

Preface

In our modern information societies, we not only use and welcome computers. We are highly dependent upon them. This is a downside, a hubris of this kind of progress. These days, everything is done with a computer. And in most cases in which the computer replaced analogue or human routines, we forgot about those alternative practices rather quickly. This renders us even more dependent. We are not only technologically dependent. We are also cognitively dependent. Life without computers has become impossible.

If computers were a 100 % reliable, this dependency would not be a problem. But they are not reliable. They might be reliable in terms of the standard continuity of their services. This is a specification which is met these days. But they are unreliable on a different front. They are insecure. They are vulnerable to attackers. They can either be attacked directly, to disrupt their services. Or they can be abused in clever ways to do the bidding of an attacker as a dysfunctional user. This is probably more dangerous than the simple disruption. A disruption can be noticed and—in most cases—managed. An abuse, a dysfunctional use need not be noticed and can serve the attacker a host of different attractive options. Information can be stolen. It can be manipulated. Criminal goods can be transported. Vital services can be eroded. Infrastructures or products can be damaged.

Given the vast diffusion of information technologies and our high dependencies, these threats grow more dangerous every day. What is even worse—over the past years, a set of new and even more sophisticated attackers got attracted by the vulnerabilities and dependencies of modern information societies. Organized crime syndicates and militaries have realized that this kind of outset is hugely beneficial for them, with little costs to be spent for substantial monetary or strategic gains.

We have to react. But we should not react blindly. Blind reactions are likely in this field. Public criticism and the press generate a pressure to act, but decision-makers of all sorts are no experts. They cannot even decide on the right kind of expert or a truly efficient company. Success in security is notoriously hard to measure. So experts and companies with good PR-strategies tend to be in the focus of decision-makers. But those are not always the ones who are right or capable to provide the right solution. On the contrary—many IT-security products are insecure themselves,

thus only adding insecurity to an already insecure system. The victim will not know for years. Neither the attacker, nor the deficient product will notify it. Concluding, the uncertainty enables security regimes with uncertain effects. Path-dependencies ensue and make it even harder to implement the security needed where it is needed. Decision-makers do not want to have made a wrong decision. So they tend to stick to whatever they have decided, and defend it for as long as possible—whether it actually provides security or not.

Implementing the wrong kind of security can even be detrimental to other political values. Freedom and security have always been in an uneasy relationship to one another. There are win-win-scenarios, and we should continue to seek them and handle them as a priority, even if they are monetarily more costly. But in many cases, freedom and security affect each other negatively. This requires even more expert knowledge. Decision-makers would not only have to be able to understand the technology, they would also have to understand its further technical and political potential, any kind of possible abuse of its functionality.

But most decision-makers still struggle with the amount of knowledge needed. And most experts struggle as well. They frequently encounter difficulties when they have to understand the implications of their field of expertise for another field of expertise. This is the burden of the complexities we live in. Technologists don't understand politics or law and vice versa.

To mitigate this problem, an approach to technological enlightenment should be initiated. More transdisciplinary knowledge has to be generated to inform lay people inasmuch as experts of other fields about the nuts and bolts of modern information societies and about the implications of technological or political progress or the lack thereof.

This is the task of this anthology. It aims to provide a spotlight onto some aspects of the uneasy relationship between information technology and information society, when it comes to security. With this general outset, it aims more narrowly to present an outlook onto some late developments and new technologies to help the dialogue not only in its current and ongoing struggle, but to anticipate the future in time and prepare perspectives for the challenges ahead. We hope you find it enlightening.

Jörg Krüger
Bertram Nickolay
Sandro Gaycken

The Secure Information Society
Ethical, Legal and Political Challenges
Krüger, J.; Nickolay, B.; Gaycken, S. (Eds.)
2013, X, 214 p., Hardcover
ISBN: 978-1-4471-4762-6