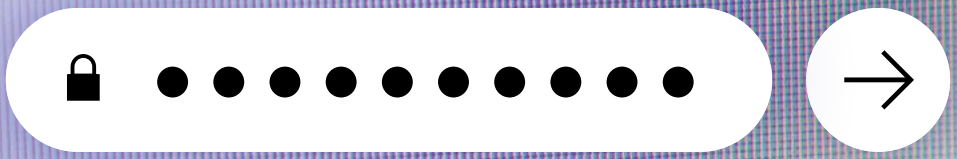
ABOUT TRUST

THE MAGAZINE OF THE TÜV SÜD GROUP 03 — 2021

Add value.
Inspire trust.



Focus: **PROTECTION**

A good password can already protect companies from hacker attacks. But is that enough? An issue about companies being targeted, about the art of defending from outer space against tiny attackers—and how networking various systems can create more security.

ABOUT

TRUST

DEAR READERS,

protecting people, the environment and assets from technology-related risks is the core of TÜV SÜD's corporate purpose. To this day we are bound by this historic commitment—and it will continue to guide us in our future activities. This protective mission has continually evolved over time with the technical innovations of the past 150 years: from the steam engines of the Industrial Revolution to safe mobility and industrial plants to medical devices, artificial intelligence and cybersecurity in the present day.

From the very beginning, protecting the environment has been an important task. Verifying the efficiency and durability of technical equipment and measuring emissions and radiation are services that TÜV SÜD has been providing for decades to help keep our environment livable. The major topic of sustainability is part of our company's DNA, so to speak. Innovative new services, for instance relating to regeneratively produced hydrogen, all aspects of the recycling economy or smart and particularly efficient buildings, show that we take our responsibilities seriously and are actively shaping the future with our services.

Not only do we want to offer our customers and society added value on the point of sustainability, we also have ambitious goals as a company. Our goal is to become the most sustainable company in our industry. On page 4, you can find out more about our efforts to help make a future fit for the coming generations. I hope you enjoy reading this issue!

PROF. DR.-ING. AXEL STEPKEN
Chairman of the Board of Management of TÜV SÜD AG

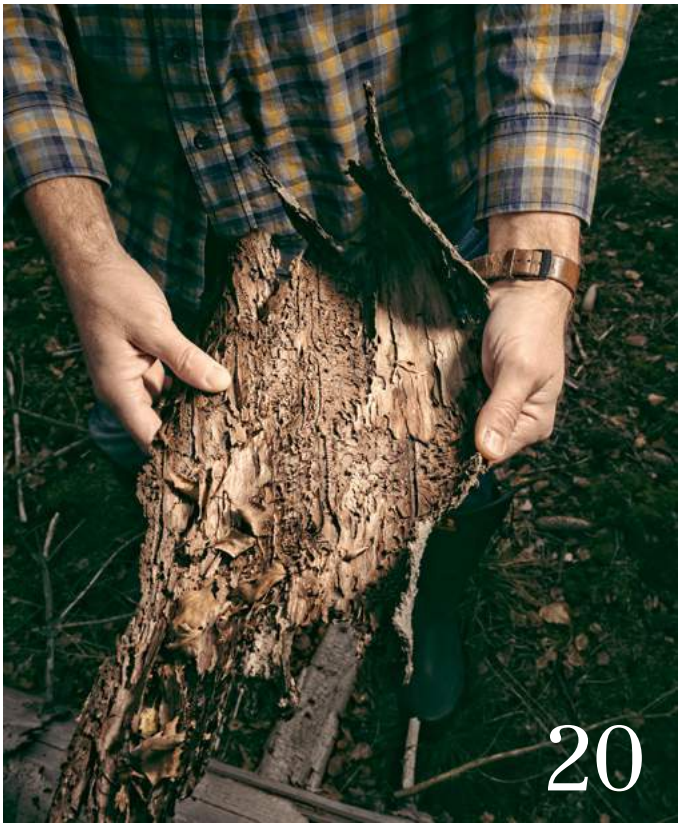
03 2021

CONTENTS

Security. Workplace psychologist Ina Goller about teamwork.

Focus

PROTECTION



Menace. How a forester in northern Germany is battling beetles.

ABOUTTRUST.TUVSUD.COM/EN

You can find even more diverse topics on the ABOUT TRUST content hub. For instance, find out how today's professional hackers work together in company-like structures.

PUBLICATION DETAILS

PUBLISHER TÜV SÜD AG, Westendstraße 199, 80686 Munich, Germany | Owner: TÜV SÜD e. V. (74,9 %), TÜV SÜD Foundation (25,1 %), Westendstraße 199, 80686 Munich, Germany | Project Director and Editor-In-Chief: Jörg Riedle | Contact: +49 89 5791-0, info@tuvsud.com | **REALIZATION** muehlhausmoers corporate communications gmbh, Invalidenstraße 112, 10115 Berlin, Germany, info@muehlhausmoers.com | Project Director: Martin Steuer | Editor: Jan Schulte | Art Director: Áine Gibbons | Image Editor: Jan Steinhauer, Charlotte Zellerhoff | Editorial Staff: Felix Enzian, Lars-Thorben Niggehoff, Zola Schumacher, Nils Wischmeyer | English Translation: Anthony B. Heric | English Editing: Penelope Krumm | **PRINTING** G. Peschke Druckerei GmbH, Taxetstraße 4, 85599 Parsdorf, Germany

Our Contribution to **CLIMATE NEUTRALITY**

TÜV SÜD offers its customers comprehensive services on the topic of sustainability and supports them in achieving their climate targets. Now the company is leading by example and has set its own ambitious climate targets. By the year 2025, TÜV SÜD hopes to be climate neutral with regard to its greenhouse gas emissions. This aim includes what are known as Scopes 1 and 2, as well as the most important sources of greenhouse gases from Scope 3.

"Our climate targets go far beyond what other companies and institutions are aiming for," says TÜV SÜD CEO Prof. Axel Stepken. "We deliberately set a very high bar because we want to become the most sustainable company in our industry." Scope 1 includes all greenhouse gases created by the use of fossil fuels in the company—particularly for heating and the corporate vehicle fleet—while Scope 2 covers indirect emissions from purchased energy in the form of electricity and district heating. In addition, all business trips from Scope 3—which covers other indirect emissions—are also to be made climate-neutral.

The basis for these efforts is the carbon footprint that TÜV SÜD drew up for its operations in Germany for the first time in 2021 and published in its sustainability report. A detailed enumeration of the worldwide footprint is underway. As a services provider, the company's largest sources of greenhouse gases by far are the operations of its offices and laboratory buildings as well as its service centers, not to mention traveling to clients. The key elements of the worldwide action plan with which TÜV SÜD hopes to achieve its climate targets include reducing resource consumption, investments to increase energy efficiency and training for employees on the careful use of resources. Offsets are also envisaged, but only as a last resort. For new buildings—at the moment, the new Asian headquarters in Singapore and the expansion of the corporate headquarters in Munich—the company is aiming to build to the highest standards of sustainability in each case. As for existing buildings, these will be maintained and made more climate-compatible with appropriate remediation measures. This also includes replacing fossil energy sources: in Germany, already about 86 percent of the electricity purchased is green energy.

Another relevant point around the globe is employee mobility, since much of TÜV SÜD's work is performed directly at the customers' premises. As a first step, the group's company car policy has been revised and emission caps have been set for new vehicles. In future, greater use is also to be made of public transportation and the digital possibilities of working remotely.

PHOTOS: *GettyImages/Siri Stafford (globe), Getty Images/stilllifephotographer (explosion), Getty Images/d3sign (smartphone), Getty Images/the_burtons (padlock)*

A BOOMING MARKET

IT security is becoming an increasingly important market. According to estimates made by the consulting firm Gartner, the industry will probably break through the 150-billion-dollar mark in 2021. Gartner also estimates that global spending on technology and services in the area of information security and risk management will increase by 12.4 percent. Spending already increased by 6.4 percent last year. The industry is also setting new records in Germany. According to IDC, a market research company, revenues in IT security are expected to be around 6.2 billion this year. Services account for the largest share of the market at about 50 percent. In 2020, total revenues in Germany were just 5.6 billion euros.

SECURE REPORTING CHANNEL FOR IT VULNERABILITIES

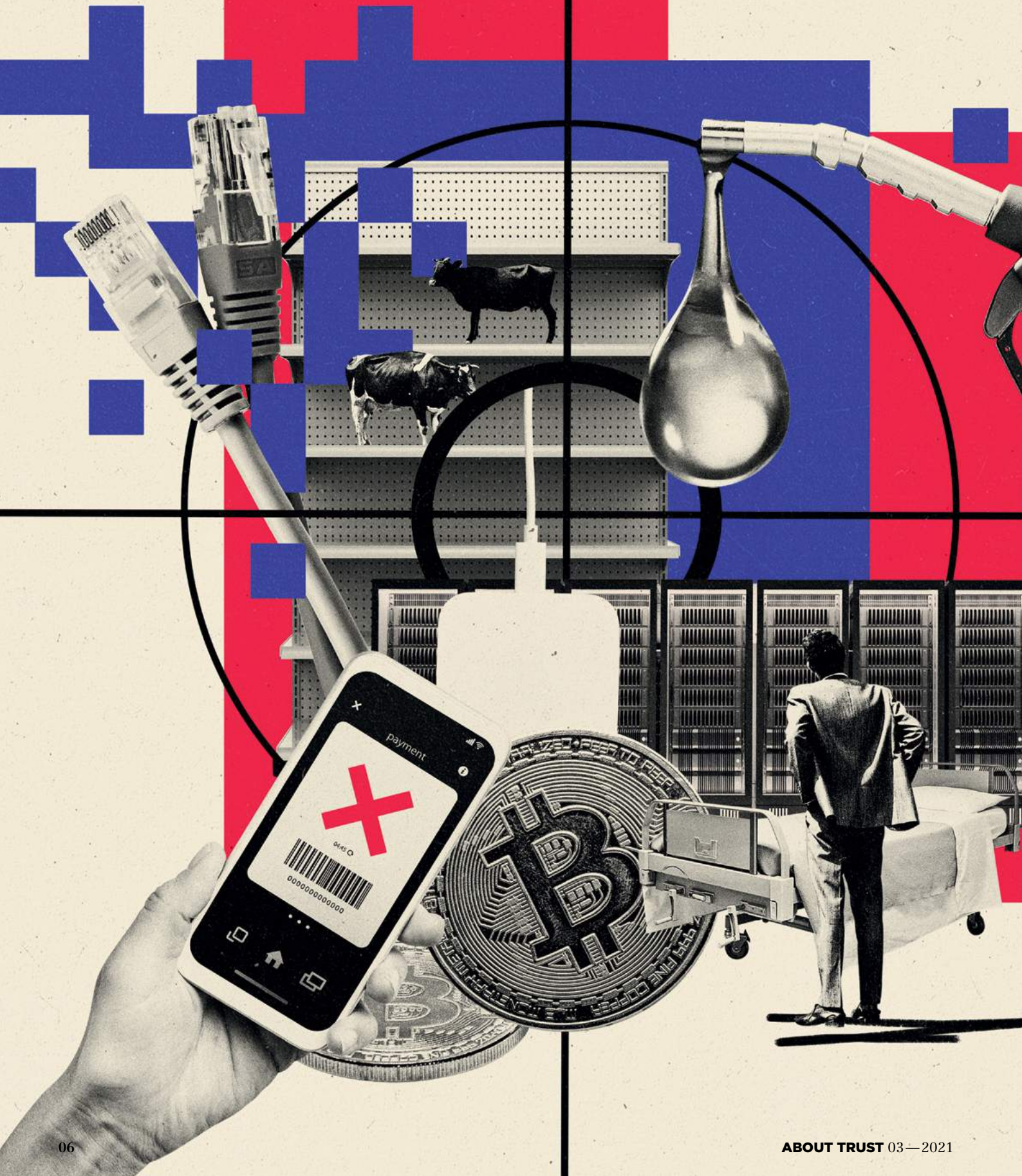
People who discover vulnerabilities in IT systems are doing an important job—as long as they aren't looking to make money but instead report them to the affected parties or the authorities. Reporting these problems has been difficult in the past, but the German Federal Government wants to change that as part of its new cybersecurity strategy. In the future, the Federal Office for Information Security (BSI), as a neutral party, will be creating a new framework for reporting security vulnerabilities. Until now, companies have taken different tacks in this area—some even pay hackers to uncover vulnerabilities in their systems. Others take legal action because they feel a crime has been committed.

