using risk management to grapple with cybersecurity challenges falls short for (almost) any challenge in relation to the digital ecosystem. After all, the description in the previous paragraph seems to suggest that challenges in this domain fall towards the right-hand side of the risk-uncertainty scale: they are at best complex statistical uncertainties, and at worst coconut or Knightian uncertainties. Perhaps risk management is not the most suitable tool for dealing with risk in the digital ecosystem?

Let us begin by stating that there are, indeed, a significant number of different kinds of uncertainty in the digital ecosystem that can be labelled as coconut or Knightian uncertainties, and that we will not be able to tackle these effectively with risk management, for all the reasons discussed above: too little data, too much complexity, too few options to model in any meaningful way, plus the role of human intentionality in instigating incidents. Having said that, let us not burn down the house to smoke out a rat. Risk management has significant limitations with respect to digital risk, but it also has value for some cybersecurity challenges, especially for subway uncertainties.

Take the example of combating spam. When email spam gained traction in the 1990s it was quite a challenge. Email spam is used for the purpose of advertisement, but also to scam people.[73] And since this was a relatively new phenomenon, and the scale at which email spam was spread was huge, the number of victims of this type of fraud was significant. Over time, however, internet service providers, network managers and email client providers found methods to scan networks for email spam and filter out messages that were flagged as such. The large volume of scam messages was an asset in this case: over a certain period, organisations were able to gather a lot of data on the content, the senders and the (writing) style of spam messages. Moreover, while these scams were instigated wilfully by senders, the evolution of email spam was not fast and advanced enough for the attackers to stay ahead of the defenders. The complexity of the phenomenon turned out to be less than originally envisioned. Collectively, these three elements contributed to the fact that email spam, over the course of the 2000s, moved from a statistical uncertainty of a challenging kind – at least in the middle of the risk-uncertainty scale – to the left, until it largely became a subway uncertainty: a patterned uncertainty that we can predict accurately, i.e. just the kind of risk that risk management is suitable for. This is not to say that email spam is gone, nor that it is never successful anymore. Especially with more recent advances in the use of AI for the creation and spread of spam messages, also on social media platforms, a new set of challenges has arisen, for which new data sets and new techniques need to be developed.[74] But the story of email spam does show that risk management methods can, in fact, be successful in combating particular types or digital risk, so long as these are, or can be turned into subway uncertainties.

More broadly, in the past decades techniques and processes have successfully been developed against some of the commonest threats in the digital ecosystem. For instance, organisations may use firewalls and antivirus software to detect malicious code or malicious activity in their networks, or intrusion-prevention systems to reduce the likelihood of being hit by a DDoS attack. Policies for patching software, preferably in an automated fashion, also contribute to blocking attacks, and using access management and encryption can help protect (critical) data and information. None of these measures and interventions is watertight, but all of them do bring us closer to making some digital risks 'manageable'. With increasing emphasis on risk-based approaches for organisations, and with the adoption of an emphasis on risk-based requirements in (European) law, the adoption of such measures will, in all likelihood, become broader over time, and organisations and individuals will become better protected against the commonest and most 'simple' kinds of attacks and outages. Risk management can play a role in helping organisations scout which preventative measures they cannot do without and getting their basic cybersecurity in order.

The trouble, of course, is that cyber risk managers need to recognize and acknowledge for which digital challenges risk management is an adequate tool, and where a priori and 'simple' statistical uncertainties, i.e.

73. Emilio Ferrara, 'The History of Digital Spam' (2019) 62 Communications of the ACM 82.
74. Ferrara (n 73).

risks, transform into uncertainties that simply cannot be predicted, i.e. more complicated statistical uncertainties and Knightian or coconut uncertainties. Lumping all uncertainties in relation to the digital environment into the single term 'risk' and then treating them all with the same approach is problematic for reasons that may have become obvious in section 3 of this article.[75] Yet this is the current practice in many organisations. By calling every uncertainty a risk, cyber risk managers limit themselves to a single tool in the toolbox. This may lead to assumptions of adequately and effectively securing organisations, when in fact no such guarantees can be given. It may lead to illusions of control, of safety and security, and this is risky – pun intended.

