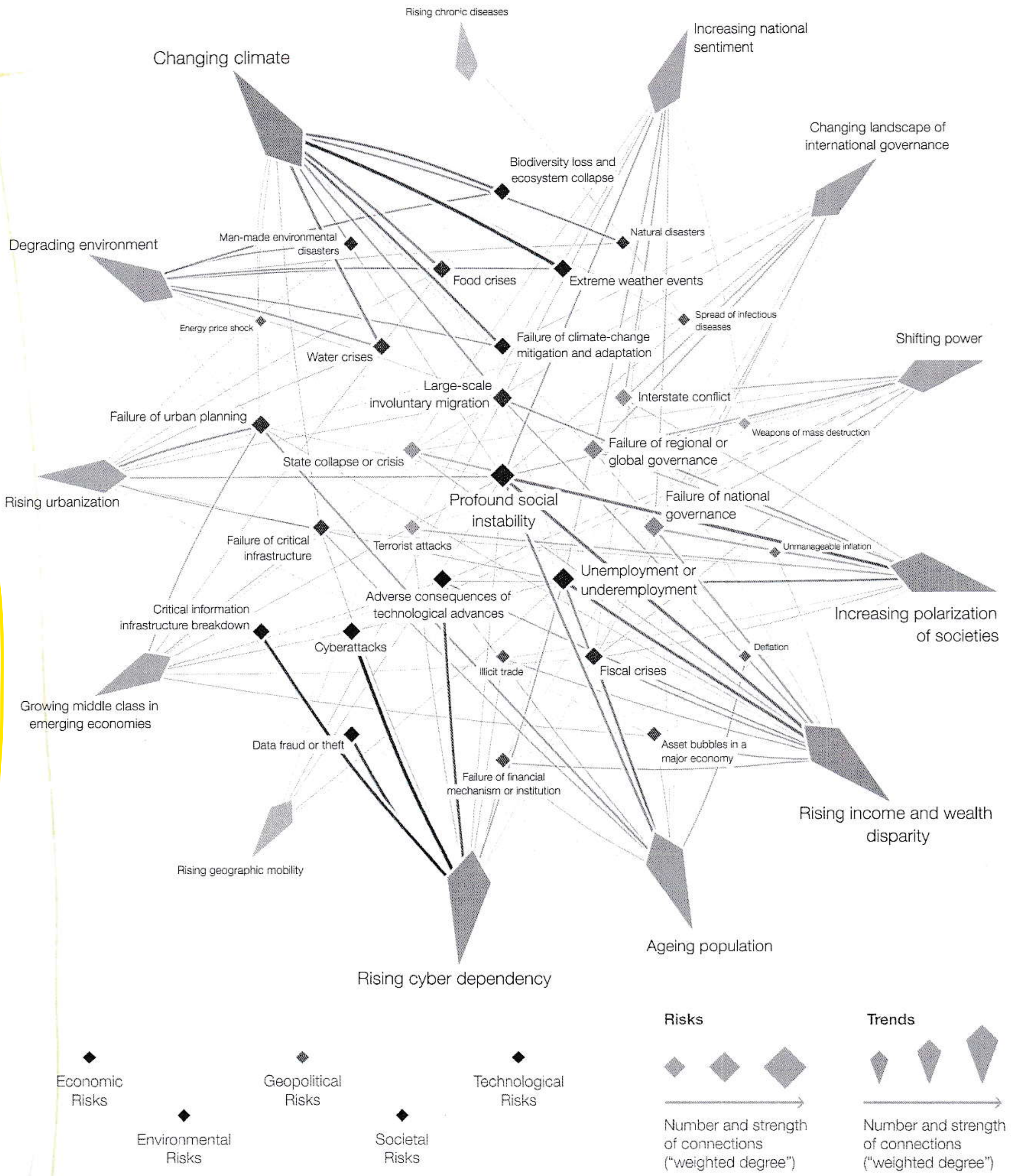
WEF, 2018

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Insight Report

The Global Risks Report 2018 13th Edition

Figure II: The Risks-Trends Interconnections Map 2018


Rising chronic diseases
Changing climate
Increasing national sentiment
Changing landscape of international governance
Biodiversity loss and ecosystem collapse
Natural disasters
Degrading environment
Man-made environmental disasters
Food crises
Extreme weather events
Spread of infectious diseases
Energy price shock
Water crises
Failure of climate-change mitigation and adaptation
Shifting power
Large-scale involuntary migration
Interstate conflict
Failure of urban planning
Weapons of mass destruction
Failure of regional or global governance
State collapse or crisis
Rising urbanization
Profound social instability
Failure of national governance
Failure of critical infrastructure
Terrorist attacks
Unmanageable inflation
Unemployment or underemployment
Adverse consequences of technological advances
Increasing polarization of societies
Critical information infrastructure breakdown
Cyberattacks
Deflation
Illicit trade
Fiscal crises
Growing middle class in emerging economies
Data fraud or theft
Asset bubbles in a major economy
Failure of financial mechanism or institution
Rising income and wealth disparity
Rising geographic mobility
Ageing population
Rising cyber dependency
Economic Risks
Geopolitical Risks
Technological Risks
Environmental Risks
Societal Risks
Risks
Number and strength of connections ("weighted degree")
Trends
Number and strength of connections ("weighted degree")