1

BILLION US DOLLARS

is what hacking attacks cost the world economy annually, accounting for about 1 percent of the global gross domestic product. At least that's what a study by American antivirus software manufacturer McAfee found for the year 2020. German companies are also increasingly having to defend themselves against hackers. A survey conducted by the German digital association Bitkom found that almost 90 percent of German companies had been affected by cyberattacks in the years 2020 and 2021. The main drivers were ransomware attacks, in which hackers block the systems of their victims and demand a ransom. The majority of these attacks occur with the help of social engineering, in which hackers try to trick employees into revealing confidential information.

In the **CROSSHAIRS**



TEXT LARS-THORBEN NIGGEHOFF **ILLUSTRATIONS** KLAWE RZECZY

Companies and government agencies around the world are increasingly falling victim to cyberattacks—launched by thieves, blackmailers and spies. Those affected are often helpless. Yet usually simple measures are all that are needed to protect them.

On July 2 of this year, much of Sweden came to a standstill. Supermarkets, pharmacies, gas stations, even the national rail system: throughout the country, stores had to close or switch to emergency operations. In some cases, it became absolutely impossible to pay for things with either cash or card. Computer systems went down, and employees had to write invoices—if they could at all—by hand. It took several days before the crisis passed and life in this northern European country returned to normal.

The cause was a large-scale cyberattack that wasn't even targeting the Scandinavian country, but a software company in Miami, around 8,000 kilometers away from the Swedish capital of Stockholm. The company, Kaseya, provides other IT service providers with a software program that installs updates on their clients' computers. Clients such as the Swedish supermarket chain Coop.

The attack demonstrated how greatly global networking increases the risk of cyberattacks. A security vulnerability in Florida can, with just a few degrees of separation, endanger the sale of foodstuffs in Gothenburg. Criminals and rogue states are taking advantage of this, trying to sneak into the computers of companies, public authorities or major infrastructure to either steal data or extort money. "The impacts are striking closer to home, and with increasing regularity," says cybersecurity expert Tim Berghoff from the company G Data in Bochum, Germany.

Indeed, the cases are piling up. In the US this year alone, for example, both the meat processer JBS as well as the Colonial Pipeline System were crippled by criminals. Facebook and T-Mobile reported data breaches. In January, hackers were able to penetrate the systems of the European Banking Authority and the Norwegian parliament, among other institutions, due to a security flaw in the email servers of technology giant Microsoft. In the German county of Anhalt-Bitterfeld, near Leipzig, everything came to a grinding halt. The public authorities couldn't be reached via email for almost a week, among other problems. Hackers had managed to insert malware that encrypted all of the data. And in September 2020, there was probably even a first fatality in connection with a cyberattack when hackers more or less knocked the University Clinic Düsseldorf out of commission.

There are myriad reasons why hackers can manage such feats. The first is the increasing spread and networking of digital infrastructure. Where there's a lot of technology, there are many points of entry. At the same time, attackers have become more professionalized—the cliché of a hoodie-wearing hacker in their mom's basement who paralyzes a company's servers just for fun has even less to do with reality these days than it did in the past. Instead, organized gangs are behind such attacks and they often offer their services to other criminals. And those affected? They're quite aware of the problem.

A survey conducted by the professional services giant Deloitte found that 77 percent of decision-makers in politics and business consider data breaches to be a problem, while 76 percent think the same about malware attacks. However, they struggle to take the necessary countermeasures, raise their own firewalls and train their employees against such attacks. If one does occur, those affected prefer to keep quiet rather than admit to their own mistakes and failures. In critical areas including the economy, infrastructure and public administration, it's important to be armed against cyberattacks. Each faces its own set of challenges, yet at the same time the measures that can be taken are often very similar. What follows is an overview of the issues across three sectors.

“Today things are much more precise. Attackers scout their targets over a longer period of time and search for individual weak spots.”

TIM BERGHOFF,
CYBERSECURITY EXPERT AT G DATA

MORE LUCRATIVE THAN DRUG TRAFFICKING

Many people have learned over the past months how centralized the meat-processing industry has become. In 2020, when a factory of the Tönnies Group in Germany was forced to shut down due to a corona outbreak, a gigantic backlog formed throughout all parts of the industry, bringing sausage and steak production in the country to a standstill. Yet Tönnies is just a lightweight compared to the true giants of the industry. The Brazilian-American meat conglomerate JBS has almost six times the sales of Tönnies. Which means, of course, that the impact is that much higher when their slaughterhouses suddenly grind to a halt. The company handles one quarter of the beef and one fifth of the pork production in the United States. In June, a ransomware attack caused five of its largest sites to close down in the US, Canada and Australia. In a ransomware attack, the victim's data is either stolen or encrypted by malware. The threat: it will be made public (in the first case) or destroyed (with encryption) unless the victim pays a ransom. JBS paid, and quite a lot: 11 million US dollars in bitcoin went to the blackmailers.

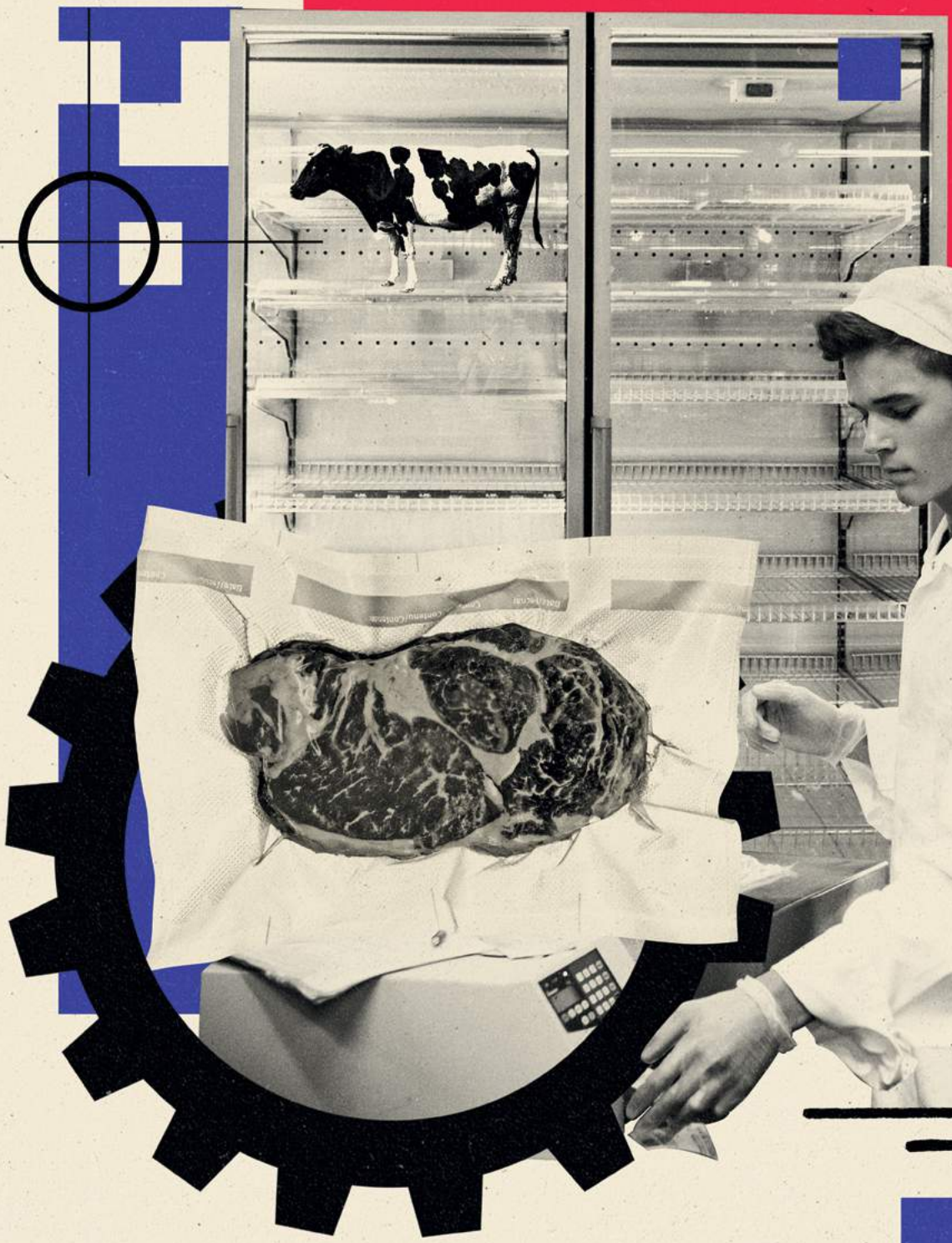
The Brazilian headquarters remained tight-lipped about the cause of the incident. Yet a culprit was quickly found. The Russian ransomware operation REvil was allegedly behind the blackmail operation.

Groups such as REvil have revolutionized the cybercriminal world. “Before, ransomware attacks were more likely to use a watering can approach,” Berghoff says. With the watering can analogy he means that the attacks used to be more broadly distributed among various targets in the hope that at least one of them would bite. “Today things are much more precise,” he says. “Attackers scout their targets over a longer period of time and search for individual weak spots.” And they find them, because companies neglect to introduce even simple countermeasures. “The basics of self-protection have principally been the same since the Nineties,” Berghoff says. Employees shouldn't click on suspicious emails and should use secure passwords.

Such emails are almost guaranteed to arrive at large companies because digital crime has become incredibly lucrative. “According to the German Federal Criminal Police Office's situation report, revenues from cybercrime have outstripped those from international drug trafficking for several years now,” says Peter Wirnsperger. Wirnsperger works for Deloitte helping clients set up effective security systems and he also co-authors the company's annual *Cyber Security Report*. This gives him a regular, close-up look at how the criminals operate. “They now have hotlines and provide manuals on data encryption,” he reports. For a long time now, they haven't just been working on their own, but offer their services to third parties. Experts speak of “ransomware as a service”.