Moreover, claims on the meaningful quantification of risks ought to be taken with a grain of salt in most cases, simply because for almost all digital risks we lack sufficient high-quality data at this point in time – spam email being one of the exceptions to this rule. The example of spam email shows that for some statistical uncertainties we may, over time, be successful in gathering sufficient data to increase our predictive control over them. But the majority of cyber-related challenges either do not occur often enough, or there is insufficient information sharing about them, or they change too rapidly to gather sufficient insight into patterns to make them (more) predictable. The aim of this article, therefore, is not to disqualify or reject cyber risk management outright, but rather to "put [it] in its 'proper' place."[76]

4. Two additions to cyber risk management

That leaves us with the 'now what' question. Since risk management is not suitable for many of the uncertainties we face with respect to the digital ecosystem, what *other* tools are there in the toolbox to use as additions to risk management, especially geared towards the more complex statistical uncertainties and maybe even Knightian uncertainties? As Townsend *et al.* explain "In dynamic environments where future possibilities evolve in unexpected ways and the future diverges from the past, complementary approaches are necessary to resolve the problem of Knightian uncertainty."[77] So what are these complementary approaches?

In the final section of this paper, I will discuss two. They share an underlying assumption, which makes them suitable as additions to risk management. This assumption is that in a digital ecosystem fraught with uncertainties incidents *will* arise, no matter how hard we work at preventing them through risk management practices. Each approach has a different answer to this premise. The approach of *preparedness* embraces the fact that incidents will materialize as a given, and places emphasis on being able to deal with incidents and crises effectively and efficiently once they do. In contrast, the approach of *Security by Design* motivates designers and developers to invest effort into making digital technologies secure when they are created and then keeping them secure throughout their entire lifecycle. Here the idea is: when designs are weak, uncertainties are part and parcel of the lifecycle of every digital technology, but if we take into consideration better how to make products secure from the start, there may be fewer uncertainties – and ideally no uncertainties at all anymore – and hence incidents may not arise anymore either.

4.1 Preparedness

As said, preparedness is about accepting that incidents will happen, regardless of all the efforts we put into preventing them and that, therefore, we need to be as well prepared as possible for when they do. In this approach, interventions are taken to think through all the products and services we might need when, for instance, an organisation is hit by a ransomware attack or crippled by an internet outage, as well as the social arrangements that need to be in place at such a time. The goal of this is to increase the organisation's ability to bounce back effectively and efficiently from incidents, to return to normal operations as soon as possible, or if this is no longer possible, to adapt quickly to a new state of normalcy.[78]

75. This applies not just to risk management in relation to the digital ecosystem, but to the blanket application of risk management to almost any kind of uncertainty in modern society, of course.
76. Pat O'Malley, *Risk, Uncertainty and Government* (Routledge Cavendish 2004) 6 http://dx.doi.org/10.4324/9781843146025.
77. Townsend, Hunt and Rady (n 31) 453.
78. Preparedness is often connected to the notion of resilience. The latter term has many meanings, but most authors agree that it revolves around entities' abilities to bounce back quickly after incidents and/or entities' abilities to adapt to changing circumstances and absorb shocks. For a discussion on this topic see Van den Berg, 'Dealing with Uncertainty in Cyberspace' (n 9).

One of the methods used to increase preparedness is scenario planning,[79] which entails that experts sit together and think of what steps to take when an incident is unfolding to reduce the impact. Holt defines scenario planning as "the process whereby 'plots' are developed to allow for the exploration of alternative futures."[80] It involves 'what if'-thinking to explore what *might* happen, rather than what may (very well) happen.[81]

For example, the employees of an organisation may think through all the potential consequences of an internet outage for the organisation's headquarter buildings and investigate in detail which functionalities will be unavailable at such a point in time. Will the entry gates still open? Will the phone lines still work? Can messages to clients about this incident be posted on the company website? Is there an overview of which employees have which roles in crisis management and who has which mandate to make decisions? Can all these employees reach one another when the phones and computers no longer work? Based on a scenario such as a large-scale internet outage, the organisation can then take steps to decrease its potential impact, for instance by installing manual overrides on the entry gates, having satellite phones available for emergency phone calls, and conducting exercises with crises teams, in which roles and responsibilities as well as lines of communication can be practiced.

The downside of using scenario-planning is that the scenarios we practice for rarely materialise as such in real life. Coconut or Knightian uncertainties take us by surprise, not just because they are rare, but oftentimes also because they appear to be unlikely, or sometimes even unthinkable. Nevertheless, when adding redundancies in systems, both technical and social, these fallback options may serve a purpose in a wide variety of different situations. A manual override for entry gates is not just important in the case of an internet outage, but equally so in the case of fire, or a terrorist attack, or any other incident whereby many people need to evacuate. Similarly, when crisis teams practice, this helps build connections and trust, so that future incidents may be handled more smoothly because people know one another and know who has which role and mandate, regardless of whether the actual incident resembles the practiced one.

