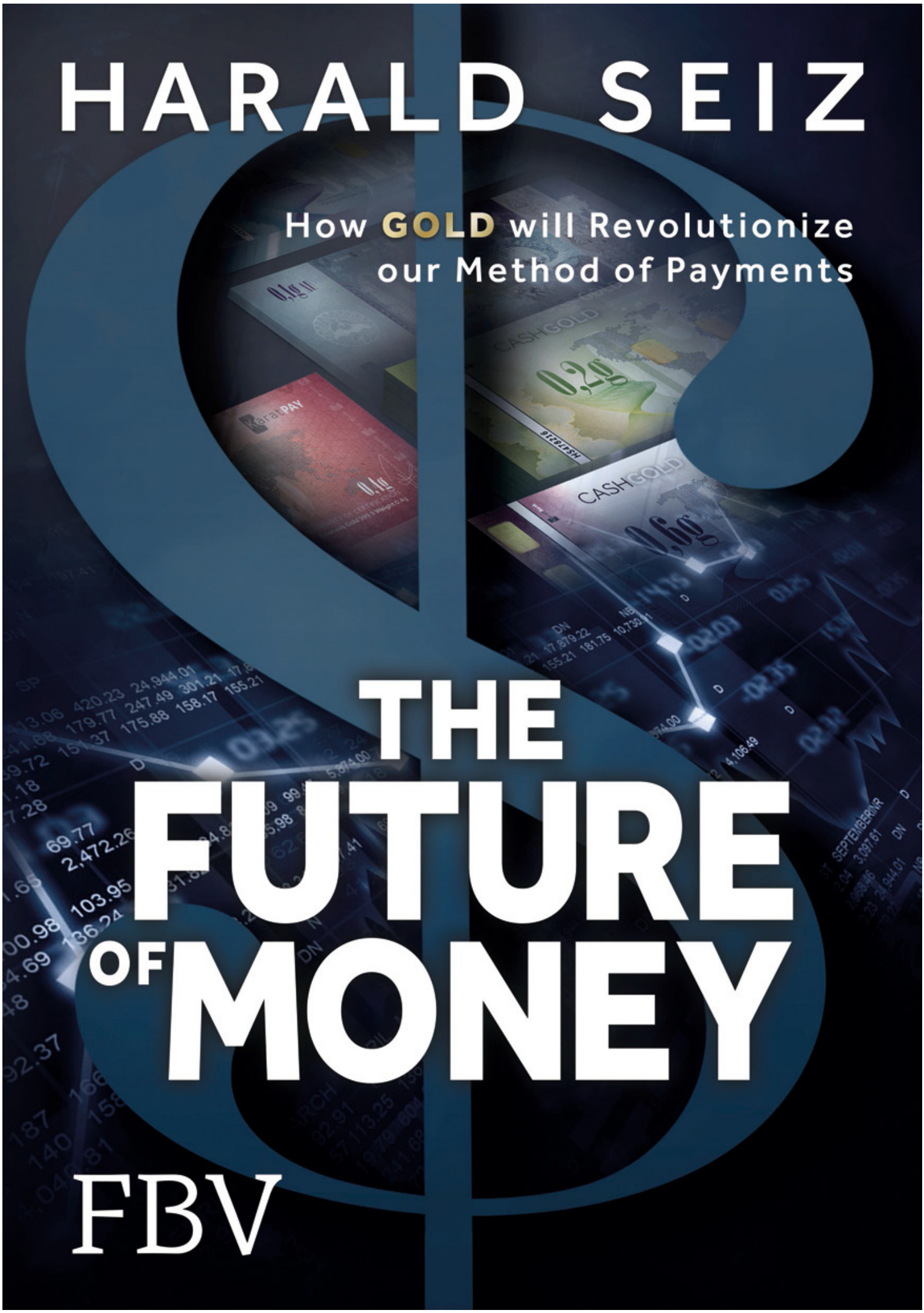
HARALD SEIZ
How GOLD will Revolutionize our Method of Payments
THE FUTURE OF MONEY
FBV

5. Crises and Catastrophes— How You Can Prepare

Currencies don't have it easy. Not only do they depend on monetary policy affairs, the economy and financial markets, they're also exposed to the general global situation as well as to all types of criminals, who I will talk more about in the next section. You don't have to explain to anyone that wars, uncontrolled flows of migrants, crises and attacks now make us feel insecure even on our own doorstep. All this causes millions of cases of suffering and sets back many people and societies for decades and, naturally, also their national economies and especially the infrastructure. Nobody can build up anything for themselves in places where uncertainty and terror prevail. In such places, apart from archaic forms of retailing and generally having to muddle through, there is a complete absence of entrepreneurial spirit and even regular investments.

All these interconnections are obvious. Yet, it's precisely these adversities and human tragedies, which are moving ever closer that, once again, demonstrate how necessary it is to be ready for all eventualities. This is because, when viewed historically, our life in peace is unfortunately an exception. However, as a consequence, we've forgotten how to prepare ourselves for crises. Our government is not only unable to pursue responsible and sustainable economic

and social policies, evidently, it can also no longer sufficiently protect our lives and social coexistence. We have to adapt to this situation—not just with stockpiles, which even the Federal Government is propagating, but also financially. Even I cannot look into the future here, nevertheless, I can only advise everyone to prepare themselves well financially with the right mix of cash, in different denominations and currencies, but also real assets, including gold. I also have to be prepared for an electronic banking system outage, whether this is because there's been a hacker attack, or because there's no power any more. Moreover, I also have to make provision in case there are food shortages. Anyone who has at least 100 liters of water as well as canned goods in the cellar and also a clever mix of money and assets, with which it would be possible to buy something when times are hard, would not need to reproach themselves very much in an emergency. Later on, I describe various possibilities and recommendations in terms of money that supplement the German Federal Government's "Civil Defense Concept."

How Secure are our Payment Systems?

It's interesting that when someone brings the abolition of cash into play, this always causes quite a stir. In actual fact, for a long time now, banking—not our private payment transactions—has been organized in a way that is exclusively electronic and digital. From a purely technical perspective, our money is already virtual and appears only as 0 and 1 in the computer systems of commercial and savings banks. The crucial thing, besides the value of our savings, is having access to them at all times. Ultimately, one of the first measures that the state usually imposes is to place restrictions on cash withdrawals. In the eurozone we experienced this in 2013 in Cyprus and, in 2015, in Greece—I discussed this in chapter 2. The aim of this section is to describe how cyber fraudsters and hackers try to extract money out of the digital system.

Indeed, they are no longer content with just a couple of hundred thousand euros that you could steal in a traditional bank robbery. The amounts involved here are staggering. Nevertheless, private online banking in Germany is secure—which is amazing when you consider the vehemence of the attacks. A whopping nine million malware attacks on German online banking platforms are carried out each month. Nearly all of them are repelled and the losses amount to just 0.01 percent of the transaction volume for all German institutions, as Hans-Joachim Massenberg, a member of the Senior Management Board of the Association of German Banks, reported at the *Bundesbank's* payments symposium in 2015. "The banks' servers as well as the communication channels from banks to their customers are basically secure."[146] However, this leads to criminals switching to the weakest link in the chain of online payments, namely, the customers. Moreover, the industry fears that the emergence of new online payment processing service providers will exacerbate the security problems. Indeed, in the case of Bitcoin service providers we've seen how young companies can provide potential targets. Furthermore, the industry representative, Massenberg, sees risks if ever more third-party services obtain access to a bank account. These risks stem not only from hacking but, for example, from spam e-mails to which users respond.[147] It's obvious that additional links in the payment chain weaken the entire system, although, we've seen that in the long term other parts could disappear completely. We're not there yet, however, and the organization of worldwide payment transactions is becoming more vulnerable through new players.

The Risks of Digitalization

Attacks on our vital infrastructure are not ideas thought up by science fiction authors and conspiracy theorists. The more heavily we depend on computers in the different areas of our life—and soon this will also extend to our refrigerators—the more potential targets we provide for attackers. In this context, the example from private

households is very real because that is frequently where the criminals begin their activities. Naturally, cyber-terrorists don't usually set out to nose around our personal environment, or even to play a trick on us. Nevertheless, as was demonstrated by the 900,000 Telekom routing devices that were paralyzed at the end of 2016, the appliances in our households are being used *en masse* to carry out attacks on other systems, namely, through a botnet—a group of malicious programs. As a next step, the targets of these actions will be essential facilities: electric utilities, hospitals, water supply companies, television broadcasters and banks. Through the hundreds of thousands of computers, routing devices and appliances they will be weakened, first, in preparation for an attack. The motivation of the perpetrators for this could be to cause chaos for a political aim, or they might simply want to steal or extort money.

However, the growing—convenient and often cost-saving—interconnectedness between our countries, devices and industries means that the systems are becoming more susceptible to cyber-attacks. The expressly decentralized nature of the Internet and the fact that there are a hundred thousand different IT service providers afford no protection here. This is because, ultimately, they all rely on a handful of IT systems, software programs and a modest number of server farms. Therefore, the benefit of a decentralized network, which can continue to function if one element fails—the basic principle of the Internet and networks generally—is reversed into its opposite. Only at the beginning of March, were we able to experience this vulnerability once again when the Amazon subsidiary Amazon Web Services (AWS) had massive computer problems (due to a trivial typo) and had to be rebooted as a result. Yet, it was not only Amazon customers who were left high and dry for four hours but also the users of Expedia and Snapchat who rely on this cloud service from Amazon.