TÜV SÜD, in its current report on trends for 2022, also warns that this type of cybercriminality will continue to increase. This development requires new measures against dubious service providers. “The increase in this trend is making it necessary for companies to boost their investments in cybersecurity and focus on protecting themselves from such sophisticated attacks,” says Head of the TÜV SÜD Cyber Security Office Sudhir Ethiraj. He also believes that it is essential for companies to share more about their experiences with hackers. Many often remain silent out of misplaced feelings of shame when they're affected by a ransomware attack. As Ethiraj emphasizes, this is a

EMPTY SHELVES
Ransomware attacks can hit any company. The meat processing conglomerate JBS had to shut down some of its factories after such an attack in June. Even the FBI got involved.



DEADLY THREAT
Attacks on hospitals are on the rise. A modern security structure is essential for protection.

mistake: "Regular monitoring of the latest threats and active participation in cross-industry threat intelligence platforms are the order of the day when it comes to staying up to date."

One example of this type of platform is the Charter of Trust. It was launched by Siemens at the Munich Security Conference in 2018. Members of this initiative include companies such as IBM and Deutsche Telekom, as well as TÜV SÜD. The goal: to create industry-spanning standards and rules for cybersecurity. Together these large companies want to do the groundwork so that smaller companies and society as a whole also benefit from increased security standards.

A CLOGGED PIPELINE

The issue of cyberattacks is increasingly affecting infrastructure, which further multiplies the danger. A few days without meat production may be a bitter pill to swallow, but it's not necessarily life-threatening. Things were much different in autumn 2020 in Düsseldorf. The local university hospital was paralyzed because hackers had snuck into the systems. An ambulance had to be turned away because of this and divert instead to Wuppertal, a good 25 kilometers away. The patient died shortly after arriving at the hospital there. It cannot be definitively said whether or not the extra half hour of transport directly led to her death. But suddenly the question was whether the cyberattack was at least indirectly to blame for it. The police quickly contacted the hackers. According to the authorities, they were sur-

prisingly cooperative when they learned they had crippled a hospital and provided the decryption codes for the ransomware without receiving payment. The hospital reported that it took four weeks after the attack to get halfway back to normal operations.

Hackers are increasingly targeting critical infrastructure, and not all of them are so forgiving. The German government reported that last year, operators in sectors including energy, water management and telecommunications reported 345 incidents, up from 254 in 2019. The government also said that not all of these incidents could be traced back to hackers, as human error can also be a cause—but it assumes that the number of unreported incidents is even higher.

Attacks on critical infrastructure are becoming an increasingly serious problem all over the world. In the US this year there was an attack on the Colonial Pipeline System, which supplies large parts of the American East Coast with diesel and gasoline. A hack of the operator's invoicing system caused a stoppage in the pumping of fuel from Texas eastward. At least five states experienced fuel shortages as a result.

It wasn't clear if the attackers would have managed to jump from the invoicing system into the system responsible for real-world operations, but the fear of this prompted the company to perform an emergency shutdown. As Berghoff explains, this is a problem that affects many infrastructure operators and companies: "Many victims don't exactly know which of their systems are critical and so don't secure them very well." Yet there are certainly ways to set up internal firewalls. Companies that use external service providers for some of their operations need these firewalls because hackers often use such services as gateways, as the cases of Kaseya and Microsoft's email servers show.

77
PERCENT
of decision-makers in politics and business think data breaches are a threat. Almost as many think the same about malware attacks.

345
INCIDENTS
of potential hacks into critical infrastructure, including energy, water management and telecommunications, were reported in Germany in 2019—almost 100 more than the year before.

117.4
MILLION
new variants of malware were recently counted by the German Federal Office for Information Security, more than 320,000 new malware programs every day.

Unfortunately, some companies often shy away from the effort and expense that a truly effective defense against cyberattacks entails. "Security is a lifelong task, not a project," Wirnsperger says. Reviewing the situation now and again isn't enough. "Companies must set up exercises and run through various scenarios based on the results of the investigations." If possible, these should match up with employees' daily working environments and not consist merely of watching a slide presentation.

One person who offers this sort of training is Julien Ahrens. This white-hat hacker has been working in the field of IT security for thirteen years. He offers his services on

A GRINDING HALT
When critical infrastructure is paralyzed, it restricts the daily lives of many people. Without a pipeline network, for example, gas stations remain closed.

THE NEW WAR

Countries have long since shifted their conflicts to the digital world. For instance, Russia has been suspected several times of carrying out attacks against other countries, including Ukraine.

the HackerOne platform, among other places. One of his money-earners these days is what are known as penetration tests, in which he tests a company's security systems for potential flaws. One way to do this is by sending fake phishing emails to employees. "The degree of realism can vary," he explains. The email could very much look like an attempted fraud, but he can also recreate the level seen from professional hackers. "But you'd be surprised how many people fall for the simpler version."

Colonial Pipeline was ultimately able to restart operations fairly quickly. This was also because a ransom of reportedly around 5 million US dollars was paid in bitcoin. That may be understandable when it comes to getting infrastructure back up and running again quickly. But, as Berghoff says, it's fundamentally the worst way to stop an attack: "You never know if you're actually going to get control back or if data has already been stolen that can be used to blackmail you again later." In the end, the US Department of Justice was able to recover a large portion of the ransom by gaining access to a bitcoin wallet. The agency didn't disclose exactly how this was done.

THROUGH THE BACKDOOR INTO A GOVERNMENT COMPUTER

However, relying on government agencies also isn't always the best idea. They, too, can become victims to cyberattacks, as happened in Ukraine in 2017. A large-scale attack with the malware Petya affected large parts of the state apparatus: ministries, banks, the subway system and telecommunications. Even the system for monitoring radioactivity at the former nuclear plant in Chernobyl was offline for some time.

"Security is a lifelong task, not a project."

PETER WIRNSPERGER,
CONSULTANT AT DELOITTE

The systems were hacked via a control software that is commonly used in Ukraine. The timing was probably deliberate, on the eve of Constitution Day, a national holiday when many civil servants would be at home and the malware could spread more easily throughout the system. At first, those affected assumed it was an extortion attempt, and computer messages suggested as much. Except that instead of just encrypting the data, as is common with ransomware, Petya corrupted it, thus disrupting the work of the Ukrainian state over the long term. One possible reason for this, as later reported by Ukrainian intelligence services: it wasn't criminals behind the attack, but rather state-sponsored hackers, possibly from Russia. The authorities were initially able to repel the attack within a day. However, they later discovered that the hackers had installed a backdoor into the software, thus leaving open the possibility of future attacks. The company responsible for the software was thoroughly screened to rule out additional attacks as much as possible.

Berghoff explains what makes state actors particularly dangerous: "They have all the time in the world, they can infiltrate systems at their leisure." At the same time, unlike blackmailers, they also frequently prefer to remain undetected. That means that some victims don't even know they've been hacked and accordingly leave dangerous backdoors open for exploitation.

However, backdoors in systems can be detected, for instance by paying so-called "bug bounties." To do this, companies offer bonuses to hackers who find vulnerabilities in their systems and report them. "Unfortunately, this isn't really widespread in Germany," Ahrens complains. In the US, for example, even the military would operate such a program.

"What everyone must realize is that there is no 100-percent security," Ahrens says. Attacks can sometimes even take well-prepared facilities by surprise. Then it's a matter of dealing with it openly to find out what the issue was. The only problem is that those affected still tend to keep such incidents under wraps and then call in experts late in the day. "We get a lot of calls on Fridays," Wirnsperger says. This isn't because cybercriminals suddenly become active before the weekend. "Companies naturally attempt to fix the problems themselves in the first few days, since a cyberattack isn't always obviously recognizable. Unfortunately, far too often the real threat isn't realized until just before the weekend." Victims also need to be made less afraid of sounding the alarm prematurely. "I would love it if I had to go out for a false alarm every once in a while."


“A team meeting
doesn’t
have to
BE WARM
and fuzzy”

TEXT FELIX ENZIAN **PHOTOS** ANNE MORGENSTERN

Security makes teams more innovative: specifically, psychological security. The Swiss workplace psychologist Prof. Dr. Ina Goller has studied this concept and explains how it works, how it protects teams and how it should be used—and why bitter disputes must be part and parcel of it.

Prof. Goller, when people think of innovation, they like to think of courage but not of security. When was it clear to you that psychological security might be much more important?

GOLLER At the beginning of my career, I was invited by a management team in a company to moderate a workshop. I was there for a strategy meeting in which they were really going at it and team members argued fiercely with one another. At least that was my initial impression. However, at the end, the participants all thanked each other for the wonderful discussion, summarized what they'd learned and went out to dinner together, everyone in a good mood. This experience surprised and deeply impressed me.

What did you learn from it?

GOLLER A team meeting doesn't have to be warm and fuzzy. Quite the opposite. Too much harmony can stifle necessary discussions because you fear offending someone by contradicting or criticizing them. Only through an open exchange of views can new perspectives and new solutions emerge. Disagreements are productive and valuable.

You call the concept behind this psychological security. What do you mean?

GOLLER It's about relationships. When people speak with each other in a meeting, social judgments are always running through their minds: How comfortable are the others with me? How will they react when I mention an idea or admit to a mistake? Will I receive support or criticism? Will my idea be supported, blocked or even stolen? Do the others think my comments are perhaps stupid? These sorts of risks and concerns often lead people to keep their opinions to themselves. The less fear the team members have that what they say will have negative consequences, the more psychologically secure they feel and the more easily they contribute to the discussion. The pioneer in this research field is Amy Edmondson, a professor of management at Harvard Business School. She calls teams where psychological security prevails "fearless organizations."

Taking risks, being open to new things, making mistakes: it all sounds like the familiar culture of error. How does psychological security differ from this concept?

GOLLER The culture of error applies to a company's entire organization. It's about the implementation of mechanisms that help employees to speak without fear about problems in the company and to learn from mistakes. Psychological security, in contrast, takes place at the level of individual teams. That's because teams are the hubs of innovation in today's working world. They are the think tanks where new ideas and strategies are born and debated. There are hardly any challenges that a single individual can manage alone. You're always dependent on the support of your teammates. That's why the question of how we deal with each other in a team is so important.

What role do managers play in this?

GOLLER The immediate team leader, in particular, has a considerable influence on whether or not people are afraid to speak. Psychological

security therefore cannot be promoted or hindered only by top-level management, but also strongly by middle management. At the same time, the willingness to take risks in meetings and to speak openly is something that each individual must choose and that must be promoted.

So if my team is psychologically secure, we'll come up with innovations. Is that how it works?

GOLLER Psychological security alone is definitely not enough to guarantee innovation. It promotes the quantity, but not necessarily the quality of ideas. The quality of the results produced is mainly determined by three factors: a visionary idea that the whole team believes in, perseverance even in difficult phases and professional expertise. You won't get anywhere without these.

Startups in particular are considered innovative. Is this perhaps partly due to the fact that startups have more psychological security than larger corporations?