Developing preparedness protocols is a widely adopted practice in relation to physical safety in both government organisations and private companies and this has been "proven [beneficial] to manage uncertainty and mitigate the impact of relatively infrequent events."[82] Perhaps lessons learnt from this domain may also increase our abilities to cope with uncertainty in the digital ecosystem?

4.2 Security by design

The second approach, as explained, takes a different tack to the claim that incidents will happen because there are uncertainties in the digital ecosystem. From a Security by Design perspective, it is certainly true that once there are safety and security flaws in systems, in data, and networks, outages, incidents and crises will indeed be inevitable. What this design philosophy rejects, however, is that digital technologies always *must* contain vulnerabilities. The solution of uncertainty in the digital ecosystem for this approach is to ask: 'what if we would try to avoid security challenges in the first place?' Uncertainties in the digital ecosystem may be overcome, its followers claim, by fixing digital products and services, by making them safe and secure from the start, and by ensuring that they remain safe and secure throughout the time they are used.

79. Thomas M Leschine and others, 'What-If Scenario Modeling to Support Oil Spill Preparedness and Response Decision-Making' (2015) 21 Human and Ecological Risk Assessment: An International Journal 646.
80. William Holt, 'The Use of Scenarios in Contingency Planning' (2001) 2001 International Oil Spill Conference Proceedings 605, 606.
81. Leschine and others (n 79).
82. Jarvis (n 30) 308.

Security by Design, like risk-based approaches, has gained increased attention in recent years in academia,[83] with designers and producers of digital technologies[84] and in policy making circles and legislative contexts.[85] It is not, however, a recent set of ideas. Early computer scientists were keenly aware of the security risks that may arise from storing information in computers and from connecting computers to one another via networks. Already in 1975 Saltzer and Schroeder published a set of eight principles that ought to be followed to ensure "an implementation without security flaws."[86] These principles include ideas like economy of mechanism – keeping designs as simple as possible since any extra feature or line of code may result in adding weaknesses – and fail-safe defaults – designing systems in such a way that end users cannot make mistakes. As I have argued elsewhere, both principles have not found massive adoption until now – quite the reverse.[87] Instead, we design digital technologies with plenty of buggy and fault-sensitive 'features'. Other principles proposed by Saltzer and Schroeder did become mainstream over time, for instance the principles of separation of privilege and of least privilege.[88] Access management builds to a significant degree on these principles.[89]

There are several reasons why Security by Design is difficult and why we may never live in a world in which technologies have no vulnerabilities that can be exploited or through which incidents may arise accidentally. For one, security testing is time-intensive and very costly, and this does not sit well with the highly competitive world of technology development, in which companies must launch new products on very short time cycles.[90] And let us not forget that fixing weak software after it has been put on the market is a big source of revenue, for instance for companies selling virus scanners and firewalls.

Second, the culture surrounding technology development is one that focuses on generating 'disruptions': of suddenly taking the market by surprise with a radically new product or service. The credo of Silicon Valley, "move fast and break things,"[91] neatly captures this aim.[92] Moving fast and breaking things is the direct opposite of Security by Design, which, as said, not only requires time and effort and a far slower pace, but also focuses on fixing rather than breaking things.

Third, technology designers and developers often point towards the complexity of software, where even the smallest software programs may contain tens of thousands of lines of code, if not far more. It is unavoidable, software designers often claim, that vulnerabilities are going to creep into software because of its complexity, and therefore, realizing true Security by Design is not feasible.

83. Cristina Del-Real, Els De Busser and Bibi van den Berg, 'A Systematic Literature Review of Security and Privacy by Design Principles, Norms, and Strategies for Digital Technologies' (2025) International review of law computers & technology 1; Mark Kreitz, 'Security by Design in Software Engineering' (2020) 44 SIGSOFT Software Engineering Notes 23.
84. Danilo Bruschi, 'Introduction to Software Engineering for Secure Systems: Security by Design' in Danilo Bruschi, Bart De Win and Mattia Monga (eds), *Proceedings of the 2006 International Workshop on Software Engineering for Secure Systems: 2006, Shanghai, China, May 20-21, 2006* (ACM Press 2006); Johannes Geismann, Christopher Gerking and Eric Bodden, 'Towards Ensuring Security by Design in Cyber-Physical Systems Engineering Processes', (*Proceedings of the 2018 International Conference on Software and System Process*, Gothenburg, May 2018); Umit Cali and others, 'Digital Energy Platforms Considering Digital Privacy and Security by Design Principles', *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference* (Association for Computing Machinery 2023).
85. Bygrave (n 11).
86. JH Saltzer and MD Schroeder, 'The Protection of Information in Computer Systems' (1975) 63 Proceedings of the IEEE 1278; also see Saltzer and Frans Kaashoek (n 59).
87. Bibi Van den Berg, 'Back to the Future: A Plea for Guardrails, Islands and Anti-Featurism (Opening Keynote)' (ONE Conference 2025, The Hague, 30 September 2025).
88. Richard E Smith, 'A Contemporary Look at Saltzer and Schroeder's 1975 Design Principle', (*Proceedings 2012 Workshop on Usable Security*, IEEE 2012).
89. Also see Saltzer and Frans Kaashoek (n 59).
90. Melissa Hathaway, 'Patching Our Digital Future Is Unsustainable and Dangerous' in Aaron Shull (ed), *Governing cyberspace during a crisis in trust* (Centre for International Governance Innovation 2019); Also see Bibi Van den Berg, 'Mind the Air Gap: Preventing Privacy Issues in Robotics' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016).
91. Josh Costine, 'Facebook's S-1 Letter From Zuckerberg Urges Understanding Before Investment' *TechCrunch* (1 February 2012) https://techcrunch.com/2012/02/01/facebook-ipo-letter/ accessed 25 September 2024.
92. Moshe Y Vardi, 'Move Fast and Break Things' (2018) 61 Communications of the ACM 7.