Besides telecommunication companies and banks, electric utilities appear to be a particular object of attack. According to the German daily newspaper the F.A.Z.: "Experts have been warning of hacker attacks specifically on companies in the energy industry. In-

adequate IT security at the utilities constitutes an increasing risk of blackouts. (...) Contrary to what is readily claimed in public, many of the energy suppliers are still not adequately equipped to defend against cyber-attacks," from a quote by Oliver Neumann, a spokesman for the IT consultancy Recurity Labs, in Berlin.[148]

Attacks on Banks: Data Blackouts and Cyber Criminality

The situation at the banks is no different, as the many digital bank raids in recent years have demonstrated. According to the F.A.Z, the *Deutsche Bank* CEO, John Cryan, has described the IT systems at his bank as being "lousy."[149] Nevertheless, up to now, there have not been any reports of spectacular digital robberies from there. Unlike what happened, for example, at NASDAQ—the biggest US technology-focused exchange—which shut down for a half day on August 22, 2013. To-date, nobody has given its customers, such as investors, a credible explanation as to what actually happened there. The gold expert and best-selling author James Rickards, who we became acquainted with in the chapter on gold, suspects that the computer malfunction behind this shut-down had not been a regular one but, instead, a cyber-attack by either criminal hackers, or even the Chinese or Russian military.[150]

It doesn't matter whether they act on their own or on behalf of another country, these days, gangs are not turning up with pistols or blowtorches, but with IT programs and equipment that are highly sophisticated. Cyber-attacks have seen a sharp increase—in 2015, IT security incidents worldwide increased year-on-year by 38 percent.[151] It's hardly surprising, then that communications security is the issue right at the top of supervisors' agendas. Mary Jo White, the head of the American exchange supervisory authority, the SEC, described cyber security as being the biggest risk to financial stability. What she had in mind, here, was not only the banks, but also the exchanges, trading platforms and clearing houses. The SEC chair believes that there is a lot of catching up that needs to be done here to enhance the security of systems. The situation is so serious

that, in its report on financial stability, the *Bundesbank* warned that: "Cyber risks result from attacks on data and IT systems and can compromise their confidentiality, integrity and availability. (...) Cyber-attacks are also used as a means of spreading misinformation and to manipulate share prices, for example."

Naturally, cyber-attacks on systemically important market participants are particularly significant. Failures there could destabilize the system as a whole, for example, if systemically important services or transactions between banks could no longer be provided. For example, this can result in the emergence of liquidity and credit risks, which can spread throughout the financial system. Naturally, cyber-attacks can also damage the reputation of relevant organizations and lead to a loss of customer confidence. This doesn't even have to be the result of fraud, but can also include, in particular, the targeted spreading of rumors on social media networks or, frequently, on obscure online financial portals. There you can also find again the "old-school" extortionists who combine the classic protection racket model with the opportunities that the Internet provides. They deliberately give false information about financial products if, for example, they're not awarded a lucrative consulting contract. This was the method employed by Heinz Gerlach, for example, who "successfully" blackmailed issuing banks over three decades, even though he was convicted several times; he died in 2010. People with similar practices are still out there. While the effects here are not systemically important, for the respective fund provider they are, nevertheless, always serious. A concerted smear campaign—for example, one that suggests that a bank is at risk of insolvency—can quickly result in a run on a financial institution.

While the evil fantasizing of extortionists, who are often market participants, cannot be eliminated through state-imposed restrictions but, in fact, through protracted and costly legal proceedings (in the case of Heinz Gerlach even this didn't help), nevertheless, there are rigorous guidelines regarding the technical aspects. These days, the banking supervisory authority and the *Bundesbank* no longer examine only the liquidity and competence of financial service pro-

viders but, also how they equip themselves to defend against cyber risks. Ultimately, protection against such attacks is just as important as the provision of equity and collateral. The list of institutions that are involved extends right up to the German Federal Office for Information Security. Internationally, there is a myriad of different bodies that concern themselves with IT protection—*the Bank for International Settlements* and, there, the *Committee on Payments and Market Infrastructures*, the *International Organization of Securities Commissions* and even a Working Group of the G7 countries—not always with the commensurate success as we'll see shortly. The G7 commission developed the fundamental elements of cyber security for the financial sector and the finance ministers and central bank governors of the G7 states adopted this. The issue of cyber security has also finally prompted the banking supervisors at the ECB to take action. They want to set up a database of cyber-attacks.[152] Nevertheless, the hits are getting closer because, evidently, it's too tempting for criminals using sophisticated programs to mount a $100 million heist on the other side of the globe.

USA 2012

In 2012, a concerted attack, which was supposed to overload computer networks, hit three large banks in the USA at the same time: The Bank of America, Chase, Wells Fargo and a number of others. At that time, it was the costliest assault of this type; however, it "only" resulted in massive commercial damage though neither money nor customer data were stolen. The banks lost a lot of money because the systems had to be restored and the customers were not able to conduct banking transactions. It was similar to a burglary where the criminals vandalize the house but don't take anything. In this case, too, the attack was launched via hijacked servers that barraged the banks with data traffic. Subsequent to this so-called distributed denial of service (DDoS) attack, the networks had to shut down.

South Korea 2013

In 2013, a malicious program called "DarkSeoul" paralyzed banks and cash machines in South Korea. TV stations were also affected and, therefore, the software was responsible not only for gridlock in public life but also for turmoil and chaos. Unlike the attacks in the other examples, this one was carried out in an exceedingly simple way. The antivirus programs of the targeted computers were switched off, then their data was deleted and the devices were simply shut down. What was really unusual, however, was that completely different computer systems, namely Windows and Linux, were compromised at the same time.

The Biggest Bank Heist in the World: One Billion Dollars (2013–2015)

Considerably less known, paradoxically, is the story of the biggest online bank heist in the world (and indeed, generally) where, apparently, one billion dollars changed hands illegally, mainly in Russia and the USA. In the investigation, Kaspersky, a Russian company specialized in security software that was working with the law enforcement agencies, was able to distinguish itself. The heist was preceded by a coordinated attack, lasting two years and organized globally, on 100 banks in 30 countries. The name given by experts to the gangster ring, which had struck before, was *Carbanak*.

The multinational group deployed malware that, months before the heist, was smuggled into the computers of system administrators and bank employees. Once the software was installed, it was possible to manipulate the computers remotely in such a way that the gangsters, or rather their computers, could masquerade as bank employees and were able to conduct transactions. The "incubation period" was used, primarily, to learn how the systems, the target computers and their users worked in order to carry out the heist later and, in one case, to steal ten million US dollars.

It was extremely clever, easy to adapt and, unfortunately, very successful—the kind of story you would expect in a Hollywood

film. As always, you automatically ask yourself just how much good could be achieved if this criminal energy were paired with great professionalism and creativity, instead. In some cases, the hackers even got access to the ATMs system. Naturally, they didn't drive up to the ATMs in person to pull the money out of the slot—which would have taken a long time in view of the sums involved—but, instead, they channeled this money to their target accounts. They didn't even use malicious software for this but standard tools with which you can control and test ATMs. On top of this, they used proven remote maintenance programs, which were on approved lists and, therefore, went unnoticed. The attackers got such wide access to the internal banking network that they were even able to watch the video surveillance of the system administrators and could see what they were doing and what was happening on their monitors. They recorded all of this over months.[153]

It's alarming that none of this leaked out until they had disappeared with the loot. In the pre-digital era, criminals at least had to use weekends and public holidays for this while, these days, it's apparently possible to perpetrate a crime, for months on end, virtually under the noses of the victims.

Russia 2016

At the beginning of December 2016, unknown hackers stole two billion rubles (29.2 million euros) from Russia's central bank. They cleared out the accounts by means of counterfeit access codes. Nevertheless, the Russian domestic secret service, the FSB, was able to thwart bigger cyber-attacks on Russia's banking system that were supposed to follow in a second wave.[154]

Over and over again and in this case, too, the question arises: Who's behind these attacks? Of course, the domestic authorities are quick to come up with suspects, in particular, with respect to traditional political enemies. However, there is of course rarely any evidence for this because covering your tracks is an important part of the job.

SWIFT: Bangladesh/Vietnam 2016

At the start of 2016, US$ 81 million were successfully withdrawn from the Bangladesh central bank through SWIFT—the international payment system of the banks. This was due to inadequate security measures, however, what is more alarming is the fact that all this was played out through SWIFT, which was attacked by the hackers. This cooperative, which is supported by banks worldwide, ultimately had to warn its customers, admitting that a weak spot in its customer software had been the cause and that an update was necessary.

Originally, the digital bank robbers, who were, unfortunately, all too real, even wanted to steal US$ 951 million and had already sent the appropriate payment instructions for this. However, a large portion of the transfers were blocked and, in the end, "only" US$ 81 million went missing. According to the information, the computers at the central bank had serious security flaws.[155] This would appear to be an understatement because, evidently, old switches costing less than ten dollars each were used by the central bank, which had no firewalls whatsoever.[156] In the end the governor resigned.

At the end of 2016, the Vietnamese Tien Phong Bank received fraudulent requests for transfers of more than a million euros. There are theories that the hackers were in North Korea, something that was also suspected during the attacks on South Korea, in 2013. This has not been proven, however. In Vietnam, just like in Bangladesh, SWIFT was used for the heist. This provider connects more than 10,000 banks around the world and it plays a key role in international transfers. The institution is organized as a cooperative and is headquartered in Brussels and operated by 3,000 financial institutions. Therefore, its remit is to process payment transactions and to do so securely.

