Dirk Helbing

Thinking Ahead

Essays on Big Data, Digital Revolution, and Participatory Market Society

Springer

Thinking Ahead—Essays on Big Data, Digital Revolution, and Participatory Market Society

Dirk Helbing

Thinking Ahead—Essays on Big Data, Digital Revolution, and Participatory Market Society

Dirk Helbing
ETH Zürich, CLU E1
Computational Social Science
Claussiusstrasse 50
8092 Zürich
Switzerland

ISBN 978-3-319-15077-2 ISBN 978-3-319-15078-9 (eBook)
DOI 10.1007/978-3-319-15078-9

Library of Congress Control Number: 2015934446

Springer Cham Heidelberg New York Dordrecht London

Cover illustration: Internet security and privacy issues with a human eye and digital binary code as surveillance of hackers or hacking from cyber criminals watching prohibited access to web sites with firewalls. Stock Photo. Copyright: Lightspring.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

About the Author

Physicist Dirk Helbing is Professor of Computational Social Science at the Department of Humanities, Social and Political Sciences and an affiliate of the Computer Science Department at ETH Zurich, as well as co-founder of ETH's Risk Center. He is internationally known for the scientific coordination of the FuturICT Initiative which focuses on using smart data to understand techno-socio-economic systems.

"Prof. Helbing has produced an insightful and important set of essays on the ways in which big data and complexity science are changing our understanding of ourselves and our society, and potentially allowing us to manage our societies much better than we are currently able to do. Of special note are the essays that touch on the promises of big data along with the dangers...this is material that we should all become familiar with!"

Alex Pentland, MIT, author of Social Physics: How Good Ideas Spread—The Lessons From a New Science

"Dirk Helbing has established his reputation as one of the leading scientific thinkers on the dramatic impacts of the digital revolution on our society and economy. Thinking Ahead is a most stimulating and provocative set of essays which deserves a wide audience."

Paul Ormerod, economist, and author of Butterfly Economics and Why Most Things Fail.

"It is becoming increasingly clear that many of our institutions and social structures are in a bad way and urgently need fixing. Financial crises, international conflicts, civil wars and terrorism, inaction on climate change, problems of poverty, widening economic inequality, health epidemics, pollution and threats to digital privacy and identity are just some of the major challenges that we confront in the twenty-first century. These issues demand new and bold thinking, and that is what Dirk Helbing offers in this collection of essays. If even a fraction of these ideas pay off, the consequences for global governance could be significant. So this is a must-read book for anyone concerned about the future."

Philip Ball, science writer and author of Critical Mass

"This collection of papers, brought together by Dirk Helbing, is both timely and topical. It raises concerns about Big Data, which are truly frightening and disconcerting, that we do need to be aware of; while at the same time offering some hope that the technology, which has created the previously unthought-of dangers to our privacy, safety and democracy can be the means to address these dangers by enabling social, economic and political participation and coordination, not possible in the past. It makes for compelling reading and I hope for timely action."

Eve Mitleton-Kelly, LSE, author of Corporate Governance and Complexity Theory and editor of Co-evolution of Intelligent Socio-technical Systems.