Source: World Economic Forum Global Risks Perception Survey 2017–2018.
Note: Survey respondents were asked to select the three trends that are the most important in shaping global development in the next 10 years. For each of the three trends identified, respondents were asked to select the risks that are most strongly driven by those trends. See Appendix B for more details. To ensure legibility, the names of the global risks are abbreviated; see Appendix A for the full name and description.

disruptions.[35] Structural economic changes in affected countries and regions could also stoke societal and geopolitical risks. There is no scope for complacency about the sufficiency of global efforts to deal with climate change and the continued degradation of the global environmental commons. Equally, however, it is time to prepare for the structural challenges and changes that lie ahead as those efforts gather pace.

/ Sector is on Risky

Cyber-defences are being tested

Moving from the environmental commons to the virtual commons, cyber-risks intensified in 2017. Although in previous years respondents to the GRPS have tended to be optimistic about technological risks, this year concerns jumped, and cyberattacks and massive data fraud both appear in the list of the top five global risks by perceived likelihood.

Attacks are increasing, both in prevalence and disruptive potential. Cyber breaches recorded by businesses have almost doubled in five years, from 68 per business in 2012 to 130 per business in 2017.[36] Having been choked off by law enforcement successes in 2010–2012, "dark net" markets for malware goods and services have seen a resurgence:[37] in 2016 alone, 357 million new malware variants were released and "banking trojans" designed to steal account login details could be purchased for as little as US$500.[38] In addition, cybercriminals have an exponentially increasing number of potential targets, because the use of cloud services continues

REUTERS/Pedro Nunes

IoT devices		Global population
8.4	›	7.6
Billion		Billion

to accelerate and the Internet of Things is expected to expand from an estimated 8.4 billion devices in 2017 to a projected 20.4 billion in 2020.[39] What would once have been considered large-scale cyberattacks are now becoming normal. For example, in 2016, companies revealed breaches of more than 4 billion data records, more than the combined total for the previous two years.[40] Distributed denial of service (DDoS) attacks using 100 gigabits per second (Gbps) were once exceptional but have now become commonplace, jumping in frequency by 140% in 2016 alone.[41] And attackers have become more persistent—in 2017 the average DDoS target was likely to be hit 32 times over a three-month period.[42]

The financial costs of cyberattacks are rising. A 2017 study of 254 companies across seven countries put the annual cost of responding to cyberattacks at £11.7 million per company, a year-on-year increase of 27.4%.[43] The cost of cybercrime to businesses over the next five years is expected to be US$8 trillion.[44] Some of the largest costs in 2017 related to ransomware, a rapidly growing form of malware that locks targets out of their data and demands a ransom in return for restoring access. Ransomware attacks accounted for 64% of all malicious emails sent between July and September last year,[45] affecting double the number of businesses compared with 2016.[46] Notable examples included the WannaCry attack, which affected 300,000 computers across 150 countries, and Petya and NotPetya, which caused huge corporate losses: for example, Merck, FedEx and Maersk each reported third-quarter losses of around US$300 million as a result of NotPetya.[47]

Beyond its financial cost, the WannaCry attack disrupted critical and strategic infrastructure across the world, including government ministries, railways, banks, telecommunications providers, energy companies, car manufacturers and hospitals. It illustrated a growing trend of using cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning. Many of these attacks are thought to be state sponsored. WannaCry's ultimate impact was relatively low, largely because a "kill switch" was discovered, but it highlighted the vulnerability of a wide range of infrastructure organizations and installations to disruption or damage. Since the 2015 attack on Ukraine's power grid—which temporarily shut down 30 substations, interrupting power supply to 230,000 people[48]—evidence has been mounting of further attempts to target critical infrastructure. In 2016, for example, an attack on the SWIFT messaging network led to the theft of US$81 million from the central bank of Bangladesh. The European Aviation Safety Agency has stated that aviation systems are subject to an average of 1,000 attacks each month.[49] Last year saw reports of attempts to use spear-phishing attacks (stealing data or installing malware using individually targeted email scams) against companies operating nuclear power plants in the United States.[50]

Most attacks on critical and strategic systems have not succeeded—but the combination of isolated successes with a growing list of attempted attacks suggests that risks are increasing. And the world's increasing interconnectedness and pace heightens our vulnerability to attacks that cause not only isolated and temporary disruptions, but radical and irreversible systemic shocks.