Institutions normally send encrypted messages via SWIFT and these effect cross border payments and other transactions. However, the cyber-attacks by means of SWIFT messages have alarmed banks. According to a report in the Wall Street Journal, the big American bank, JP Morgan, has limited access to SWIFT to spe-

cifically authorized employees. At the other banks, too, the SWIFT systems are currently under review. This is also likely to be the case at *Deutsche Bank*, as it's one of the largest transaction banks in the world. The German daily newspaper the F.A.Z also wrote that: "Following recent incidents, the important SWIFT customers, including the American and European banks, expect reinforced security measures. Clearly, there are concerns that the next hacker attacks will no longer be restricted to banks in developing countries. Doubts about security would be a disaster for SWIFT."[157] Since, based on the attacks, it is possible to deduce that there is very good knowledge of the internal banking systems. It is thought that, in the above cases, spy software (malware) was smuggled in through the banks' PDF readers. According to a report, the hackers also had secret SWIFT codes for at least seven other banks. What is more, the response from SWIFT reminds us somewhat of the problems that Bitcoin had. According to SWIFT, its own system was not affected, however, the banks should check their own security measures for their fund transfer systems.[158]

Interim Conclusion

The financial sector depends on well-functioning IT systems. SWIFT is a symbol here, both for our interconnected world and for its vulnerability. There are around 200 national banks and tens of thousands of commercial banks. However, if their most important representatives are connected with each other through only one single channel, just one attack could lead to a worldwide systemic domino effect. I find this more disturbing than attacks on newcomers to the Bitcoin movement. Nevertheless, nobody is questioning this system, as we seem to have gotten far too used to it—along with all types of fraud.

My comments on cyber-attacks have demonstrated how vulnerable IT systems are. With its "Civil Defense Concept," which I will address shortly, the German Federal Government is also thinking about such attacks in general. It has, therefore, told the operators

of important infrastructure to take good note of the general requirements, which apply especially to banks, as well. "In view of the large number of potential causes of outages or disruptions, the utility services should be set up, structurally, in such a way that the overall system is operable and regenerative in spite of disruptions. All operators should assume responsibility, voluntarily and at their own initiative, for an adequate level of security in their spheres of competence. On the basis of a necessity assessment, the state will impose specific conditions in order to enhance the resilience and security of critical infrastructures."[159]

It remains to be seen if these requirements will also provide protection against attacks on computers by extremely clever but misguided IT criminals. The attitude of James Rickards was predictable. He believes that the threat of a financial cyber war is "another reason to own physical gold because it's non-digital and you can't hack it or erase it."[160]

What Should You Do in a Crisis?

In the previous section, I discussed the disasters that, from time to time, are already happening, now, in the IT systems of the banks (in terms of the sums involved, the staff and technical costs and the huge effort involved, these can already be considered as real wars). In the following section, I would like to outline what can blow up in our faces in "real life" during a fully-fledged crisis and how we can best gear up for this. I may seem like a prophet of doom, however, in my function as a business owner I've always been, and still remain, optimistic. I believe that people are constructive at heart, and based on my experiences as an owner of a medium-sized enterprise, I also know that I have to plan for many eventualities and contingencies so that I can guide my ship to a safe haven. If I'm passing through periods of especially fair weather (which is rarely the case with business challenges) that's wonderful. However, if there's a storm approaching then I need to have the right equipment and

a competent crew on board. In figurative terms, this would be my insurance policy and I would ask you, please, to understand my personal recommendations, in this chapter and the next one, in this way. As is generally known, with insurance you're glad when no damage or loss occurs, conversely, however, damage or loss won't drive you to ruin if you've paid your insurance premiums. In our upcoming examples and scenarios concerning financial provisions for a crisis, the insurance premium is actually something you can hold in your hand. While it changes its value from time to time, apart from that, it doesn't get old and doesn't need elaborate and costly maintenance like a ship does, for example.

The German Federal Government's "Civil Defense Concept" (KZV)

Before we come to the provisions for the average person, we should take a look at official activities and plans in the event of crises and disasters. Ultimately, it is first and foremost the task of the state to take responsibility for and to organize the provision of public utilities and public services. The duty of a government to protect is part of the constitution. However, we should certainly not sit back and relax as a result. After all, in recent years we've seen how the current German Federal Government has repeatedly broken laws and, in the opinion of former constitutional court judges, also violated the constitution. *Made in Germany* and our world famous German efficiency have become tarnished.

In August 2016, the "Civil Defense Concept" (KZV) surprised many citizens. Many Germans still believed that they were living on the Isles of the Blessed. In this respect, the German Federal Government acted responsibly by producing such a concept, on the other hand, it naturally caused uncertainty—something that the competent Federal Minister of the Interior, Thomas de Maizière, had almost proverbially wanted to avoid elsewhere. This is because, for somebody who grew up in a society with comprehensive insurance

cover, the scenarios and eventualities that are described there are unbelievable.

In practical terms, the concept comprehensively describes how all the important bodies that are legally and economically responsible for infrastructure and the provision of public utilities and public services should prepare for an emergency. This ranges from hospitals, security authorities, electric utilities and transport companies right up to banks. The concept sets out in detail what needs to happen if something goes very wrong. This includes obvious things that would be dictated by common sense that have, however, now been placed within a firm framework; and the pertinent legal foundations and obligations, such as, the *Emergency Postal Service & Telecommunication Control Act* and the *Emergency Food Control Act*. I would recommend that, for a start, everyone take look at this 70-page document and assess for themselves what would be beneficial for them. The document also shows, in particular, what incidents the German Federal Government believes could happen. Moreover, up to now, the German government has not been known for being a scaremonger but has tended to allay concerns in the face of risks (including those to which it is a contributor). In spite of this, it tells us nothing about how probable it is that such events could affect us.

The current document replaces the last new civil defense concept form 1995 that was still characterized by the "easing in security policy after the end of the Cold War." As a result, many civil defense structures and institutions were dismantled. The terror attacks in New York and Washington, in 2001, and the floods in the summer of 2002, were the reasons for producing a new concept that, at the same time, highlights the range of "damaging events." While the number of natural disasters in Germany has remained relatively stable and manageable, the report continues nebulously that: "Over a period of more than ten years, the security policy environment has changed again."[161]

The Civil Defense Concept provides only a rough guideline for detailed functional requirements and specifications. The ultimate

objective here is "to maintain state and government functions and to supply the public with essential goods and services." Besides the traditional military threats, the Civil Defense Concept follows the threat assessment of the German Federal Government and the "changed security situation" as described in the "2016 White Paper on Germany Security Policy and the Future of the German Army (Bundeswehr)": "With a view to national defense, special attention was given here to hybrid threats by both players at the government level as well as non-government players. It is the responsibility of civil defense to organize itself so as to be able to repulse these new dangers without neglecting its duties with respect to traditional national defense and alliance defense. The growing vulnerability of modern infrastructure and the dependence of modern societies on resources provide many potential targets for attackers."[162] Besides attacks with weapons and mass destruction weapons, in particular—as described in the previous section—"cyber-attacks and the outage or disruption of critical infrastructures" are mentioned.

Indeed, when reading about the "hybrid threats" that are described you can easily begin to get scared. In the minds of the civil servants from the Federal Ministry of the Interior our idyllic world already appears to be history:

- a variety of open and covert attacks,
- a combination of conventional and irregular forces/capabilities,
- a combination of military and civilian means,
- a focus on vulnerable structures as potential targets,
- the complexity of potential scenarios of damages,
- complicated perception and classification,
- short or absolutely no warning times.[163]

In addition, there are potentially damaging events of an entirely different nature, in the truest sense, namely, chemical (C), biological (B), radiological (R) and nuclear (N), or CBRN to use the military jargon.[164] In December 2015, the NATO foreign ministers published a strategy (on which this concept is based), for combating

these threats of war. According to this, the following basic capabilities have to be safeguarded above all:

- maintenance of state and government functions,
- supplies of food and water,
- supply of energy,
- provision of communication services,
- provision of transport services,
- dealing with displaced persons and population movements,
- management of mass casualties.[165]

Keeping banking and the supply of cash going is not mentioned at this point. However, further on in the document, both aspects are discussed in an appropriate way.

In this book, I wanted to explore and describe how we would finance our daily life in an emergency, so I singled out the topic of "food" as the most important aspect. Later on, we'll still need some statements from the German Federal Government and that is why I'll be quoting from it extensively. According to the Civil Defense Concept:

"Basic food supplies will be provided by a large number of food producers and food retailers without any particular minimum requirements. The supply will continue for as long as possible by the privately organized industry through the free market.

If the German Federal Government determines that the supply of basic provisions to the public can no longer be ensured through the free market then the public would be supplied with essential foods by the state. It would take control of food production and food distribution in order to achieve this. The German Federal Government may issue regulations pertaining to the entire food supply chain that place disposition restrictions and impose provision obligations with respect to the farming, processing, distribution and sale of foods. Furthermore, the competent enforcement authorities will be granted temporary powers of intervention that would extend to the right to issue regulations accordingly. The legal bases for the

state food emergency preparedness would have to be adapted, accordingly.

To ensure that there is a basic supply of food the German Federal Government can hold its own food reserves.

Ultimately, the self-protection of the population should be reinforced through appropriate state measures. People are asked to hold an individual stockpile of food that would last for a period of ten days in order to be able to support the measures taken by the state with the appropriate self-provision."[166]

Unfortunately, the reality behind this directive is significantly relativized in a major report by the German *Bundestag* (parliament), which I enlarge upon subsequently. There it says: "The increased demand makes the food retail industry the weakest element in the food supply chain. Serious food supply bottlenecks can be expected after just a few days. (...) Despite best efforts, however, it is highly unlikely that it will be possible to ensure satisfactory extensive distribution of food supplies to meet requirements."[167] Therefore, private provisions—not only of food but also of the means of payment – would appear to be urgently needed.