GOLLER They do, at least at the beginning. Startups are mainly characterized by a small conspiratorial group pursuing a common visionary idea. Although it's true they have a lot of disagreement in stressful situations, these issues can usually be easily resolved because the common idea binds the team members together so strongly. But as soon as the startup grows, the centrifugal forces also increase and psychological security suffers. Issues such as workload, competition and hierarchies become more prominent and can overshadow the unifying vision. This critical size is reached as soon as the company has around twenty employees and breaks up into several development teams.

What are the noticeable signs that the psychological security of a team is breaking down or even lacking?

GOLLER One unmistakable sign in a meeting is when one person speaks and everyone else remains silent. Then it's a problematic, psychologically insecure situation—unless someone is giving a presentation that is followed by lively debate. The distribution of speaking is a good indicator for measuring psychological security. The exchange of opinions thrives on everyone having an equal say—regardless of hierarchies.

What does that look like in most companies today?

GOLLER The reality is different in many companies. The share of talking in meetings is linked to power relationships. As a rule, it's usually the superiors who literally have the most to say. In psychologically insecure teams, members with dissenting opinions quickly make themselves unpopular, which is why many of them prefer to keep their heads down. Even if problems are actually addressed, these are often sham debates where the speakers agree with each other to create a supposed harmony.

What are the negative consequences of psychological insecurity?

GOLLER We know how disastrous the lack of psychological security can be through simulations of medical operations. If the operating team uncritically agrees with the decisions of the senior physician, more patients die. There are also serious consequences in business if problems cannot be debated.

Can psychological security be learned?

GOLLER Definitely. In our research, we've developed a toolkit with 24 exercises, 15 minutes each, that are to be practiced in teams for 24 weeks.

Can you give us some examples of the communication exercises?

GOLLER Some of them are very simple, but effective. In both English-speaking and German-speaking countries, discussion participants tend to respond to proposals with a, "Yes, but…". This wording blocks constructive dialogue. That's why we train people to instead say, "Yes, and…". This allows opinions to build on one another and lets the ideas flow freely. There are also more complex training units. For instance, we practice conducting negotiations in a cooperative yet tough manner. That's difficult for many people. They think: Either

"The distribution of speaking is a good indicator for measuring psychological security."

Personalia

Prof. Dr. Ina Goller heads the Innovation Management Executive MBA program at the Bern University of Applied Sciences in Switzerland. The graduate psychologist is fascinated by teams and the question of how individual team members can contribute to successful and innovative solutions. As the founder of Skillsgarden AG, she offers consulting and training on psychological security, change management and leadership development.

I conduct tough negotiations and get what I want, or I try to be cooperative and compromise. But successful negotiations are characterized by both approaches.

You've tested your ideas in the real world. What were the results?

GOLLER In practice, some of the participants included the telecommunications company Swisscom, the Swiss Post Office, Switch and a major online retailer. Many of the participants were relieved that psychological security had nothing to do with harmony or sentimentality. In Switzerland in particular, corporate culture is frequently very consensus oriented and thus conflict avoidant. But disruptive ideas don't emerge from teams where everything's just soft and cuddly.

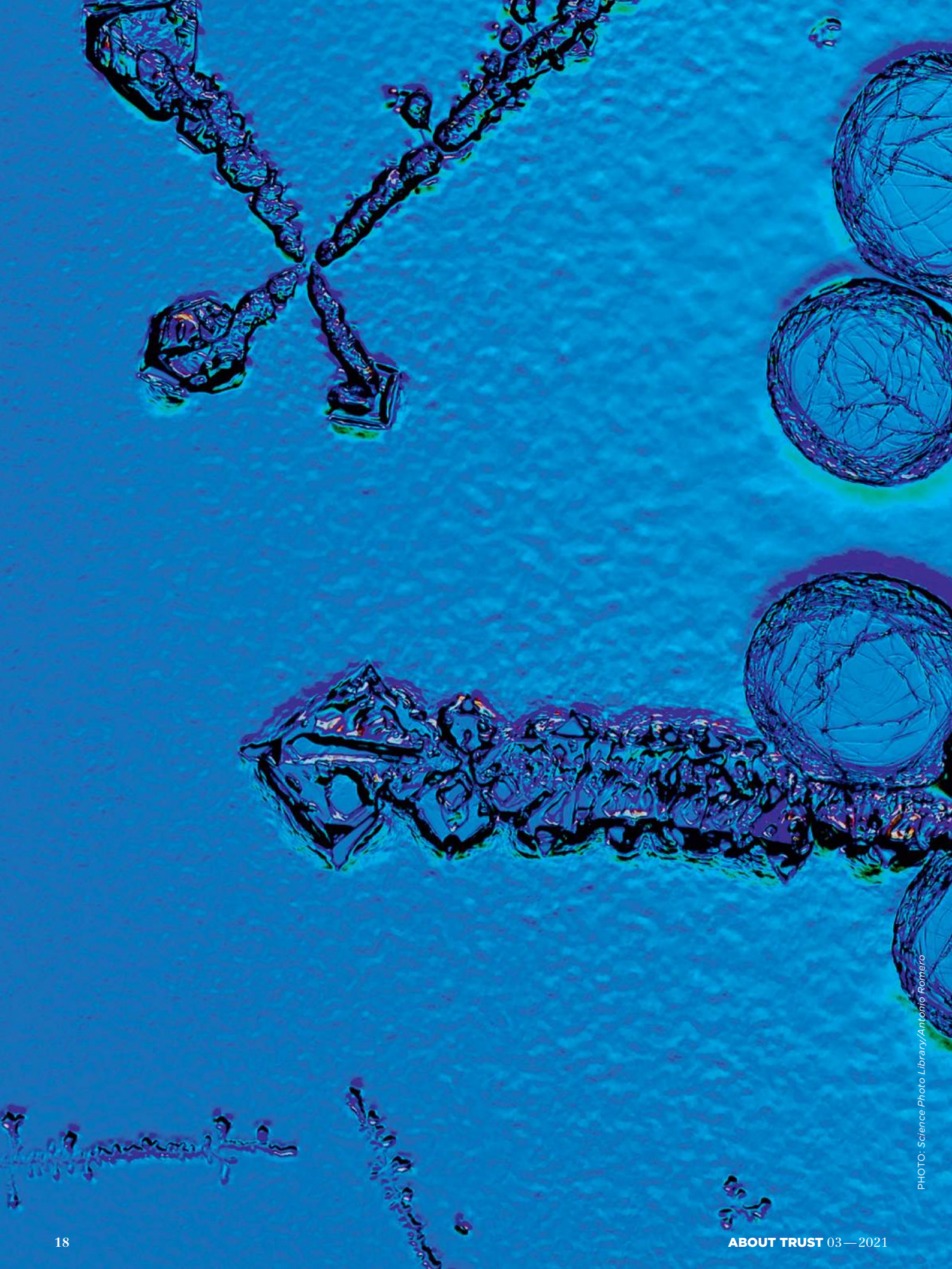
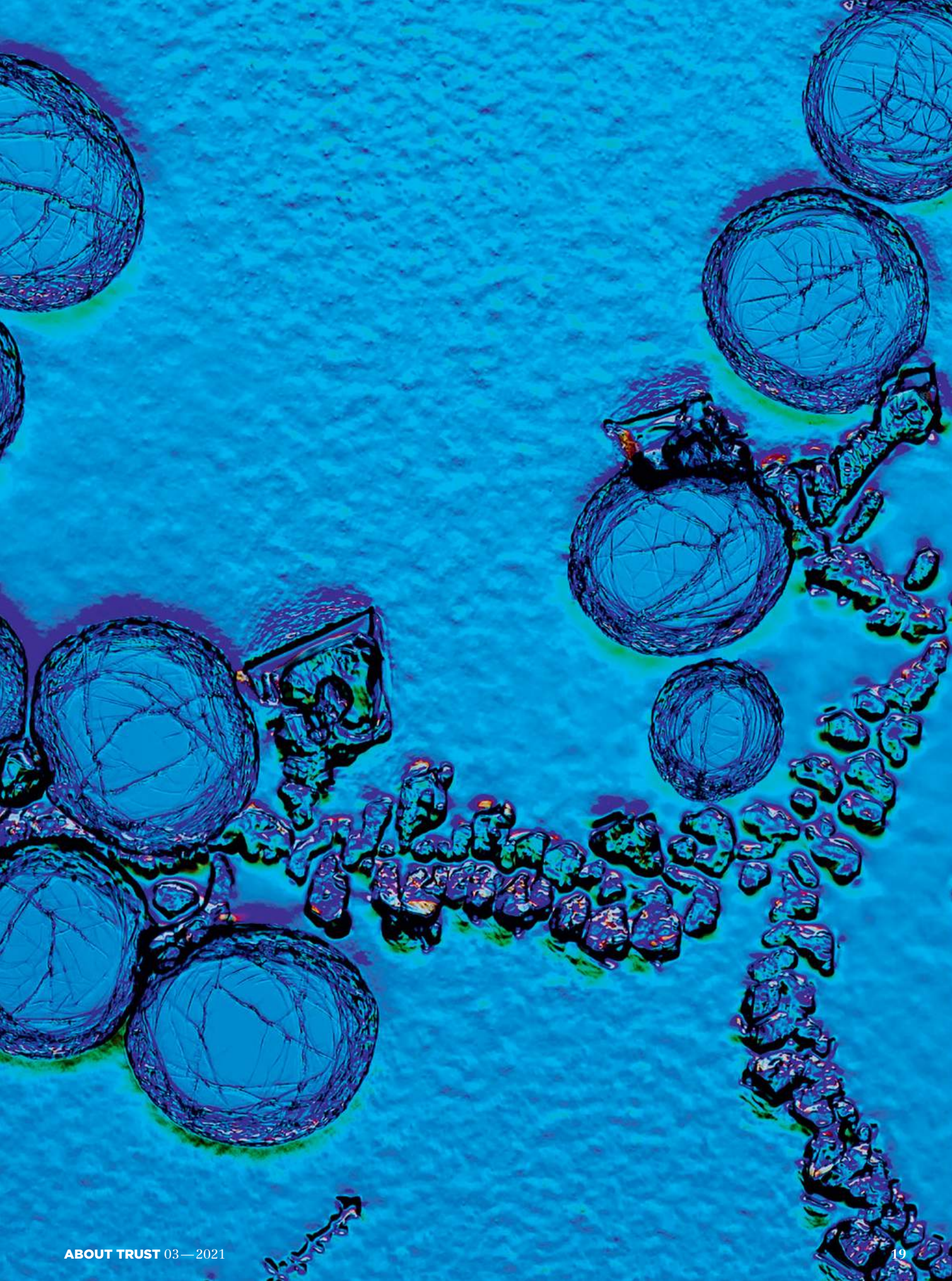
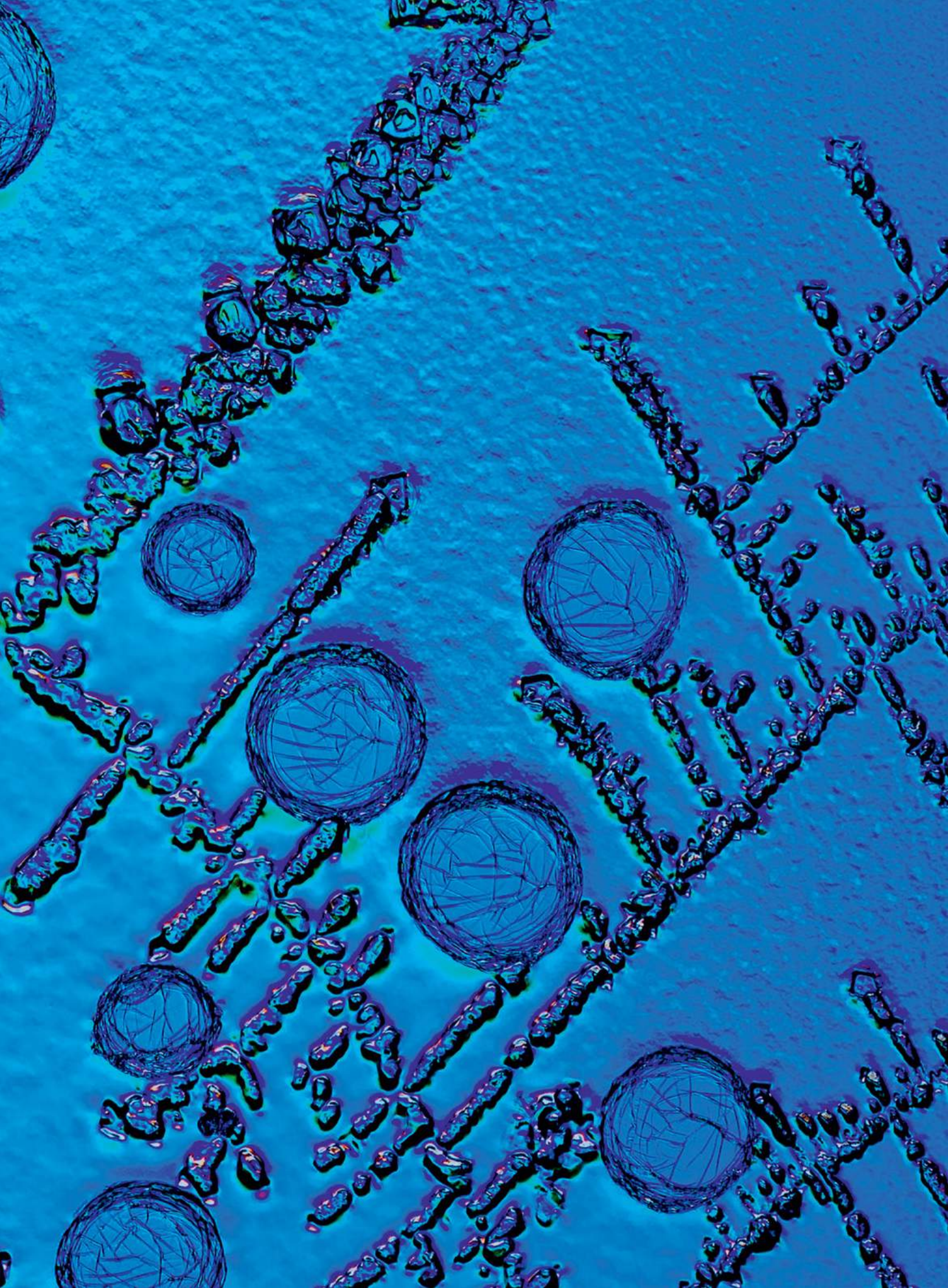