Our growing vulnerability to systemic risks

Humanity has become remarkably adept at understanding how to mitigate countless conventional risks that can be relatively easily isolated and managed with standard risk-management approaches. But we are much less competent when it comes to dealing with complex risks in systems characterized by feedback loops, tipping points and opaque cause-and-effect relationships that can make intervention problematic.[51]

Resilience in complex organizations

By Roland Kupers

In a deeply interconnected world, stresses and shocks propagate across systems in ways that evade forecasting. Climate change is linked to the Syrian civil war, which is connected to heightened concern over immigration, which precipitated Brexit. Lehman Brothers was an investable company, until suddenly it wasn't and it catalysed a global financial crisis. None of these links are causal in a strict sense, nor could they reasonably be assigned a probability, but they nevertheless clearly form a web of cascading events. Organizations increasingly recognize how rapidly and often unexpectedly such events unfold. Since the 2008 financial crisis, the terms "black swans" and "fat tails" have become a familiar part of the risk conversation. Yet we don't always fully spell out the consequences.

Standard risk management tools assume that the risks follow a normalized distribution, mainly because this provides easy-to-understand narratives. But fat tail risks are not normal distributions. The only way to maintain the traditional tools is to neglect and wish away the fat tails. Simply denying the existence of black swans is hardly a way to deal with them. This approach may be approximately right most times, but in principle it is wrong. The consequences of being so wrong can impact an enterprise, perhaps catastrophically. Fortunately there is an alternative, which consists of applying a resilience lens where complexity prevails and traditional risk management is insufficient.

Resilience is, in fact, a property of complex systems. And complexity is the science of interconnected systems that has been driving a slow-motion revolution in science over the past 35 years or so. In 2013 the World Economic Forum published a comprehensive overview in *Perspectives on a Hyperconnected World*, describing the impact of complexity for policy and business. The conclusion is not that policy-makers and managers must become complexity experts. But a level of complexity literacy is crucial to navigate the modern age.

Nine resilience lenses

At the World Economic Forum's annual meeting in 2012, prominent companies began to take note of resilience. Peter Voser, at the time Shell's CEO, asked nine of his colleagues from across sectors what the impact of considering resilience would be on their business, on their clients and on their risk management. This led to the creation of the Resilience Action Initiative (RAI), which in turn resulted in a set of resilience tools and approaches informed by complexity theory but grounded in practice. One critical application is enterprise resilience: the capacity of a company or other organization to adapt and prosper in the face of high-impact, low-probability risks.

Working on the RAI project, we broke resilience into a set of lenses that could be applied across an organization's operations. We used the resilience lenses to examine the systemic risks and evaluate mitigation strategies. These lenses were then tested and tuned for applicability with the risk managers of the RAI companies. The new resilience tools are intended to be used in addition to traditional risk management tools, not instead of them. Organizations will continue to face normalized risks, which require the traditional tools. It is systemic risks that require the new tools.

The RAI work led to nine resilience lenses, grouped into the following three categories to provide the agenda for a fat-tail risk conversation:

- "Structural resilience" considers the systemic dynamics within the organization itself.
- "Integrative resilience" underlines complex interconnections with the external context.
- "Transformative resilience" responds to the fact that mitigating some risks requires transformation.

Structural resilience

This category encompasses redundancy, modularity and requisite diversity. The focus of structural resilience is on bouncing back faster from a disturbance. **Redundancy** is possibly the most familiar resilience strategy, but like the spare tyre on a car, it is the most expensive approach, because it requires non-performing assets. System **modularity** builds resilience only if the modules are loosely coupled: separate them too much and you no longer have a system, couple them too tightly and you lose the adaptive capacity. As in nature, diversity is a key resilience strategy. For organizations, however, this requires addressing the hard question of which diversity is fit for purpose for this problem at this time. That is what is meant by "**requisite diversity**".

Trends

A "trend" is defined as a long-term pattern that is currently evolving and that could contribute to amplifying global risks and/or altering the relationship between them.

Trend	Description
Ageing population	Ageing populations in developed and developing countries driven by declining fertility and decrease of middle- and old-age mortality
Changing landscape of international governance	Changing landscape of global or regional institutions (e.g. UN, IMF, NATO, etc.), agreements or networks
Changing climate	Change of climate, which is attributed directly or indirectly to human activity, that alters the composition of the global atmosphere, in addition to natural climate variability
Degrading environment	Deterioration in the quality of air, soil and water from ambient concentrations of pollutants and other activities and processes
Growing middle class in emerging economies	Growing share of population reaching middle-class income levels in emerging economies
Increasing national sentiment	Increasing national sentiment among populations and political leaders affecting countries' national and international political and economic positions
Increasing polarization of societies	Inability to reach agreement on key issues within countries because of diverging or extreme values, political or religious views
Rising chronic diseases	Increasing rates of non-communicable diseases, also known as "chronic diseases", leading to rising costs of long-term treatment and threatening recent societal gains in life expectancy and quality
Rising cyber dependency	Rise of cyber dependency due to increasing digital interconnection of people, things and organizations
Rising geographic mobility	Increasing mobility of people and things due to quicker and better-performing means of transport and lowered regulatory barriers
Rising income and wealth disparity	Increasing socioeconomic gap between rich and poor in major countries or regions
Shifting power	Shifting power from state to non-state actors and individuals, from global to regional levels, and from developed to emerging market and developing economies
Rising urbanization	Rising number of people living in urban areas resulting in physical growth of cities