The basis of civil defense is "the ability of the public to protect and to help itself (and one another) until skilled assistance arrives, usually organized by the state."[168] The essential basic necessities here are drinking water and, as already mentioned, food, as well as medical provisions. It's only afterwards, understandably that the focus moves on to the aspects of a "minimum provision of public utilities and public services" which is also the core topic of this book:

- post and telecommunications,
- storing and processing data,
- supply of cash,
- garbage collection,
- waste water disposal.

The Supply of Cash

I don't how the order for the list of the "minimum provision of public utilities and public services" was determined, it obviously wasn't alphabetically. It's noteworthy, however that the supply of cash at least still crops up before garbage collection and waste water disposal. In order to understand my general topic of "money and precautionary provisions," indeed my basic idea, I believe that, at this point, it's extremely important to quote in full the government's plans for the supply of money. After all, it shows what's included in the (theoretical) guidelines for the *Bundesbank*, credit institutions and their service providers and what isn't, in other words, what you have to take care of yourself.

"According to the German Banking Act (*Gesetz über das Kreditwesen*, or KWG), individual credit institutions are required to perform banking operations and financial services properly. This includes the paying out of deposits. Provision has to be made for this. Currently, every institution determines for itself which risks it rates as critical and to what degree. If a credit institution classifies problems with the supply of money to its customers as a critical area for the institution then it has to have at its disposal the appropriate emergency and contingency plans. This then also applies to business areas that have been outsourced such as, for example, the filling of cash dispensers by cash-in-transit companies. There is no obligation to have a cross-company emergency plan ready in the event of a crisis situation that would contribute toward maintaining and restoring the overall movement of cash.

According to Section 3 of the German *Bundesbank* Act (*Gesetz über die Deutsche Bundesbank*, or BBankG), the *Bundesbank* shall ensure the processing of payment transactions conducted by banks in Germany. It is responsible for providing the necessary funds, or accepting the funds that are delivered at the counters of its 35 regional branches. For this purpose, the *Bundesbank* holds cash reserves in all denominations for its account holders (credit institutions, authorities, payment service providers and personnel). Furthermore, there are strategic cash reserves at the eurosystem level.

With respect to the supply of cash, for its own operations the *Bundesbank* has very comprehensive precautionary measures for dealing with risk and crisis management plans as well as business continuity strategies. Above all, these strategies are geared toward ad hoc measures during shorter crises (one to a maximum of five days) and, in this way, provide lead times for adopting measures in the event of crises that go on for a longer period of time.

It cannot be guaranteed that the *Bundesbank* itself could supply cash to the public directly throughout Germany (e.g. the 35 branches that the *Bundesbank* currently has would be completely insufficient when compared with the approx. 50,000 ATMs plus over 30,000 bank branches; a reciprocal offsetting/debiting option for individual citizens doesn't exist). That's why a functioning logistics infrastructure (which is not within the *Bundesbank's* sphere of influence and includes both the credit institutions as well as the cash-in-transit companies) is absolutely essential for the orderly supply of cash to the public.

The distribution of cash to the public is carried out through credit institutions that usually rely on cash-in-transit companies to transport the cash. Owing to the enhanced automation (e.g. automated teller safes in bank branches or ATMs) the options for paying out cash in a crisis situation could be affected. Therefore, it is vital to ensure IT system availability and the supply of energy to the credit institutions and the cash-in-transit companies. (...)

Against this background, it is necessary for all the private sector stakeholders within the cash cycle (the credit service sector and cash-in-transit companies) to be included in the general crisis preparedness. These stakeholders should also undertake to play a part in creating a comprehensive crisis program for the overall system for the provision and acceptance of cash (cash transactions)."[169]

Assessment

From the perspective of a citizen and a business owner, I feel that the reflections on the supply of cash (but also the overall concept)

are adequate for the moment. It shows everything that has to be done, but also where the limits are. You can't prepare yourself in terms of staff and logistics for all eventualities and the monstrosities of Islamic terrorists—and certainly not mentally. Each catastrophic event is unique and if a big system failure occurs, in the general sense (caused by people, it certainly won't be a natural disaster), nobody, today, can assess how the momentum would unfold. An ordinary member would only be able to do all that is humanly possible and, ideally right away, today, to at least mitigate adversity. In the next section and in chapter 6, I'll demonstrate what this could be, specifically.

At the same time, it is worrying that the German *Bundestag's* report on the consequences of a blackout for important areas of our lives comes to a general verdict that is negative: "Disaster management by the authorities suffers considerably from the lack of a uniform picture of the situation; this also significantly hampers interregional planning and coordination of measures."[170]

Incidentally, it's interesting that the German Federal Government is urging the public to stockpile enough food supplies for ten days. Such advice is completely missing in the "Supply of Money" section, although that would be much easier to accomplish and would also require less storage space than a 10-day supply of canned goods, pasta and water, which I also advocate, of course.

By the way, as you will have read, the German Federal Government is also giving some thought to the issue of "accepting" cash. On this point, I consider the "Civil Defense Concept" to be pretty unrealistic.

A Blackout—Results of a Study by the Berlin Institute of Finance, Innovation and Digitalization (BIFID)

In an emergency, i.e. when the infrastructure of the banks breaks down for a period of several days, it will no longer be possible to supply enough cash to the public. That is the key finding of an academic report titled "Alternative Means of Payment in the Event of an IT Blackout" from the *Berlin Institute of Finance, Innovation and Digitalization*, which specializes in research on the digitalization of economic processes.[171] The loss of confidence in a currency that we have mentioned, in general, so far in the other chapters, could cause—under certain conditions—rampant inflation according to the study titled "Alternative Means of Payment in the Event of an IT Blackout."

What should not be underestimated, in this case, although it's not part of this study, is that there will be a process with its own dynamics—which has been described already several times—and the all-too-human reactions. There would be a run on the supermarkets, the people would stockpile, and the supplies would barely be replenished as, ultimately, the payment systems would have broken down. Merchandise would become scarce and, consequently, the prices would go up further.

We would, therefore, experience classic inflation caused by high demand, scarce supply and a loss of confidence in the currency. Therefore, one conclusion that the authors draw from this is: "in an emergency situation, precious metals would offer protection against a loss in value."

Naturally, these are all just scenarios and as with household insurance, which helps in the event of a burglary, we hope that it will never actually come to pass. And yet, it's easy to prepare for this – almost like taking out insurance cover at the click of a mouse – with an appropriate mix of different currencies and precious metals. Let's hope that we'll never need these, but with them you'll at least be able to sleep more soundly.

The researchers at the institute, which is part of the Berlin School of Economics and Law (*Berliner Hochschule für Wirtschaft und Recht, HWR*), simulated thousands of scenarios of what could happen if the entire banking system were to come to a standstill. (It's quite possible that this would be caused by a wide-ranging power outage—a "catastrophic event" that, in turn, was explored in a separate and very comprehensive report from the German *Bundestag* that I discuss in the next section). Not all the scenarios necessarily lead to great distress and many things can be quickly restored. Yet, the momentum of the situation is key as well as the potentially fatal combination of different factors. This is because computers and power grids don't usually simply break down just like that (unless there's been a typing error), but precisely because someone has launched an assault for a particular purpose or with an agenda. If there are also attacks, as we have already experienced, then panic is not far away.

In our civilization, we've become used to having all the basic amenities constantly available. It's quite natural for us, therefore that we don't even think about it anymore that there are complex systems and masterly feats of logistics behind them. These are all features that we've created ourselves and we can be proud of them. We use them and we lead modern lives, however, we don't think about what would happen if parts of our society were to break down and the domino effect that would then ensue.

Our Cash Reserves

According to the statistics, each German citizen carries around, or has at home, a total of 103 euros in cash.[172] That's relatively little, given that there's one billion euros of cash in the eurozone. However, most of this is stored in the vaults of banks and, in particular, retailers, or even outside of the eurozone. If the ATMs and card readers at supermarket check outs were to stop working for a few hours then that wouldn't be the end of the world (see next section). However, what would happen if this were to last longer and was

coupled with other incidents? The researchers at *BIFID* gave this some thought and undertook some highly complex simulations that covered three, five and ten days of chaos in each case. The starting point was the question of how much cash and in what form is needed to withstand a period of up to ten days in a "data crisis situation" where there are restrictions on the sourcing of cash. To come straight to the point—103 euros is not enough, neither the 103 and certainly not the euros.

Furthermore, there is also the simple statistical fact that the above-mentioned figure is an average value. Therefore, there are many people who have nothing whatsoever in their wallets—not because they're poor, for example (which certainly raises the probability, see chapter 2), but rather because it will have been a few days since their last visit to the ATM. People who have 200—300 euros in their wallets, in turn, won't be able to help you, quite literally.

What should be done, then? And anyway, what would happen to prices and our food supplies in the event of a blackout?