PHOTO: *Science Photo Library/Antonio Romero*





Inside View

“An ethical **OBLIGATION** to patients.”

“In-vitro diagnostics is one of the most important fields in medicine today. It includes every type of laboratory testing of samples taken from the human body. Well-known examples include pregnancy and blood-sugar tests, but also tests for HIV. At TÜV SÜD, we certify these products. Firstly, we examine whether or not the tests perform as promised and secondly, whether they are safe and meet the legal requirements. Our clients include the most renowned and largest manufacturers in the industry.

Of course, we need highly qualified personnel for this task. A degree in the natural sciences is a prerequisite, and many of our colleagues have doctorates. Alongside this, relevant experience is another requirement—our employees should have been working in the field of in-vitro diagnostics for at least four years. At the moment, we have an unprecedented demand for new employees. Starting next year, the new EU regulation for in-vitro diagnostics will come into full force, according to which companies will only be allowed to self-certify their products in exceptional cases. This had previously been allowed if the company’s quality management system was audited by external providers.

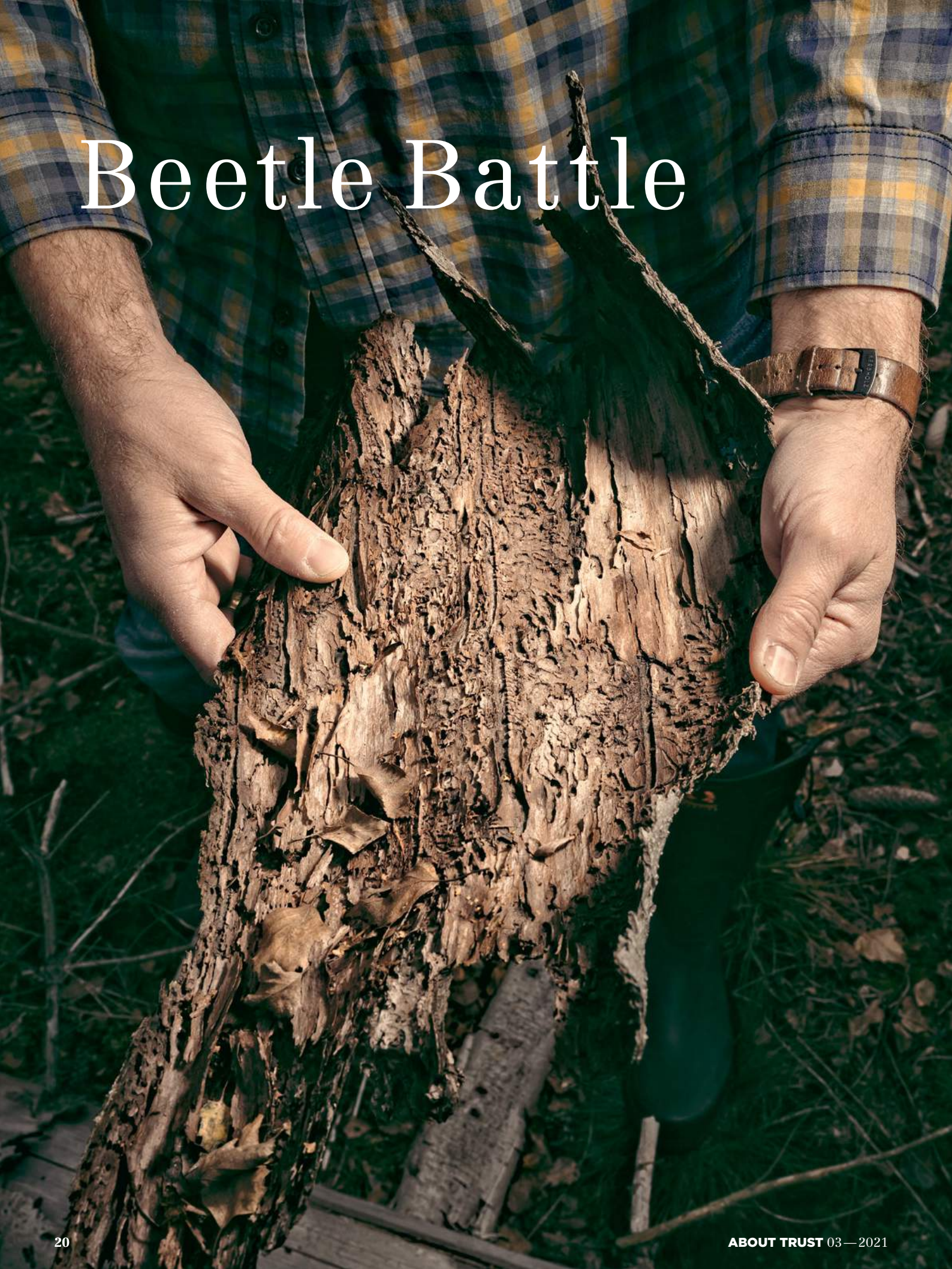
The past two years have been very challenging for almost everyone working in the medical environment. At TÜV SÜD, for example, we coordinated with Germany’s Federal Institute for Drugs and Medical Devices regarding certification and approval of tests for the Covid virus. At times we were receiving up to ten inquires a day. We always view such tasks as an ethical obligation to patients, who must be able to rely on the safety of the products. The fact that we were able to ensure the safety of the corona tests with our screenings and thus contribute to containing the pandemic makes me proud.”

DR. THOMAS THEISEN
HEAD OF THE IN-VITRO DIAGNOSTICS DEPARTMENT AT TÜV SÜD

IN VITRO
The Latin term means “in the glass” and refers to organic processes that take place outside of an organism. Such diagnostics form the basis for blood glucose tests, for example. The large image shows insulin crystals as seen through a light microscope. Insulin deficiency is one cause of diabetes.

PHOTOS: *Florian Thoß (Portrait); Getty Images/MEHMETTAYLAN (Hands)*

Beetle Battle



from ABOVE

TEXT ZOLA SCHUMACHER **PHOTOS** ROMAN PAWLOWSKI —— Due to a warming climate, the bark beetle has become one of the greatest threats to German forests. Can satellite imagery help stop the plague and protect the trees?

A few years ago, when Thomas Meyer heard that a landowner in his area wanted to sell a section of forest, he thought: How about it? For his whole life, the 48-year-old forester had been responsible for other people's forests, some 3,000 hectares located around the city of Nauen in Brandenburg, Germany. So why shouldn't he have his own forest for a change? He looked at the parcel: around 8,000 square meters—about one and a half football fields in size—full of birch and spruce trees, typical for the area. Meyer decided to buy it for the price of 5,500 euros.

Now, a few years later, Meyer is at his plot and looking at what's left of it. It's 40 meters wide and 200 meters long and half of the area is empty; almost all of the trees have been cut down. There are still a few young larches that Meyer recently planted, an oak tree that survived and a handful of old spruces, but the latter no longer have needles—in fact, they're dead. "Of the 5,500 euros, maybe about 500 remain," Meyer says, clearly disappointed.

Meyer's plot fell victim to the bark beetle—not just one bug, of course, but thousands upon thousands of them. A single insect is just four to five millimeters in size and yet is one of the greatest threats to German forests. Every year, the number of trees felled due to bark beetle infestations reaches new records. Foresters have been forced to clear-cut entire forests. In North Rhine-Westphalia alone, the tiny insect has destroyed around 44 percent of the spruce stand since 2018.

Of course, bark beetles are nothing new. They've always been around, but trees used to be better able to defend themselves against them. If a bark beetle tried to get under a tree's bark, the tree started producing resin, which the beetle then got stuck in and died. Yet the warming weather has changed conditions in favor of the beetle. Trees need plenty of water to produce resin, and water is becoming increasingly scarce. And the bark beetle has been able to reproduce like never before.