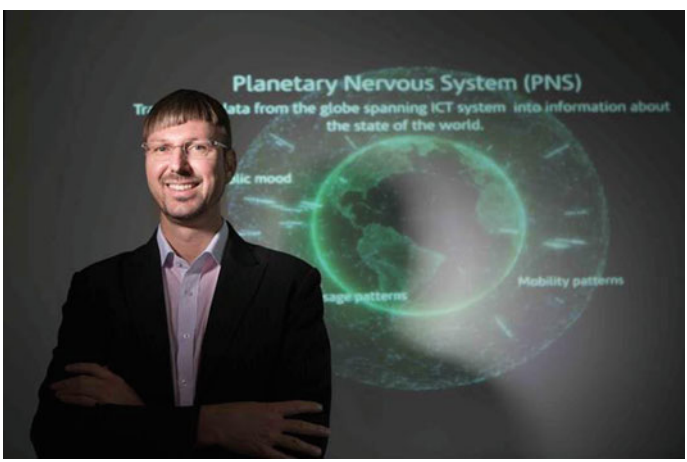

Foto: Sabina Bobst

Preface

This booklet presents a collection of essays and discussion or white papers on Big Data, the ongoing Digital Revolution and the emergent Participatory Market Society. These have been written since the year 2008 in anticipation of and response to the financial and other crises. While we have seen a pretty peaceful period after the fall of the Berlin Wall in 1989, the world seems to have increasingly destabilized in the aftermath of September 11, 2001.

If we want to master the related challenges, we must analyze the underlying problems and change the way we manage our techno-socio-economic systems.

I would like to thank many friends and colleagues, in particular the worldwide FuturICT community, for the inspiring discussions and the continued support. I am also grateful to Stefano Balietti, James Breiding, and Markus Christen for their reprint permissions regarding two of the chapters in this booklet.

November 2014 Dirk Helbing
Zürich

Contents

1
Introduction—Have We Opened Pandora's Box?

This chapter first appeared in the FuturICT Blog on September 10, 2014, see http://futurict.blogspot.ch/2014/09/have-we-opened-pandoras-box_10.html, and is reproduced here with minor stylistic improvements. Acknowledgments: I would like to thank many friends and colleagues, in particular the world-wide FuturICT community, for the inspiring discussions and the continued support. I am also grateful to Stefano Balietti, James Breiding, and Markus Christen for their reprint permissions regarding two of the chapters in this booklet.

1.1 Global Financial, Economic and Public Spending Crisis

The first of the contributions in this booklet dates back to March 2008, when Markus Christen, James Breiding and myself became concerned about the stability of the financial system that we felt urged to write a newspaper article to alert the public (see the English translation in Chap. 4). Unfortunately, at that time, the public was not ready to listen. Newspaper editors found our analysis too complex. We responded that a financial crisis would be impossible to prevent, if newspapers failed to explain the complexity of problems like this to their audience. Just a few months later, Lehmann Brothers collapsed, which gave rise to a large-scale crisis. It made me think about the root causes of economic problems [1–4] and of global crises in general [5, 6] (see Chaps. 4, 5,

D. Helbing, *Thinking Ahead—Essays on Big Data, Digital Revolution, and Participatory Market Society,* DOI 10.1007/978-3-319-15078-9_1

and 7). But my collaborators and I saw not only the financial crisis coming. We also voiced the surveillance problem early on and the political vulnerability of European gas supply. We studied conflict in Israel, the spreading of diseases, and new response strategies to earthquakes and other disasters. Shortly after, all of this turned out to be highly relevant, almost visionary.

When I attended a Global Science Forum in 2008 organized by the OECD [7], most people still expected that the problems in the US real estate market and the banking system could be fixed. However, it was already clear to me and probably also to many other complexity scientists that they would cause cascade effects and trigger a global economic and public spending crisis, which we would not recover from for many years. At that time, I said that nobody understood our financial system, our economy, and our society well enough to grasp the related problems and to manage them successfully. Therefore, I proposed to invest into a large-scale project in the social sciences—including economics—in the very same way as we have invested billions into the CERN elementary particle accelerator, the ITER fusion reactor, the GALILEO satellite system, space missions, astrophysics, the human genome projects, and more. I stressed that, in the twenty-first century, we would require a "knowledge accelerator" to keep up with the pace at which our societies are faced with emerging problems [8]. Today, business and politics are often based on scientific findings that are 30 to 50 year old, or not based on evidence at all. This is not sufficient anymore to succeed in a quickly changing world. We would need a kind of Apollo project, but not one to explore our universe—rather one that would focus on the Earth and what was going on there, and why.

1.2 Need of a "Knowledge Accelerator"

As a consequence, the VISIONEER support action funded by the European Commission (http://www.visioneer.ethz.ch) worked out four white papers proposing large-scale data mining, social supercomputing, and the creation of an innovation accelerator [9]. Already back in 2011, VISIONEER was also pointing out the privacy issues of modern information and communication technologies, and it even made recommendations how to address them [10].