A smoothly functioning financial services sector is an essential part of our daily lives. In chapter 2, I described how intricate and complex the network of credit institutions and service providers is. This includes the banking services system that covers the payment transactions between employers, employees, banks and borrowers. Participants in systems for payment transactions and data transmission include payers, payees, banks, clearing organizations and central banks. Although the number of banks in the system is enormous, the risks are supposedly spread out, in actual fact, risk minimization is limited, as we have already seen in the case of SWIFT. This is because, these days, banks rely on clearing centers and on centralized server farms for storing data that are admittedly highly secure—except until a resourceful hacker, on his own or on behalf of a hostile government, proves the opposite. However, the risk also lies in the system being overloaded with incredibly high volumes of data (a *distributed denial of service, DDoS, attack*), or a system breakdown, which can be internal or even caused from the outside.[173] However, according to the BIFID researchers, in a crisis, the threat

doesn't necessarily lie in the total breakdown of all systems. In fact, the unexpected breakdown of individual but important components of the banking services and data transmission systems should also be understood to be part of this risk.[174]

It would be bad enough if all of this were to break down. It's obvious that I then wouldn't be able to make electronic bank transfers any more, or that a shop wouldn't accept my credit card because the card reader would no longer have access to the central computer. However, I would also not be able to get hold of cash any more as most of the ATMs—namely, those not connected to a bank branch and, therefore, to an emergency power system—would stop working immediately. Naturally, in that case, as mentioned already, you could fall back on the clerks at the bank counter. Yet, even if all the available staff from the call centers were ordered back to the bank branches, you could well imagine how long the queues would be, how complicated and tedious proving your identity would be and how long it would take to fill out the forms. (There is a more precise simulation of what would happen in the "*Bundestag* report" from which we've quoted extensively in the next section.

Therefore, the supply of cash would come to a standstill, especially as we still haven't talked about the fact that the banks would also run out of cash, eventually, and their supplies would need to be replenished. Moreover, people will want to withdraw as much cash as possible, which would presumably be a limited amount, however, then all the members of a family would simply queue up one after the other. I don't have to continue outlining this scenario as everyone can envision the ensuing chaos that they would be subjected to, to just be "solvent" again—something that, only a few days previously, could have been done easily and without a great deal of thought, because the process is so automated.

"The functional structures of the financial services sector—combined with the use of modern Internet-based technologies—give some idea of how dependent these systems are but, above all, their risk proneness," say the researchers.[175]

High politics has addressed this topic not only in relation to civil precautions but also with respect to a power outage—which could indeed be a realistic reason for a system breakdown and, therefore, could effectively constitute a potential target for an attack—and flanked it with academic research. In 2011, under the simple title of "What happens during a blackout," the *Office of Technology Assessment* at the German *Bundestag* examined the "consequences of a prolonged and wide-ranging power outage," namely, for the essential parts of our infrastructure. One of the core messages in the report is: "The financial services sector is heavily dependent on a continuous and stable power supply. This is due to the mains-based information and communications infrastructures used for communications, for data management, for tracking and controlling flows of goods and money and for the transmission of payments and data traffic. These information and communications infrastructures represent the sector's 'nervous system.' A failure of these infrastructures and the resulting difficulties in providing, or the inability to provide key financial services would have serious consequences for industry and society."[176] If these systems were to break down, or if they could function only to a limited extent then we would be talking about a data crisis.[177]

At this point, the German Federal Government's Civil Defense Concept would come into play. We recall that the individual credit institutions, "according to the German Banking Act (Gesetz über das Kreditwesen, or KWG), are required to perform banking operations and financial services properly (...) This includes the paying out of deposits. Provision has to be made for this."[178] Therefore, according to this concept, it is up to the credit institutions themselves to determine the supply of cash. In view of the financial crisis in 2008 and the continuing euro crisis and, related to this, the supply of cash to the Greek public, in 2012, critical questions had to be asked in the course of a careful examination of these issues, as the BIFID authors remarked.[179]

Private net financial assets are EUR 47,681 per capita in Germany.[180] Firstly, it could be argued that this is reasonable credit-

worthiness (when compared with other countries). However, this wouldn't help me at all as, during a crisis, I would have no access to this. Thus, the principle set out in financial textbooks that "liquidity ensues from creditworthiness" would be abrogated, as the BIFID experts laconically observed. By logical implication, therefore – cash is, indeed, king. Yet, the *Bundesbank* and the commercial banks would hardly be able to organize a proper supply of cash—with or without the *Bundesbank* Act and the Civil Defense Concept. That is what the authors at the Office for Technology Assessment wrote in their report, too.

Well, what happens then?

Alternative Means of Payment

According to the definition of the *Bundesbank*, "legal tender" is the designation for the means of payment that "nobody can refuse to settle a monetary obligation without experiencing legal disadvantages. In the eurozone, euro banknotes and coins are legal tender." Therefore, an alternative means of payment can be understood to be cash or a cash substitute that nobody would refuse to settle a monetary obligation.[181] Yet, what are these? The BIFID study likewise examined this and proposed practical solutions.

Whether or not an alternative means of payment would be used depends on the confidence in the means of payment and on its purchasing power—both these aspects, as we recall, are at the core of a currency and its acceptance. This is because, should there be a crisis of confidence in the legal tender the past has shown, in various inflationary configurations, the reactions that can happen in the public. Particularly, in Germany, where the trauma of the destruction of the currency several times during inflationary periods has been etched deep into the German soul. So, the researchers drew up several scenarios:

1. Use of another, thus an alternative currency that is still endowed with confidence, for example, the US dollar, Swiss franc, or British pound.
2. Use of valuables, such as jewelry, stamps or pictures.
3. Use of precious metals, so gold, silver, or diamonds.
4. Use of goods—during the postwar period these were often cigarettes, which, on the black market, could be exchanged for "useful" consumer goods.[182]

In chapter 2, I described not only the colorful history of cash but also some rather unusual means of payment. Hardly any of these proved to be sustainable: jewelry, stamps or pictures—these are not only exotic but also impractical. Substitute goods such as cigarettes are conceivable, in principle, and in Romania, for a long time, this was practiced with the *Kent* variety. However, here, too, the question arises as to the standard, or some sort of convertibility—a point that we'll keep coming across over and over again. Therefore, the researchers concentrated on the means of payment in points 1 and 3 because they view these as being the most likely.

Yet, even with a currency there are problems: Which one should we take? After all, we're talking about times of crisis and not times of fair weather. For example, for a long period of time, the British pound was regarded as one of the key currencies in the world. However, long gone are the days when you would say "if the pound coughs, Europe goes into decline." Not only did the empire—on which the sun never set—melt away, it took the value of the pound with it. While it is still a recognized currency, events such as the Brexit vote, in the summer of 2016, showed us how quickly it can fall onto hard times. Then again, the pound is an alternative to the euro. So, why not add it in a particular denomination to the domestic reserve?

By contrast, the strength and solidity of the Swiss franc is proverbial. At least, in terms of the past, you can argue that it's more than just something for a rainy day. While the dollar always fluctuates, nevertheless, it's the number 1 key currency and is ahead of the

euro by a huge margin. However, which alternative currency would be generally accepted if there was a shortage of cash?—That's the point, as there certainly won't be several equal options available in parallel. However, this is something that I'm also not able to predict. Therefore, everyone should have a mix of currencies on hand.

At this juncture, we can finally focus on the subject of gold again. I've demonstrated, several times and in a separate chapter, its irrefutable importance for our culture and (earlier) currency systems. Gold is the central theme of this book and so it's only logical to include this precious metal in your private precautionary reserve.

Historically, gold has not been a means of payment or a unit of account for the last 45 years only. Prior to the invention of paper money, electronic bank transfers and virtual Bitcoins, it was, to a certain extent, the general means of payment. The value preservation nature of gold and also its practicability are backed by historical evidence. Its capacity as a means of exchange in times of uncertainty is recognized and beyond question.

Although, the crucial issue is divisibility and how to determine small amounts. It's obvious that gold checks, for example, or gold deposited at a bank would not be accepted in cash transactions. However, the smallest unit that can reasonably be traded is one gram—today this is the equivalent of 36 euros.

Simulation of a Breakdown in Payments

BIFID specialists simulated a situation where a technically induced breakdown in payment systems occurs and, consequently, there are massive problems with respect to the supply of cash. As is usually the case, the researchers made various assumptions in the course of their simulation. The study focused uniquely and exclusively on food supplies. Other essential expenses were not simulated in this case, although, for the sake of simplicity it was assumed that the provision of healthcare would be guaranteed.

The researchers assumed—as was also the case in the *Bundestag* report but not the German Federal Ministry of the Interior—that

the logistics system for food supplies would cease to function and that only the food stocks in the stores would be available. In the simulation, this circumstance was modeled along the lines that price increases could occur depending on the available quantities of food.

The key factors in this simulation were, therefore, the dynamic price increases, price elasticity, the available quantities of food, the average daily expenditure on food per head as well as the duration of the breakdown in the supply of cash.[183] The result was a multidimensional model that focused on the question of whether or not 103 euros per person would be sufficient and for how long. Overall, the researchers analyzed 9,100 potential situations that could arise and which they were able to model from the combination of a decreasing quantity of goods and increasing price elasticity. Price elasticity measures the change in supply or demand after a change in the price. The higher the price elasticity, the stronger the responsiveness of the quantity to the change in the price.[184]

The timeframe considered by the authors of the study was set at up to ten days. Furthermore, the cumulative euro amount was formulated as a dependent variable, which was required over the timeframe that was analyzed. The changes in the available quantity of food were considered from a level of 100 percent down to a level of one percent. Thus, 100 percent means an uninterrupted supply with regard to the daily calorie needs from food. Therefore, through elasticity, the quantity of food affects the price level of food. A shortage of food supplies would naturally lead to an increase in prices.

According to the statistics, the average daily expenditure on food per person is 6.47 euros.[185] Therefore, in a 2-person household, the monthly expenditure on food, beverages and tobacco products amounts to 388 euros. Households where there are children will have higher expenditures in this case.