Meyer is almost helpless against the bark beetle, and he's not alone. There are around 2 million people who own private forest plots in Germany, totaling almost half of all German forests, around 5.5 million hectares—almost twice the size of the US state of Massachusetts. Almost all of these owners are desperately searching for a way to protect their forests against the tiny insect. Meanwhile, young entrepreneurs in Stuttgart, Germany, and Graz, Austria, are working on highly sophisticated technological solutions to contain the spread of the beetles. Using satellites, clever algorithms and infrared scanning, they hope to contain the pest. Will they be able to win this lopsided battle?

ATTACKED
The beetle crawls underneath the bark, where it then bores small tunnels that cause the tree to die.

The end of Meyer's plot was insidious. It started in autumn 2017 with a big storm and winds that devastated the forests in the area. On Meyer's plot alone—just under a hectare—the storm felled 20 to 30 trees; around 1,000 succumbed in the entire forest. Fallen timber is even more attractive to bark beetles. The fallen trees should have been taken out of the forest quickly, but it took Meyer a year until he finally got the equipment he needed: what are known as harvesters, special wood harvesting machines that grab trees, fell them and sometimes even process them into wood chips. For trees that are dangerously close to streets or buildings, then Meyer needed cable skidders. None of that was available, at least not quickly enough.

RACE AGAINST THE CLOCK— AND AGAINST LARVAE

Then came a drought in 2018: perfect weather for reproduction among the beetles. In 2019, his trees weren't looking so good any more. Meyer immediately recognized the presence of bark beetles from the sawdust on the ground around the trees. The trunks were peppered with tiny holes. The bark was already falling off some trees, but they hadn't yet died. Meyer knew time was of the essence.

"Time is everything," Meyer says. "As soon as you think there might be something, you take a piece of bark and look to see how far along it is," he explains. He walks over to one of the dead spruces on his plot and breaks off a piece of bark to illustrate what he means. "There's even still one in its full glory." And, in fact, Meyer pulls out a tiny black beetle from a tunnel and holds it between his fingers.

The bark also reveals how the beetle proceeds. First the beetle bores its way beneath the bark and digs out a large tunnel where it lays its eggs. As soon as the larvae have hatched, they too dig tunnels that are smaller and daintier than those of the mother beetle.

A bark beetle larva needs six to eight weeks to develop, then the young beetle flies away and bores its way into the next tree. The previous tree is left behind, dead, because its bark functions much like a circulatory system, transporting the water supply for the entire tree. The tunnels bored by the beetles

EXTERMINATED
Thomas Meyer stands in the forest. There used to be a magnificent stand of trees here, but in recent months they've fallen victim to a tiny enemy: the bark beetle. There's not much left of his investment.

FELLED
It's all about time for Thomas Meyer. As soon as the first trees have been infested by the bark beetle, they need to be felled as quickly as possible. To protect his saplings from animals, he's encased them in tree tubes.

interrupt these connections and the tree dies of thirst, so to speak.

"To prevent the infestation from spreading, the trees must be felled together with the beetles beneath the bark and removed from the forest as quickly as possible and taken to the sawmill," Meyer says. But to do this, the equipment must be available to chop down the trees and take them away, for example the harvester or the cable skidder. Since forests throughout Germany are suffering from bark beetle infestations, foresters and equipment are in high demand, but scarce. Aside from which, the sawmills are hopelessly overfilled. "They've been drowning in wood in recent years," Meyer says.

Meyer had to store some of the wood in the forest until the sawmills could take it. While it lay there, the beetles were able to spread further. At some point, Meyer just gave up and left the dead spruce where it stood. He knew he had lost the battle.

"My job hasn't been fun the past few years," he says dejectedly. Nauen's forester has been observing the area's forests for years. It all used to be green, but now the forest would look like a patchwork of color from above. What percent of the spruce trees have been lost in total? "In all of Nauen?" Meyer asks in reply. "In Nauen, all the spruce trees are dead."

CREATIVE ENTREPRENEURSHIP TO THE RESCUE

In Stuttgart, 600 kilometers southwest of Nauen, sits the young engineer Tobias Jäger. The 33-year-old with brown hair is in a small, somewhat sparsely furnished office, and is talking about how it happened that his startup, Waldstolz—Forest Pride—is trying to help private forest owners in their fight against the bark beetle, even though he's had almost nothing to do with trees his entire life. At least not professionally, until now.

After studying mechanical engineering in Karlsruhe, Germany, Jäger quickly made a career in business. He had been working for three years when he noticed that he was slowly becoming dissatisfied. He increasingly found himself asking what the point of his work really was. So Jäger confided this to his friend Fabian Popp. Popp is a creative entrepreneur who founded his first startup while attending university and launched a card game, Pub Quartets, with coupons for local bars in Karlsruhe. At the time, Popp was working for a chainsaw company and was craving something more.

The two told themselves that they were too young for such monotony and decided to leave behind the security of their regular jobs to start something together. Without knowing exactly what they wanted to do, they submitted their resignations and started brainstorming. They spent a year juggling ideas.

"We quickly arrived at the forest," Jäger recalls. Also because Popp had spoken with a lot of foresters at the chainsaw manufacturer and had learned a lot about their struggles against the bark beetle. "In the forest, we're experiencing a changing climate right on our own doorstep. That's what we wanted to build on." The topic of forest protection also seemed to have potential from an economic standpoint as well. After all, half of the forests in Germany are privately owned.

So the two of them sought out foresters and forest owners and asked: What is the biggest problem in the fight against the bark beetles? "The answer was always: time," Jäger says. "As a private owner of forest plots, as soon as the weather gets warm, you have to check each tree every two weeks and see if the beetle has flown in. That's not feasible for many owners. So we asked ourselves: How can we solve this problem?" The solution they came up with: remote monitoring.

Four weeks after a beetle has landed on a tree, its needles begin to slowly turn brown. The tree isn't dead yet, nor has the beetle moved on. There are now two to four weeks' time to fell the tree and get it out of the forest. If the color of the trees could be monitored from above, it would be possible to recognize the presence of the bark beetle without needing constant monitoring of the site from the ground. But how?

Drones are far superior to satellite technology as far as image quality is concerned. "But drones are logistically costly. You have to physically go there, and then you're not allowed to fly the drone during certain bird breeding seasons and so on," Jäger says. "Satellite images are more independent. They're up in the air no matter what. And take new pictures every five days."

In 2020, Jäger and Popp came across the Austrian company Joanneum, which was pursuing the same idea as part of a research project and had developed a program that detects color changes in the Austrian forest on satellite images. They formed a cooperation. "It was ideal for us because we didn't have to reinvent the wheel, just adapt the technology to the different configuration of the forests in Germany," Jäger explains.

"Of course the bark beetle isn't always present when there's a warning. But in the past few weeks, we've had a hit rate of 70 to 80 percent."

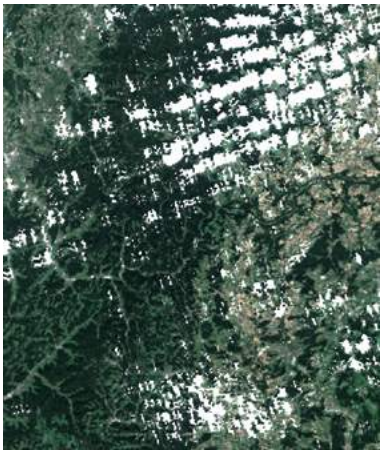
TOBIAS JÄGER, FOUNDER OF WALDSTOLZ

Jäger opens some current satellite images from the European Space Agency on his computer. The satellite that sends new images to the startup Waldstolz every five days is called Sentinel-2 and belongs to the European Union's Copernicus Program. "Sentinel-2 has a comparatively good camera and also displays a lot of data in the non-visible range, for instance in the near-infrared range," Jäger explains. "And especially in this near-infrared range is where there's a lot of information about a tree's health and vitality."

The human eye alone can only recognize a tree's leaf color. Sentinel-2, on the other hand, scans with infrared beams, which hit needles and leaves and then are reflected back to the satellite. The strength of the reflection is a measure of how healthy the tree is. If it's very unhealthy, it reflects hardly anything back at all. Jäger and Popp make use of this data.

Each image from Sentinel-2 shows a square with an area of 100 square kilometers. Jäger opens one showing the Allgäu region in southern Germany and enlarges it. If you think you're going to see individual trees, you're sadly mistaken. What you actually see is mostly just individual green pixels. Each pixel represents an area of ten-by-ten meters. The pixels on satellite images from Google Maps show 30 by 30 centimeters, but such detailed images are only taken every few years and don't have any data from the near-infrared range.

Each new satellite image must first be processed. This means, for instance, that clouds and shadows cast by the sun must be calculated out. The program developed by Joanneum uses an algorithm to calculate how the forest should be developing at this or that location. To do this, the algorithm uses satellite images from the past four years and the vitality data available from them. "It's a very complex model, because the vitality can only be determined in relation to the previous data," Jäger says. Explaining what he means, he continues: "Every small area of forest behaves differently and thus has different health and vitality values depending on how it is planted or what season it is." For instance, a section of the forest with deciduous trees can be expected to have a radical drop in values in autumn when the trees suddenly lose their leaves. That's no reason to panic. If, on the other hand, a coniferous tree suddenly has low vitality values in autumn, that's much more worrisome.



MONITORING
Tobias Jäger and Fabian Popp have developed an app that aims to contain the bark beetle with the help of satellite imagery.

The algorithm then compares the data from the new satellite image with the data that the model had previously predicted for the forest. If the data deviates too far from the predicted value, the algorithm flags the image at that spot. However, a single tree with changed values isn't sufficient on its own; the algorithm requires a small group of at least two or three trees with lower vitality data to be able to recognize the changes and sound the alarm. Forest owners are then automatically warned via text message and email. Armed with a map and GPS data, they can then check to see if the bark beetle has arrived and no longer have to examine every single tree.

FIFTY CLIENTS FOR THE PILOT PROJECT

In the forest in Nauen, forester Thomas Meyer is skeptical when he hears about the monitoring service by Waldstolz. He believes that if you own a forest, you also need to be present. He also worries about false alarms. "Just because the crown discolors, it doesn't mean that the bark beetle has actually infested the trees," Meyer says. "Maybe it's discolored because the trees are suffering due to drought conditions."

In Stuttgart, they disagree. "Of course the bark beetle isn't always present when there's a warning," Jäger says. "But in the past few weeks, we've had a hit rate of 70 to 80 percent." At the moment, Waldstolz only offers its monitoring service in the Black Forest and in the Allgäu. A total of fifty clients are using the service in its pilot project phase, most of whom are private owners. Next year, Jäger and Popp plan to expand their services and monitor other areas in Germany.

It's already too late for Meyer. He isn't planning to plant any new spruce trees on his plot and instead will focus on larch and maple. The bark beetle isn't so keen on those species.

Meyer carefully examines a small maple sapling that is showing its first leaves, close to a path through the forest. It's already over a meter tall. "One more year and it will be so big that the deer won't be able to eat it," Meyer says, full of hope. That is an enemy he can handle on his own.

ZAPPED

Lightning causes billions in damages worldwide every year. The technology company Trumpf hopes to remedy this situation using a laser cannon.