Then, in response to the European call for two 10-year-long one billion EURO flagship projects in the area of Future Emerging Technologies (FET), the multi-disciplinary FUTURICT consortium was formed to turn this vision into reality (see http://www.futurict.eu). Thousands of researchers world-wide, hundreds of universities, and hundreds of companies signed up for this. 90 million € matching funds were waiting to be spent in the first 30 months. But while the project was doing impressively well, to everyone's surprise it was finally not funded, even though we proposed an approach aiming at ethical information and communication technologies [10, 11], with a focus on privacy and citizen participation [12].

This possibly meant that governments had decided against FuturICT's open, transparent, participatory, and privacy-respecting approach, and that they might invest in secret projects instead. If this were the case, a worrying digital arms race would result. Therefore, while spending my Easter holidays 2012 in Sevilla, I wrote a word of warning with the article "Google as God?" (see Chap. 9). Shortly later, Edward Snowden's revelations of global mass surveillance shocked the world, including myself [13]. These unveiled past and current practices of secret services in various countries and criticized them as illegal. Even though an informed

reader could have expected a lot of what was then reported, much of it just surpassed the limits of imagination.

The sheer extent of mass surveillance, the lack of any limits to the technical tools developed, and the way they were used frightened and alarmed many citizens and politicians. The German president, Joachim Gauck, for example, commented: "This affair [of mass surveillance] concerns me a lot. ... The worry that our phone calls and emails would be recorded and stored by a foreign secret service hampers the feeling of freedom—and with this there is a danger that freedom itself will be damaged." [14] Nevertheless, many important questions have still not been asked: How did we get into this system of mass surveillance? What was driving these developments? Where will they lead us? And what if such powerful information and communcation technologies were misused? Such questions will be addressed in this booklet.

1.3 We are Experiencing a Digital Revolution

One of the important insights is: We are in the middle of a digital revolution—a third industrial revolution after the one turning agricultural societies into industrial ones, and these into service societies. This will fundamentally transform our economy and lead us into the "digital society" [15]. I claim that not only the citizens haven't noticed this process early enough, but also most businesses and politicians. By the time we got a vague glimpse of what might be our future, it had already pervaded our society, in the same way as the financial crisis had infected most parts of our economy. Again, we have difficulties to identify the responsible people—we are facing a systemic issue.

Rather than blaming companies or people, my effort is to raise awareness for the implications of the techno-socio-economic

systems we have created: intended and unintended, positive and negative ones, and to point the way to a brighter future. As it turns out, we do in fact have better alternatives. But before I discuss these, let me first give a reasonably short summary of the current insights into the side effects of information and communication technologies, as far as they must concern us.

1.4 Threats to the Average Citizen

Let me begin with the implications of mass surveillance for citizens. It is naive and just wrong to assume mass surveillance would not matter for an average citizen, who is not engaged in any criminal or terrorist activities. The number of people on lists of terror suspects comprises a million names [16]—other sources even say a multiple of this. It became known that these lists contains a majority of people who are not terrorists nor linked with any. Furthermore, since friends of friends of contact persons of suspects are also under surveillance, basically everyone is under surveillance [17].

Of course nobody would argue against preventing terrorism. However, mass surveillance [18] and surveillance cameras [19] haven't been significantly more effective in preventing crime and terror than classical investigation methods and security measures, but they have various side effects. For example, tens of thousands of innocent subjects had to undergo extended investigation procedures at airports [20]. In connection with the war on drugs, there have even been 45 million arrests [21], where many appear to be based on illegal clues from surveillance [22]. Nevertheless, the war on drugs has failed, and US Attorney General Eric Holder finally concluded: "Too many Americans go to too many prisons for far too long, and for no truly good law enforcement reason" [23].