The Results of the Simulation

We, therefore, have a five-dimensional model consisting of price elasticity (changes in supply and demand against the background

of price changes), the volume of goods, the price level, a time interval covering up to ten days and the 103 euros. To provide the reader with a better understanding, and also because this answers the all-pervasive question, the focus was on whether or not 103 euros per person would be sufficient and for how long. This depends on the price elasticity and the volume of goods that is available.

The results of the simulation show that, depending on which situation occurs, the liquid funds available in cash would not be sufficient for German citizens to provide themselves with food over a certain period; naturally, as time goes by, the situation would change. After three days, the situation is still very calm—the researchers found that a situation where the cash reserves of 103 euros were not sufficient occurred in only ten of the 9,100 scenarios. Things look similarly undramatic after five days—it was only in a few extreme situations, namely, in 27 cases out of 9,100 that the available liquid funds of 103 euros were exhausted.[186] Although, in the event of payments breaking down for ten days, the BIFID experts already found 133 scenarios where the cash holdings were not enough.

However, the general results of the simulation, which, at first glance, are rather reassuring, don't take into account that confidence in the currency would be lost and, therefore, the prices would go up accordingly. Although, this is what the experts did in an additional analysis and, of course, the result was that the cash reserves lasted less frequently, namely in 64 percent of all the scenarios, thus, for 5,800 out of 9,100. The consequences would be drastic—if the quantity of food were to contract to one quarter of the original volume then the expenditure that would be needed, extrapolated for a period of ten days, would total 680 euros. For the last tenth of a given quantity of food, over a period of ten days, you would have to shell out 1,894 euros. When you consider the 103 euros that was available originally, it's obvious that you wouldn't get very far with that—based on certain assumptions, please note.

Recommendations

While the authors of the study refrain from making a binding recommendation, they still make some neutral and, consequently, serious statements. Readers can draw their own conclusions from these: "If a foreseeable finite data crisis occurs, which doesn't shake confidence in the currency, then the available cash reserves would be sufficient." However, further on it says: "However, if an author were also to include the developments of recent years into the evaluation and perform not just a quantitative analysis but, if required, also one with estimates then, in some circumstances, it would be sensible to hold higher amounts of cash. If, in addition, there was a loss of confidence in the local currency then holding foreign notes and coins for one/several currencies could be viewed as a sensible measure. As in this case, too, there could be changes in the estimate so it is difficult to make a statement on which foreign notes and coins should be held. With a view to possibly minimizing this risk, a precautionary measure could be to hold precious metals."[187]

Here, the authors advise having precisely the amount of 1,894 euros available with which, in the worst-case scenario, you would be able to make it through ten days given the massive price hikes. Against the background of average assets of 47,681 euros this would appear to be feasible. The question now is in what form?

In the course of the 2008 financial crisis, the German Federal Government provided a state guarantee, for the first time, for all the savings deposits of private investors. These were later incorporated into the German Deposit Guarantee Act (*Einlagesicherungsgesetz*). The aim was to minimize the run on the banks and to prevent uncontrolled withdrawals of cash.

Today, we find ourselves ultimately confronted with those challenges that play a part in this book and chapter, namely, the heavy dependence of the financial sector on the functionality of the IT systems.

Therefore, the authors extended the previous recommendations to hold cash reserves to include other means of payment. According

to this, "besides cash holdings in euro, stocks of other currencies regarded as safe and which are internationally accepted, such as the US dollar, as well as precious metals, such as gold and/or silver (in small units), should be held in reserve."[188]

The recommended amount depends heavily, in this case, on the duration of the IT blackout (where nobody can foresee the end). However, for the ten days in question, they recommend (per person) holding the equivalent value of 2,000 euros, which should be spread across the separate means of payment in roughly equal shares. This means "all the three key recommended means of payment—the euro, a stable currency from outside the eurozone and precious metals—should be available and each should account for a third," say the financial experts. They immediately highlight that, "based on the source of the crisis, a loss in confidence in other currencies cannot be ruled out. This would point to a higher proportion of precious metals in small 'tradable' units."[189]

So, the researchers are saying that gold belongs in the private financial provision basket. (While they talk generally about "precious metals," however, this means only gold and silver and silver is clearly second choice). It is clear that domestic dental gold, granny's heirloom and gold coins are not suitable for such purposes. This is because, in an emergency, it would be difficult to buy bread with these. In the following two chapters, I'll reveal the form of gold that would be of practical help to us in such situations. However, prior to that, I would like to present the German *Bundestag's* report on a "blackout" that has already been mentioned several times. It's a few years old but it pulled no punches. This is because when it was written its contents were considered to be more in the realm of academic theories and ended up forgotten in a drawer but, now, they are more topical than ever, unfortunately. Therefore, this is an excellent complement to the reflections on an IT blackout.

Excursus—The German Bundestag's Report on a Blackout

"What happens during a blackout. Consequences of a prolonged and wide-ranging power outage." Report by the Office of Technology Assessment at the German Bundestag (Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, TAB), 2011.

In the previous section, I described how far (or precisely not far) we would get in the event of a blackout with 103 euros to buy food for ourselves. The background to the BIFID study was the collapse of the banking systems due to an IT blackout. In 2011, the *Office of Technology Assessment at the German Bundestag* carried out an extensive examination of a general and longer lasting power outage, which would have an immediate drastic effect on all areas of infrastructure and, therefore, also on banks and their IT systems. "With electrically operated devices now virtually omnipresent in our living environment and our world of work, the consequences of a *prolonged and widespread power outage* would combine to produce an extremely serious damage situation. All critical infrastructures would be affected and it would be almost impossible to prevent a collapse of society as a whole. Yet despite this potential for threat and disaster, society exhibits limited awareness of the risks involved."[190] Such a "prolonged and interregional" power outage could be caused by technical failure and human error, criminal or terrorist acts, epidemics, pandemics or extreme weather events. What would happen then—and the authors expressly describe this situation as a disaster – with our financial services and cash supply, was part of the integrated scenarios of the above-mentioned report titled "Consequences of a prolonged and wide-ranging power outage."

The authors do indeed describe individual sub-sectors within the financial services system as being relatively resilient. "According to experts, the transmission of data and payments between banks, the clearing organizations and the stock exchanges, and also data management and also other critical business processes can be guaranteed for a long period through the use of emergency power

supplies, or can be outsourced to a region that is unaffected by the blackout."[191] By contrast, the communication channels between the banks, clearing organizations and trading centers, on the one hand, and the individuals and companies who require financial services, on the other hand, were deemed to be less robust. "Many banks that remain open after the onset of the power outage will close after a few days. As cash dispensers have also stopped working, the supply of cash to the public threatens to collapse. It can be assumed that this and the failure of electronic payment facilities in businesses and banks will eventually lead to anger and to aggressive altercations as members of the public find themselves unable to effect payments."[192]

The lack of electronic payment facilities and the dwindling ability to supply cash are expressly described as the Achilles heel within the sector.[193]

At this point I would like to document in detail the very realistic scenarios, letting them speak for themselves. The researchers simulated, in each case, the consequences from several hours to two weeks and provided a vivid description (the highlighting in bold in the text is mine).

Consequences of a prolonged and wide-ranging power outage for financial services (P. 168ff.)

Major banks, insurance institutes, pension funds and other bank-like organizations have preparations in place to deal with power outages. Although their BCM (Business Continuity Management) processes vary in terms of managing power outages, they do exhibit numerous similarities (EBP 2010, p. 42). Generally, the individual business divisions within a company (e.g. payment transactions, investment management) define their critical business processes and specify how they will continue these in the event of a prolonged power blackout. Critical business processes refer in particular to activities relating to payment transactions and data traffic, data management and account movements, trading and

securities settlement and also the supply of liquid funds (including the supply of cash) (Bankenverband 2004, p. 20 ff.).
A basic technical means of safeguarding these processes is to establish a corresponding emergency power supply for essential information and communications infrastructures (servers and data lines) and also for workstations and important facilities (e.g. safes). In addition, many organizations make provision for data and also staff to be transferred to an unaffected location (e.g. abroad, often to London) in the event of a widespread and/or prolonged incident. Some banks maintain alternative locations for this purpose with a corresponding communications and information infrastructure in regions that are in some cases a considerable distance away. Banks also generally have a secure emergency power supply (diesel-driven emergency power system) that can last for around one week, but also have corresponding supply contracts with suppliers designed to guarantee a power supply if a power outage were to last longer. During this period, critical business processes could be outsourced to regions not affected by the blackout (EBP 2010, p. 12 ff.).
Round-the-clock availability of cash ranks as one of the most important financial services. If cash is not available in a crisis situation this further exacerbates the existing uncertainty felt by the public. Demand for cash is likely to increase rapidly in a crisis situation; it is estimated that on average, a citizen of Germany carries around 118 euros in cash (*Deutsche Bundesbank* 2009b, p. 40). It is therefore likely that if a power outage lasts for a long time, banks and private cash-in-transit companies will be unable to guarantee the distribution of cash throughout the blackout. However, the *Bundesbank* states that in order to "manage an emergency or disaster situation ... special measures have been taken within the context of crisis management organization." (BBK 2008a, p. 120).

0 to 2 hours

Following the sudden onset of the power outage, the banks immediately start to implement the measures planned as part of BCM. Major banks have generally made provisions to ensure that key financial services (critical business processes) can still be guaranteed with the

aid of an emergency power supply for the necessary information and communications systems. All banks' critical servers (containing data on payment transactions, investment management, etc.) are secured against power outages to ensure essential data are not lost.

Major banks also have sufficient emergency power to supply employees' workstations (back office, counters). To start with, these can continue to work as normal. By contrast, many employees at smaller banks that have not made the necessary arrangements cannot continue to work. Since it is not initially known how long the power outage will last, employees remain in the building for the moment (EBP 2010, p. 45 ff.).