Ancient peoples interpreted thunder and lightning as threats from the gods. In Europe, they saw the bright flashes of light in the sky as a sign of an angry Thor throwing his hammer or the Olympic god Zeus exploding in rage. Nowadays, the explanation is a bit more scientific: raindrops can become electrically charged in a thundercloud. The particles in the upper part of the cloud have a positive charge and those in the lower part have a negative charge, creating electrical tension. This is released in a flash of lightning.

This type of natural phenomenon can be extremely dangerous. In Germany alone, between thirty and fifty people are hit by lightning every year, often while jogging or cycling. The economic impact is also sizeable. There are billions in damages annually from lightning strikes to airports, power plants, skyscrapers and forests. In the United States, lightning causes annual losses amounting to 5 billion dollars, mostly due to disruptions in air traffic and damage to planes and high-voltage power lines. German household and residential building insurers had to pay out around 200 million euros for lightning and power surge damage in 2019.

Hope is now being offered by a supplier of machine tools in Swabia, Germany. To help prevent damage from random lightning strikes, TRUMPF has been working with the University of Geneva on the EU project Laser Lightning Rod. At the top of Mount Säntis, in Switzerland, the team is attempting to divert lightning from thunderclouds in a controlled manner using a laser cannon. The EU has pledged 2 million euros in funding for the research project.

Clemens Herkommer, an engineer at TRUMPF Scientific Lasers in Unterföhring, near Munich, has been working on this project for four years. At least the idea behind it is easy to explain: the powerful laser beam is shot into the clouds during a thunderstorm, electrically charging the air around the beam to such an extent that it creates a plasma channel. "We're shooting the laser beam into the clouds at a rate of one thousand pulses per second," Herkommer says. Since the channel is good at conducting electricity, lightning bolts strike inside the laser beam and are then guided to the ground through the channel. The laser beam cannot be seen because its radiation is at the infrared end of the spectrum and thus invisible to the human eye. But it does hum: the highly energetic laser flashes heat up the air surrounding them, thereby creating small pressure waves.

Implementation of this ambitious plan has been anything but easy. Just getting the laser to the mountain's summit, at 2,500 meters, took two weeks. The team used cable cars and helicopters to transport the partly disassembled laser up Mount Säntis at the end of May 2021.

Thus far, at least, the TRUMPF laser is one of a kind. Other projects haven't managed to create the plasma channel through the clouds for long enough and barely made it to ten laser pulses per second. In this case, the lightning seeks its own path and doesn't react to the laser.

Fortunately, the company won't have to worry about having enough data to measure. Hundreds of lightning bolts strike the Mount Säntis summit during the peak season for thunderstorms from June to September—more than enough for some electrifying results.

PHOTO: *Trumpf*

Ice, Ice, SAVE

TEXT JAN SCHULTE **ILLUSTRATIONS** ANTON HALLMANN — Special airbags are designed to save the lives of winter sports enthusiasts caught in an avalanche. The technology is likely to become more and more important in light of the increasing popularity of ski mountaineering and backcountry tours. Here's a look at how they work.

HOW AVALANCHE AIRBAGS WORK

Avalanche airbags are anchored in a special backpack. Once deployed, they quickly maximize a skier's total volume so that the person rises to the top of the avalanche debris instead of sinking to the bottom. A skier triggers the airbag by pulling a handle on a cord. This sets off a carbon-dioxide cartridge that inflates the airbag. Relatively new to the market are also airbags that use an electric blower for inflation.

TÜV SÜD TEST

When purchasing this sort of product, winter sports enthusiasts should make sure to choose one that bears the blue TÜV SÜD octagon. The seal confirms that the backpack has been tested according to DIN EN 16716, the European standard for avalanche airbag systems. Such systems are tested both in the laboratory and out in the snow in real-world conditions.

EFFECTIVENESS

How much of a difference these airbags really make has long been a matter of debate. What's certain is that they reduce the risk of being buried or at least reduce the depth of burial. According to a 2014 study, the mortality rate for people without an airbag backpack was 22 percent. For skiers with the proper equipment, the rate was 11 percent—but for airbag wearers whose rescue bag wasn't inflated, the rate of death rose to 13 percent. So an airbag can cut the number of avalanche deaths almost in half.

M E !

↳ PEOPLE AND SNOW, SNOW AND PEOPLE

THE WHITE HAZARD
Researchers believe that avalanches will become more common due to a warming climate. The number of victims in the Alps varies greatly from season to season, but the long-term average is around 100 fatalities per season. Whether and how avalanches occur depends on a variety of factors, including the structure of the snowpack and the different layers of snow.

90

PERCENT
of all avalanche victims trigger "their" avalanches themselves

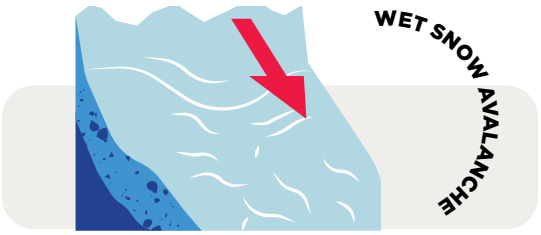
MORE PROTECTION FROM AVALANCHES
An avalanche airbag should always be just an additional means of protection against avalanches. The risk of being surprised by an avalanche can be greatly reduced with good preparation. People skiing on groomed slopes usually don't have to worry about avalanches, because for safety, avalanches are triggered beforehand, diverted or kept in check with special fences. Skiers who go off-piste, however, should plan their tour well in advance, including the most recent avalanche situation report. A probe, avalanche beeper and shovel are part of the mandatory equipment.

MINIMUM REQUIREMENTS
There has been an EU standard for avalanche airbags since 2017. Accordingly, their minimum volume is 150 liters, and they must reach maximum volume five seconds after deployment. If the avalanche comes to a stop before the airbag is completely deployed, the likelihood of being buried increases.

↳ TYPES OF AVALANCHES

Snow on mountains usually builds up in layers. In large snow slab avalanches, an entire slab of snow begins to slide on a looser layer and can reach enormous dimensions and speed. 95 percent of all fatal avalanches fall in this category.

In these avalanches, individual snow particles lose their grip in steep terrain, roll downhill and gather more particles as they fall. This type of avalanche is usually harmless because it doesn't contain as much snow as other types.



Probably due to climate change, wet snow avalanches are becoming more common. They can occur completely without warning as snow melts and can happen at any time of day or night.

Safe, safer, **SMART**

TEXT FELIX ENZIAN **ILLUSTRATION** BRATISLAV MILENKOVIĆ —— Digitally networked administrations and systems are probably the best key to controlling natural disasters, epidemics and other dangers. How smart cities and regions can help protect us.

The earth shakes and a tsunami begins to surge—and people know about it, several minutes before it hits land. This is possible today thanks to sensors on the coast and seabed that send data about the earthquake via GPS to the mainland, where millions of people can then get an emergency alert on their cell phones. This Smart Region achievement protects people all over the world from natural disasters. Even in our immediate environment, data helps prevent the worst on a daily basis. During a pandemic, for instance, vital information can be bundled in an app so that authorities and the populace will always be up to date on the availability of hospital beds, doctors, vaccines and other resources. Even in more normal times, cameras and sensors assist in monitoring roads and buildings, preventing accidents and helping solve crimes.

However, the crises in 2021 have revealed that there's still a lot to be done in terms of digital networking. During the corona pandemic, vaccine campaigns were often too slow, also due to insufficient flows of information. People drowned in their homes during the catastrophic floods in Germany because they didn't receive warnings or the urgency of the situation wasn't clear. Forest fires in southern Europe, California and north Africa have shown affected communities how vital efficient warning systems will be in the future.

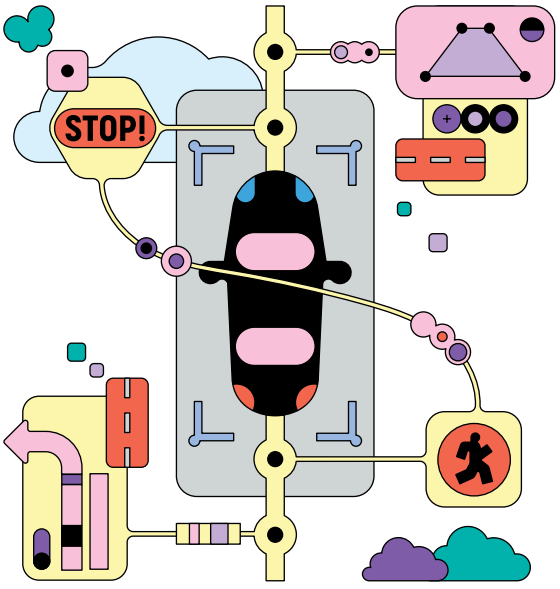
NOT ONLY BIG CITIES NEED TO BE SMART

One person who is possibly following this more closely than anyone else in the world is Soo-Jin Kim. She is an executive at the OECD Centre for Entrepreneurship, SMEs, Regions and Cities. This department in the OECD, an intergovernmental economic organization, advises national and local governments in improving the effectiveness of Smart City systems. She says: "During the early stage of the corona pandemic, some countries such as South Korea proved to be much more prepared/equipped than some other countries because of their advanced degree of digitalization and their experience with past epidemics." The South Korean capital Seoul, for example, benefited from the fact that it had already developed a data hub and a digital strategy to quickly trace and break chains of infection, even before the corona pandemic. Visits to shops and restaurants are recorded by scanning a QR code. While this is common practice in other countries, South Korea takes it a few smart steps further. If there's an infection, the data flows to the Korea Disease Control and Prevention Agency (KDCA) for contact tracing, otherwise it's deleted.

In addition, the KDCA also examines cashless transactions and cell phone networks to supplement the information on the whereabouts of infected persons and to send anonymized alerts to potential contacts. "South Korea has managed to balance data transparency and data privacy in their pandemic response due to a higher degree of public acceptance, which is not necessarily the case in other countries for cultural and historical reasons," Soo-Jin Kim says.

Nonetheless, Smart City concepts shouldn't just be tailored to metropolitan areas. Rural and underdeveloped areas will require support in establishing Smart Regions. "If digitization strategies are thought through in an interdisciplinary way and include all parts of the population, this can produce smart communities where people can live more sustainably and safely," she adds.

So how can we all benefit from clever algorithms and rapidly flowing data? The following five examples from disaster management, healthcare, crime prevention, environmental safety and road safety show what's possible right now.