Recently, many people have also been chased for tax evasion. While I am not trying to defend drug misuse or tax evasion, we certainly see a concerning transition from the principle of assumed innocence to a situation where everyone is considered to be a potential suspect [24]. This is undermining fundamental principles of our legal system, and implies threats for everyone. In an over-regulated society, it is unlikely that there is anybody who would not violate any laws over the time period of a year [25]. So, everyone is guilty, in principle. People (and companies) are even increasingly getting into trouble for activities, which are legal—but socially undesirable, i.e. we are increasingly seeing phenomena comparable to "witch hunting." For example, in December 2013, thousands of people got sued by a law firm for watching porn [26]. For the first time, many people became aware that all of their clicks in the Internet were recorded by companies, and that their behavior was tracked in detail.

1.5 Threats so Big that One Cannot Even Talk About Them

On the side of the state, such tracking is being justified by the desire to prevent danger to society, and child pornography is often given as one of the reaons. Again, nobody would argue against the need to protect children from misuse, but this time the subject is even so taboo that most people are not even aware of what exactly one is talking about. You can't really risk to look up information in the Internet, and you are advised to delete photographs depicting yourself when you were a child. Only recently, we have learned that Internet companies report thousands of suspects of child pornography [27]. It is not known what percentage of these people have ever touched a child in an immoral way, or paid money for unethical pictures or video materials. This is particularly problematic, as

millions of private computers are hacked and used to send spam mails [28]; illegal material might easily be among them.

Note that passwords of more than a billion email accounts have been illegally collected, recently [29]. This might imply that almost everyone living in a first world country can be turned into a criminal by putting illegal materials on one of their digital devices. In other words, if you stand in somebody's way, he or she might now be able to send you to prison, even if you have done nothing wrong. The evidence against you can be easily prepared. Therefore, your computer and your mobile device become really dangerous for you. It is no wonder that two thirds of all Germans don't trust that Internet companies and public authorities use their personal data in proper ways only; half of all Germans even feel threatened by the Internet [30].

1.6 Are we Entering an Age of Discrimination?

On the side of big business, our clicks are being collected for the sake of personalized advertisements, but also to make cash in ways that are highly problematic. Whenever you apply for a loan or a health insurance, between 3000 and 5000 personal data about you might be used to determine the rate you have to pay—or whether you get an offer at all. You would probably be shocked to see what is known about you, and how many thousands or millions of people in the world have access to these data. The people looking into our sensitive personal data, including health data, range from secret services over border police to banks and insurance companies to the businesses that sell and provide advertisements.

While these data are collected even if you don't implicitly agree to share them (by accepting the terms of use of a software, browser, or app), it has become common to apply them in increasingly

more business areas. Some of the data that were collected without informed consent may be "whitewashed" by intermediary data providers buying illegal data and declaring their legal origin ("data laundry"). Personal data are used, for example, to make personalized offers when buying products on the Internet. In fact, offered products and prices now often depend on your country, neighborhood, and salary. In other words, if you live in the "wrong neighborhood," you may have to pay a higher price, and if you don't walk enough or if you frequently eat at fastfood restaurants, your life insurance may be more expensive. In other words, discrimination will increasingly become an issue (see Chap. 11). Besides, about half of the personal data sets contain mistakes [31]. As a consequence, you will get wrong offers without any chance to check and challenge them. It is obvious that we have currently a great lack of transparency, and also of mechanisms to get wrong data corrected.

1.7 Threats to Companies

But the age of Big Data is not only becoming a threat to citizens. The same applies to companies as well. There is an increasing risk of espionage of sensitive trade secrets. For example, it has been proven that intellectual property of the Enercon company was stolen and patented by a competing company [32]. One may wonder, how such cyber espionage works, but most computer systems are more vulnerable than one would think [33]. Every hour, there are thousands of cyberattacks, and it is often just a matter of time until one of them succeeds. It does not have to be a secretary who opened a virus or trojan horse attachment of an email. Stuxnet, for example, was even able to reach computers that are not directly connected to the Internet [34]. Any USB port may be a problem [35], too, and even your water boiler in