The counters are initially still occupied and customers are still served. Sufficient cash is available. Cash transport operations that were underway when the power outage struck are still able to reach their destination, although some delays are encountered due to mounting traffic problems such as traffic jams and closures (chapter III.2.2). Some smaller banks have not made any provisions for continued counter operations and are forced to shut their counters.

Pure administration of deposits by the public and of (financial) investments is not affected at the start of the power outage, provided the bank in question can supply the necessary back-office workstations with emergency power. Data are backed up and orders that had been sent to the corresponding trading platform before the power outage can still be executed. Loans can also still be issued after the start of the power outage.

In many parts of the affected area the members of the public are no longer able to withdraw cash from or pay in cash at cash dispensers. Cash dispensers do not generally have an uninterruptible power supply or an emergency power system and consequently stop working immediately the power blackout strikes. This does not apply to cash dispensers that are actually fitted to bank buildings and are connected to their internal emergency power system. However, the number of such cash dispensers is very small (EBP 2010, p. 46). Customers, therefore, line up at the counters of their banks to withdraw money as it has meanwhile also become clear that it is no longer possible to pay for

goods in shops by electronic means using debit or credit cards.
Wage payments that have already been commissioned by an employer and for which there is corresponding cover at the bank are still executed. In some cases, it has already become difficult to issue instructions for new wage payments because the information and communications structures of many smaller companies have stopped working (EBP 2010, p.47).

2 to 8 hours
Operations in larger banks can largely still be maintained. Critical business processes in particular are ensured. However, in some areas it becomes clear that communications systems that are based on the public telephone network are gradually ceasing to function.
Counters are still manned and service is still provided where this is possible and, where appropriate, provision is made as part of BCM. There are significantly more customers visiting the counters who wish to withdraw money from their accounts as cash dispensers are no longer working. Sufficient supplies of cash are available, and cash transport operations are still being carried out. The uninterruptible power supply at some smaller banks is no longer working or the counters have been closed from the outset. Some complaints are voiced by customers. In view of the uncertain situation, some transactions are initially recorded on paper so that they can be posted in the books at a later date (EBP 2010, p. 47).
While some employees who are unable to work (especially those in the back office of smaller banks) are sent home, others have to remain at work. They are especially deployed at the counters in order to serve the gradual rise in customer numbers as best they can. Along with an increasing demand for cash disbursements, staff also have to answer concerned questions about wage payments, transfers, etc. **In some cases, chaotic scenes break out in banks where staff are not adequately prepared and/or where cash cannot be issued properly. In some locations, it becomes necessary to enlist the assistance of the police—provided they are available**. These banks decide to close early and resume (unfinished) transactions the next day—in the assumption that elec-

tricity will be restored by then (EBP 2010, p. 47 f.).
At the latest eight hours after the start of the power outage, the day's business is closed out as far as possible. No information is available on the anticipated duration of the blackout. Nevertheless, the managers and BCM officers in some larger banks start to consider next steps to cover the eventuality of a prolonged power blackout. They examine whether critical business processes should be outsourced to areas of the country not affected by the blackout, or even to other countries. In addition, some employees of larger banks have to stay in the buildings overnight in order to ensure that the critical business processes can be continued the next day if the electricity supply has still not been restored by then (EBP 2010, p. 48).
Management of deposits by the public and of investments stops when banks are unable to provide their employees with workstations that are equipped with an emergency power supply. This especially applies to smaller banks. Larger institutions continue normal administrative activities at their most important branches until the end of the working day and, where this is possible, use their data lines that are secured against power outages to transfer the management of deposits by the public and of financial investments to branches that are not affected by the blackout.
Customers in the affected area find it increasingly difficult to communicate with their banks. In most cases it is no longer possible to receive/give instructions via the telephone (mobile and land line) or via the Internet. Investors and companies thus suffer financial losses due to lost profits (EBP 2010, p. 48). Fewer loan negotiations are conducted because the people concerned are unable to meet due to the traffic chaos. Inter-account transfers within the banking sector continue to function. Just a few hours after the start of the power blackout it becomes impossible to conduct negotiations via phone.

8 to 24 hours

Even on the day after the power blackout, the major banks are still largely able to maintain their critical business processes. However, working conditions deteriorate because, for example, most banks

are unable to operate their staff restaurants and the lifts and heating no longer work. Lighting and workstations are still available. Around two-thirds of employees who are obliged to turn up for work do so (EBP 2010, p. 19). Together with the teams who have remained in the building overnight, they must maintain the critical business processes and man some of the counters. Communication is now only possible via secure data lines (payment transaction systems, connections to clearing organizations and trading venues, connections to other major banks) (EBP 2010, p. 49).

The counters at larger banks are manned and cash can still be issued. Money transport operations are still possible. Increasing numbers of people want to withdraw cash as purchases can only be made using cash. Questions on salary payments and invoices also have to be answered. Smaller banks initially don't open at all and only perform back-office functions/critical business processes (EBP 2010, p. 49).

Management of deposits by the public and of financial investments comes to a halt, especially at smaller banks whose workstations are not equipped with an emergency power supply. Although larger institutions continue management operations, this is done with many restrictions (deterioration in working conditions, hardly any contact or no contact at all with customers/investors). However, they take initial steps to outsource these activities to unaffected areas.

Investors and companies in the affected area now have almost no means of communicating with their banks. It is no longer possible to give/receive instructions via the telephone (mobile and land line) or via the Internet, even if the investors/companies concerned have functioning terminals. They, therefore, suffer financial losses. Negotiations on the issuing of loans are only conducted in extremely urgent cases, provided the relevant parties are able to meet despite the traffic problems.

Since it is still assumed that the power supply will soon be restored and since the scale of the incident is not yet known in many places, managers and BCM officers only initiate the first steps for dealing with a prolonged power blackout at the end of the day following the onset of the blackout (e.g. transferring critical business processes to unaffected

regions) (EBP 2010, p. 50).

24 hours to 1 week

In the week following the power blackout the larger banks are able to maintain restricted operations (i.e. maintenance of critical business processes and a—restricted—counter service). Towards the end of the first week critical business processes are outsourced to unaffected regions. To this end, the necessary staff have been transported, by bus, from unaffected areas to the alternative venues that are kept on standby for such cases. Once at these locations they are able to perform the critical business processes using the redundant information and communications infrastructures that have been re-started by an advance team. However, additional staff from unaffected regions have to be mobilized because not all of the required staff were prepared to leave behind their families and homes in the affected area (EBP 2010, p. 51).

After a few days, it is virtually impossible to make over-the-counter cash payments; this is, in particular, due to the fact that private companies are no longer able to transport the required volumes of money from the *Bundesbank* branches to their destinations. The *Bundesbank* does implement the measures planned for such a situation (distribution of bank notes independently of private transport operations) once it realizes that the power outage will last for some time. It is supported in this by other official agencies (e.g. the police) (BBK 2008a, p. 119). The situation is compounded because transport problems and hoarding push up the prices of basic foodstuffs and other goods. However, the size of the affected area means cash remains in short supply. The public is now very insecure as it is becoming increasingly clear that the power blackout will continue for some time (EBP 2010, p. 51 ff.).

At the end of the first week even the larger banks start to experience problems in maintaining their emergency power supply. The fuel supplies for the emergency power systems dry up and there are problems with deliveries of replenishment supplies. Most counters are therefore closed. Critical business processes are not affected by this as they have been outsourced to unaffected regions. (101 footnote in original report)

Smaller banks suspend their critical business processes and endeavor to prevent data losses (EBP 2010, p. 52). Management of deposits by the public and of financial investments has either been outsourced to unaffected regions or halted.
Companies that have not transferred their activities to unaffected regions or whose (smaller) banks are unable to continue administering financial investments via an alternative infrastructure are now no longer able to invest and obtain finance. They, therefore, suffer major financial losses. Negotiations on the issuing of loans and the actual process of issuing loans have come to a complete standstill within the affected area.
The first businesses encounter liquidity bottlenecks towards the end of the week because, on the one hand, they are unable to generate any income and their customers can't pay any invoices due to the power blackout; on the other hand, numerous outstanding debts can still be paid (automated payments are still executed by the banks despite the power failure) (EBP 2010, p. 53).

A look at week 2

Thanks to the alternative venues, the major banks are still able to guarantee their critical business processes. Following the initial shortages in staff to operate the alternative venues, this has now been rectified by enlisting staff from unaffected areas.
Although the main branches of some banks have plans to open at certain times and to man a limited number of counters, by the second week most managers have decided to close the counters. Such decisions are based on a lack of security for staff (dissatisfied and in some cases aggressive customers), **a shortage of cash**, a threat to the emergency power supply and the fact that large numbers of employees stay away from work in order to look after their families and homes. Banks that store valuables in safes are exposed to a higher risk of break-in and require surveillance by private security firms or the police where applicable.
Measures adopted by the *Bundesbank* only enable the supply of cash to the public to be maintained to a limited degree.

Investors and companies who/that were unable to transfer their activities or do not have an alternative infrastructure are no longer able to invest or obtain finance and suffer financial losses. Many companies whose commitments continue despite the power blackout experience liquidity bottlenecks.

PAYMENT TRANSACTIONS AND DATA TRAFFIC SYSTEM 2.6.3.2

As previously outlined, the payment transactions and data traffic system between financial intermediaries (banks and bank-like organizations), the trading platforms and the central banks is extensively protected against a widespread and prolonged power outage.