There are counterarguments against all three claims. First, security-testing is indeed costly, and it entails that technology producers cannot push new products into the market as quickly as they may deem necessary in a competitive world. However, security can also be a unique selling point in a world of buggy products, and some large technology producers are, in fact, starting to move in this direction. The demands of regulators, who are moving towards legal demands for software quality and liability regimes for buggy products and services certainly help in this trend.

Second, imagine how much money organisations, end users *and* technology producers themselves would save if they would make products less buggy from the start. Many of the investments now made in risk management, in awareness programs, in protective and preventative measures would disappear or at least be diminished significantly. In a competitive world this seems like a more lucrative approach than going fast and breaking things, especially in the middle to longer term.

And third, software is indeed oftentimes complex and consists of many, many lines of code. One way of dealing with this is to aim for simplicity in design, as we already encountered above when discussing economy of mechanism. Kanat-Alexander explains that keeping software as simple as possible reduces the likelihood of vulnerabilities in its code. This does not mean that all programs should be as small as possible. Sometimes software simply needs a large number of lines because it seeks to execute complex functions. Simplicity, according to Kanat-Alexander, means that software should be divided into small pieces that each are easy to understand and maintain by code designers.[93]

Add to this the potential of automated code review and automated software debugging with the help of generative AI and far more vulnerabilities may in fact be detected before a product is put on the market in a much shorter time span and against a fraction of the cost.[94]

The point here is not to debate whether 100% secure design is feasible. Again, as this article has shown, the level of uncertainty in the digital ecosystem is such that attaining a (near-)complete level of security in it is near impossible. Instead, Security by Design entails a fundamental rethink of the way in which technology producers develop, implement and maintain their products and services, one which pushes for solving issues prior to selling them and thus reducing a significant number of vulnerabilities in the digital ecosystem. Overall, the assumption is, this will have a positive impact on the level of uncertainty in that environment.

5. In sum

To this day, risk management is considered the gold standard for many areas of life in which uncertainties are at play, from industrial safety and public health to finance and the realm of digital technologies. And rightly so, because it has been a key driver in making our world more safe and secure. At the same time, however, the risk management paradigm often conflates a range of different types of insecurity, some of which can, indeed, be 'managed' well, while others not so much – or not at all. Moreover, with its emphasis on quantification risk management sometimes falls into the trap of generating illusions of safety and security where none are warranted. These are concerns, especially for cyber risk management, where most challenges can be labelled either a complex statistical uncertainty or a coconut uncertainty.

Alongside risk management, therefore, other approaches are needed to address the uncertainties we face in the digital ecosystem. One of these is to focus on preparing for incidents by increasing redundancies and practicing through scenario planning. Another is to aim at decreasing uncertainty in the digital ecosystem by improving the quality of design and generating security throughout the entire lifecycle of products and

93. M Kanat-Alexander, *Code Simplicity: The Fundamentals of Software* (O'Reilly Media, Inc 2012).

94. Rahul Vadisetty and others, 'Leveraging Generative AI for Automated Code Generation and Security Compliance in Cloud-Based DevOps Pipelines: A Review' (2023) 31 Journal of Computational Analysis and Applications 544.

services. When combined, these three approaches provide us with a more complete coverage of the entire span of the risk-uncertainty scale.

5.1 Acknowledgements

The research in this document was conducted under the 'Cyber Security by Integrated Design (C-SIDe)' project, which was funded by NWO (grant number NWA 1215.18.008).