TRAFFIC SAFETY

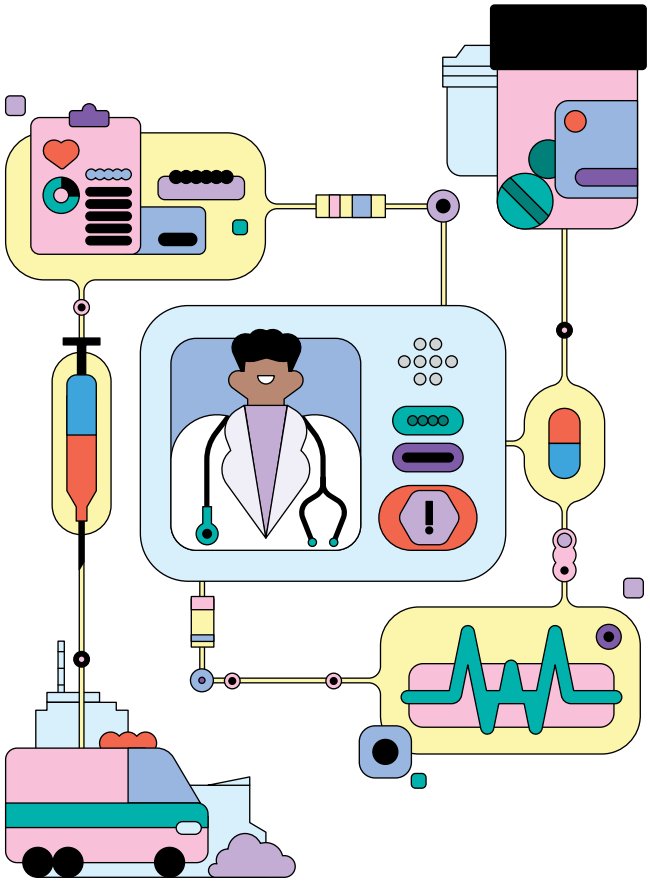
AUTONOMOUS DRIVING REDUCES ACCIDENTS

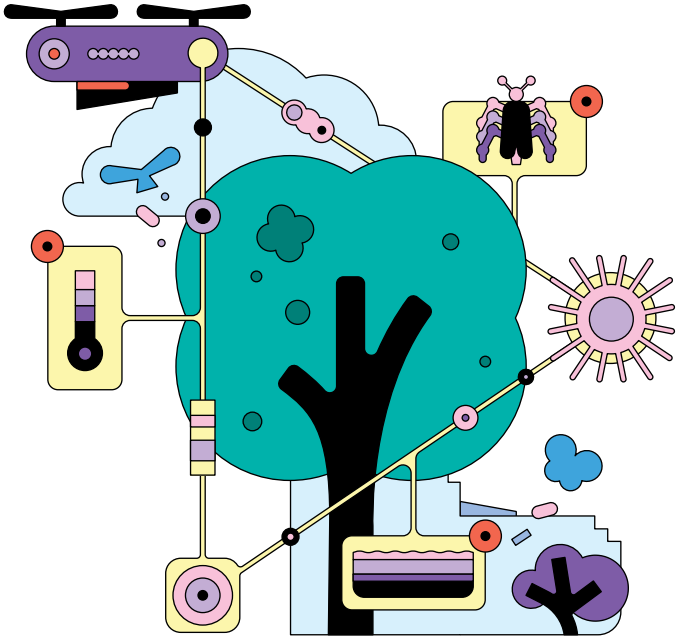
Traffic planners expect autonomous driving to improve traffic flows. With the help of radar, cameras and sensors, driver assistance systems are already monitoring and controlling speed, safe distance between vehicles, lane-changing and turning. Emergency braking is already much faster and safer with automatic systems than when attempted by drivers. The new 5G mobile communications standard enables vehicle sensors to reliably communicate with each other and with those in the traffic infrastructure. In poor visibility situations, for instance, drivers can receive an automatic warning signal from vehicles ahead of them at a traffic light—and thus begin braking in time. Smart street lighting also makes use of this technology. As soon as a vehicle or pedestrian approaches, the lighting gets brighter and thus safer.

HEALTHCARE

PRECISE MEDICINE WITH ROBOTS

Technological advances are making it possible for public health systems to provide people with better care—without them even having to leave their own homes, in some cases. Take Barcelona for example, which has been demonstrating this for a number of years. The Catalan city began its telecare system back in 2013, providing elderly and infirm people with specially designed telephone intercoms and a remote control that they can wear around their necks. If they have an emergency, they can use this remote control to activate the phone, even if they are in another room. A loudspeaker and microphone switch on and the health services center can hear what's happening there. If necessary, the center can decide to send an ambulance. This system could theoretically be expanded to include other services. The telecare system could also be used to monitor the vital signs of participants and, for instance, alert the ambulance if it detects an irregular heartbeat. Especially during epidemics, contact tracing and quarantine monitoring could also be carried out using this model.





ENVIRONMENTAL SAFETY

SMART FORESTRY PROTECTS THE WOODS

Environmental risks can be controlled and reduced through digital networking. In Lower Saxony, Germany, the Ostfalia University of Applied Sciences is implementing the Smart Forestry project. They're monitoring the condition of trees and plants via walk-throughs, counts, aerial photography and drone flights. The use of 5G makes it possible to utilize an especially large number of autonomous sensors with long ranges and low energy consumption. The data acquired can then provide information about climatic influences, pest infestations, drought and fire risks. Sensors can also be used in bodies of water, for example to measure water quality or monitor river levels, to better predict the chances of flooding.

CRIME PREVENTION

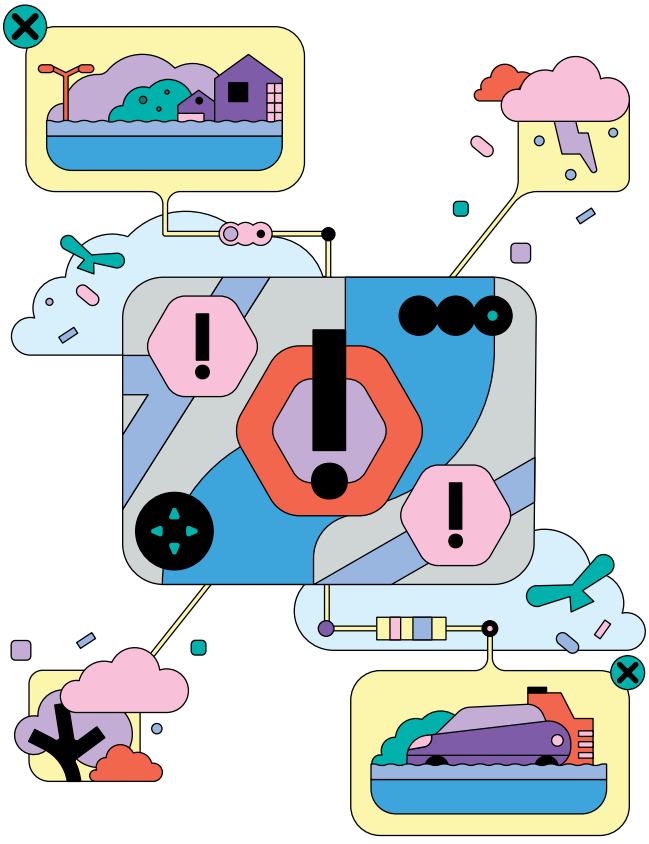
SENSORS DETECT GUNSHOTS

Bang! When shots are fired out on the street, people rightly flinch, but it often isn't exactly clear where the noise came from or whether or not it came from a weapon. In Denver in the US state of Colorado, authorities have now tested sensors that detect and locate potential gunshots. They send an audio recording to a human analyst who can then alert the police in less than 60 seconds in the event of an emergency. This way police can reach the scene sometimes even before residents have dialed the emergency 911 number. Injured people can receive treatment more quickly and the police can more quickly apprehend criminals.

DISASTER MANAGEMENT

THE DISASTER BOT SAVES LIVES

During the rainy season in Indonesia, when the Ci Liwung River overflows its banks and floods the streets of Jakarta, PetaBencana.id, a disaster bot, evaluates the situation. The software scans social networks such as Twitter and Facebook for photos and news about the floods. As soon as someone in Jakarta posts the word *banjir* (flood) and tags @PetaJkt, the bot automatically answers and asks for confirmation of the tweet with georeferenced photos. The platform combines all the incoming information and creates a visualization. Within just minutes, a continually updated online flood map is created. It shows which sections of streets are affected and how severely. Residents can avoid those areas and the city authorities know where help is most urgently needed. In this case, high-water selfies can literally save lives. The use of the disaster bot has proven its value in the Indonesian capital and will now be expanded for use in other regions of the country.



Just One Word

Mr. de Masi, what do you think about …

S E C U R I T Y ?

Fabio de Masi, 41,
is passionate about the future of the financial markets. Among other things he is a writer, (former) politician and member of the German far-left party "Die Linke". In the German "Bundestag" he made a name for himself as a financial investigator and pushed forward political investigations into several major financial scandals. He was deputy chair of his party's faction from 2017, and a member of the European Parliament from 2014 to 2017.

Our finances require protection. This is a prerequisite for planning our lives. A lot depends on the security of our finances, for instance whether we dare to try something in life or how free we are. I noticed this for myself very early in life. I come from a low-income household and left home at an early age. At seventeen I had to take odd jobs and it usually wasn't enough to pay for my apartment. So I borrowed money from my aunt that I wanted to pay back quickly, and later I had to take out student loans to study abroad. It felt like a burden to me. I can still exactly recall how I was able to finally pay off the last of my loans with my first allowance payment as a member of the European parliament. It was such a sense of liberation.

But I'm not the only one who feels this way. People are increasingly asking how they can manage to afford collateral, such as their own home, and whether or not their old-age pensions are still secure. On top of all this are the low interest rates, which mean that savings accounts are no longer a reliable investment. We've had phases in the past with lower real interest rates, but wages were increasing much more back then. In other words, we didn't notice it as much. That's why I understand that many people are looking for alternatives, such as investing in the stock market. That can make sense if the investments are broadly diversified, but this should only be supplemental to a strong government old-age pension. And to achieve that, we need everyone to pay into it. After all, financial crises are happening more often and if everyone turned to the stock market, then the returns would fall there, too!

To ensure that we don't lose trust in our money, we must also protect it in the digital age. I view the rise of cryptocurrencies with skepticism so far. We will also see crises in this field, perhaps even panics, and, accordingly, people's money there is also at risk. Unlike with state currencies such as the euro, dollar or British pound, there's no institution like a central bank behind crypto. I think that is crucial. To counter this, we need a digital euro, one guaranteed by the ECB. We need to be able to use it to make payments quickly across borders on the internet so that we can continue to trust our money in the future.

ILLUSTRATION: *André Gottschalk*; PHOTO: *Getty Images / Morris MacMatzen*

Picture This

The worker fearlessly faces the seething and sizzling fire. Temperatures in industrial blast furnaces can rise to more than 1,000 degrees Celsius and, once lit, the fire can remain burning for years to satisfy the world's hunger for steel. The industry produces 700 million tons of crude steel every year. Despite a high degree of automation, some jobs still need to be performed by hand and that will remain the case for the future. For instance, workers must clean the run-off channel or check the quality of the steel in the furnace. It's dangerous work. Protection comes in the form of special suits, reminiscent of those used for space walks. They are composed of several layers—the inside ones are often made of insulating materials such as aramids or imides with a metal coating such as aluminum on the outside. This allows the suits to withstand radiant heat of 1,000 degrees, protecting workers from the blazing heat.

HACKERS in black hoodies
in a **DARK ROOM** aren't
REALLY a thing any more.

Find out how companies can protect themselves from cyberattacks in our web magazine: **ABOUTTRUST.TUVSUD.COM/EN**