By contrast, (electronic) payment transactions and data traffic between beneficiaries and payers and their respective payment intermediaries are not protected. In many shops, when a power blackout strikes it immediately becomes impossible to make payments using a debit or credit card because the end terminals stop working. If a shop has an uninterruptible power supply, it should be possible to continue to make electronic payments for as long as the telephone land line network still functions (up to around eight hours).

0 to 2 hours

After the power supply fails, uninterruptible power supplies and then emergency power systems at both payment intermediaries and also the corresponding clearing organizations ensure that systems can still function. This prevents the loss of data for electronic payment transactions. The communications infrastructures (secure data lines) also work, meaning (automated) exchanges between the payment intermediaries, clearing organizations and central banks can continue throughout the entire duration of the power outage (EBP 2010, p. 62). The activities of the European Central Bank and of the *Bundesbank* are not restricted either, as these are also protected against a power outage. In principle, the pan-European payment transactions system is not affected by the power outage and continues to function throughout the blackout.

However, payers and beneficiaries do encounter problems. In many

shops, when a power blackout strikes it immediately becomes impossible to continue to effect payments using debit and credit cards because the corresponding terminals (card readers) stop working. This means that cards can't be read and the corresponding payment instructions can't be sent to the payment intermediaries. Purchases can now only be made using cash. However, even instructions for distance payments (effected from home via the Internet) are no longer possible because the people who wish to make payments cannot use their computers and give corresponding instructions. During this phase, larger companies who are prepared for a power blackout and who have installed an uninterruptible power supply for their computers are still able to transmit payment instructions to banks or to receive confirmations.

2 to 8 hours

In shops, purchases can now only be made using cash. In the first few hours since people have become aware of the power blackout and accepted it, this inability to conduct electronic payment transactions does not yet represent a major problem. Many people assume that the power will be restored in a few hours and delay their purchases. Others withdraw money from their banks, a process which is still largely unproblematic. Private individuals postpone the payment instructions they wanted to place via the Internet until later, again in the assumption that power will soon be restored. Larger companies who are prepared for a power blackout can continue to transmit their payment instructions for as long as the communications lines on which the Internet is based are still functioning.

8 to 24 hours

Some shops have opened despite the power blackout and offer products on a cash payment basis; in some cases the range of goods offered is reduced. Many people continue to assume that power will be restored in the next few hours. Purchases are, therefore, postponed until later. Other people withdraw money from banks because cash dispensers aren't working. However, smaller banks shut their doors. Even

larger companies are now unable to issue payment instructions. In addition, many companies are running reduced operations, if at all, and many have closed completely.

24 hours to 1 week

In the first few days the public can still be supplied with cash from bank counters that remain open; demand for cash remains moderate as most people expect that the power blackout will end soon. Purchases are put off to a later date.

As soon as it is announced that it is not possible to say when the power blackout will end, concerns about supply bottlenecks grow among the public, not least because of the lack of means of payment. Chaotic scenes break out at some banks and in retail businesses as people attempt to obtain cash or to purchase daily requisites. The situation is compounded because some suppliers (can) no longer supply businesses—in some cases this is due to a lack of means of transport but in others it is for fear that deliveries will not be paid for. There are sporadic incidents of theft and looting.

A look at week 2

The measures taken by the *Bundesbank* to supply the public with cash are only partly effective because shops are empty and there are sharp rises in the prices of goods that are in especially high demand. There is also a rise in the number of mobile traders who sell daily requisites at vastly inflated prices. People who had a supply of cash or who have obtained cash via the measures adopted by the *Bundesbank* use this to purchase goods from farmers and other food suppliers (including some black-market dealers). Exchanging valuable items for consumer durables and food tends to remain the exception (EBP 2010, p. 65).

CONCLUSION 2.6.4 BANKING SERVICES 2.6.4.1

Within this sub-sector, all critical business processes are guaranteed by means of UPS or emergency power systems that can function for longer periods. These measures generally last until critical business processes can be outsourced to an unaffected area.

In line with BCM, corresponding teams are deployed immediately after the onset of the power blackout to ensure critical business processes are maintained. Some employees, therefore, have to stay overnight in the building. At the latest when the extent of the blackout becomes known after two days, measures are implemented to outsource critical business processes or to safeguard them on a long-term basis. Data traffic and payment transactions, data management and other critical business processes are, therefore, ensured throughout the power blackout. Banks that have valuables stored in safes must take special security measures. Steps are also taken to ensure the (emergency) supply of cash; this also requires the deployment of police.

Employees can continue to work on a limited basis for up to one week, and counters in larger banks can still be manned. However, employees suffer from a deterioration in working conditions. After one week at the latest it becomes necessary to gradually suspend operations. Very little damage to bank buildings is likely, although some branches are no longer able to carry out urgent repair and maintenance work (e.g. caused by frost damage).

Communication connections between the banks and customers gradually start to fail. After just a few hours, if both mobile and landline telephony have stopped working, customers are only able to contact their banks by visiting them in person. **Immediately after the power blackout strikes, people are unable to withdraw cash from cash dispensers and this service is not restored for the entire duration of the blackout (people are also unable to make electronic payments in shops). The supply of cash to the public, therefore, threatens to collapse. Since cashless payment forms can't be used for purchasing, feelings of uncertainty and aggression grow among the public.**

PAYMENT TRANSACTIONS AND DATA TRAFFIC

Technical measures (emergency power supply) enable payment transactions between banks, clearing organizations and central banks to continue throughout the power blackout. Prepared emergency plans are implemented. Selected banking personnel maintain critical business processes within banks. This means considerable pressur on the

personnel resources deployed.
Businesses that are equipped with UPS and/or emergency power systems are still able to effect electronic payments for the first few hours. However, this becomes impossible as soon as landline telephone connections stop working. Other businesses and shops are only able to process cash payments.
A widespread power blackout thus has only a limited detrimental impact on the banking services system. Larger banks in particular can generally administer deposits from the public throughout the power blackout and can also maintain their connections with clearing organizations, the central bank and the stock exchanges. This is made possible by the emergency power supply systems and by the outsourcing of critical business processes to unaffected regions. Electronic payment transactions and data traffic between banks, clearing organizations and trading venues are also protected against a prolonged power blackout and are able to continue. Similarly, operation of the trading venues, and in particular of the main stock exchange in Frankfurt, is also protected against a prolonged power blackout and trading activities are not really affected to any significant degree. Regional stock exchanges represent an exception, however (EBP 2010, p. 78).
By contrast, disruptions to communication paths between the banks, clearing organizations and trading venues on the one hand and on the other hand individuals and companies who require financial services represent an Achilles heel within the sector. Consequently, most of the people who require financial services are unable to use them. **After a certain time, therefore, transactions such as cash disbursements, salary transfers, borrowing, etc. become impossible. Payments cannot be made by card, either.**

VULNERABILITY, OPTIONS FOR COPING AND NEED FOR ACTION—CONCLUSIONS

221: **Whereas payment transactions and data traffic of banks and also stock market trading activities prove relatively resilient even during a power blackout, banking services for customers soon threaten to collapse due to the failure of communication channels.**

VULNERABILITY AND COPING CAPACITIES

Customers are unable to conduct transactions with their banks via telephone or the Internet. Banks cannot issue cash from cash dispensers and customers are unable to make cashless payments in shops. Demand for cash will, therefore, rise quickly, not least because people in Germany apparently only carry 118 euros on them (*Deutsche Bundesbank* 2009 b, p. 40). Despite an initial calmness, the immediate breakdown in the supply of cash via cash dispensers and subsequently at bank counters and also the collapse of cashless payments, lead to expressions of annoyance in shops and banks and to aggressive altercations in some cases. Once it becomes clear that the power blackout will last for some time, uncertainty grows among the public. **People are afraid they won't be able to get supplies of food and other daily requirements because they soon won't have any money left and won't have the option of cashless payments, either. In some cases, this leads to violent altercations, theft and break-ins. The police are forced to intervene at times. Moreover, as the power blackout continues it becomes necessary to guard individual shops**. Shop sales plummet. It is also not possible to rule out the possibility of prices of everyday essentials increasing even during the course of the first week. Informing customers and ensuring appropriate risk communication in consultation with the disaster control authorities thus becomes even more important.

Getting cash supplies to the population becomes a key focus. According to the *Bundesbank* "special provisions have been made as part of crisis management organization to manage an emergency or disaster" (BBK 2008a, p. 120). However, it is questionable whether sufficient supplies of cash to meet requirements can be continuously transported into a large area over a long period of time by private cash transit companies, distributed and subsequently issued by the banks.

The economy suffers due to the extensive inability of the public and companies to make cashless purchases, conduct loan negotiations, make wage payments, issue stock market orders; it also suffers due to the liquidity shortages that soon emerge.

NEED FOR INFORMATION, PROSPECTS FOR ACTION

The analyses of consequence have identified the provision of cash supplies to the public as a particular weakness. Therefore, the *Bundesbank* must cooperate with other organizations and civil protection task forces and also the banks in order to ensure at least a rudimentary supply of cash for the public (EBP 2010, p. 79). To create better conditions for this, it is necessary to examine whether the *Bundesbank* should also be included among the organizations authorized to request priority access to transport capacities pursuant to the Traffic Services Act (VerkLG). An extended logistics and security concept is probably required for disaster situations because, for example, it is not possible to ascertain whether and how private service providers could adequately safeguard higher volumes of cash deliveries.

There are plans to close numerous branches of the *Bundesbank* over the next few years. Consideration should be given as to whether and to what extent these cuts to the infrastructure will affect the supply of cash in a disaster situation.