

**GLOBAL THREATS –
AND SOLUTIONS**

The destructive power of cyber attacks, and how ethical hacking and other creative responses can prevent dangers and protect infrastructure

THE PRIVACY PARADOX

Why people fail to keep their personal information confidential – and how insights from hacking can help shape human behaviour

SECURE RETURNS

Pictet on why businesses which provide security solutions in diverse market sectors provide an attractive and profitable investment theme

TO SEE IS TO BELIEVE

An Israeli entrepreneur helps local communities film human rights abuses and corruption, distributing the images to change-makers

PICTET REPORT



Foreword

We live in a digital world where security threats are proliferating and becoming more sophisticated. On a personal level, people find hackers trying to access their personal information online for criminal purposes. Commercial organisations and public bodies face similar attacks, while terrorists and hostile governments use cyber attacks to further their political ambitions.

In this issue of Pictet Report, we examine the nature of these threats and the measures that can protect society against them. Two international security experts set out the fast-growing challenges posed by cyber attacks and call for more creative threat responses to avoid the destruction of critical infrastructure and the deaths of large numbers of people.

Four entrepreneurs explain how their businesses can protect the security of digital information. One uses ethical hackers to eradicate vulnerabilities in online systems, while another uses quantum mechanics to make it impossible to decode data. The third securely destroys redundant hard drives to prevent data theft from old equipment. The fourth provides industries old and new with independent validation to ensure that they comply with global standards of protection.

Two researchers reveal the behaviour that makes hackers' jobs easier. One has investigated why people disclose confidential information which they know they should keep private. The other, a former hacker, is using neuroscience to investigate how the brain shapes human behaviour – and how to change it.

The historian of Britain's Bletchley Park shows how its brilliant code-breakers gave the UK and US a vital advantage in the second world war by deciphering the German military's Enigma code. Their techniques were later used to develop modern computer technologies.

The manager of the Pictet Security Fund at Pictet Asset Management says that investing in security solutions has become an attractive investment theme, with growth driven by innovation, urbanisation and regulation.

Finally, an Israeli entrepreneur tells us how he empowers local communities with security technologies which can be used to expose human rights abuses and corruption.

We hope that you will find it interesting to learn more about the security threats facing the world, and about the solutions being developed by some remarkable entrepreneurs and researchers.

Rémy Best
Managing Partner
Pictet Group

COVER IMAGE – Wheels of German cipher machine Lorenz SZ 42, used during World War II by the German High Command for the most sensitive intelligence

PICTET EDITORIAL TEAM – Ninja Struye de Swielande

DESIGN & EDITORIAL CONSULTANCY – Forth Studio **WRITER** – John Willman

PHOTOGRAPHY – Porter Gifford, Wolf Mike, Anthony Tahlir, Carlotta Cardana, Wes Sumner, Yadid Levy, Christoffer Rudquist and Aurélien Bergot

SUMMER 2017 – For subscription information please contact: privatebanking@pictet.com

HUMAN BEHAVIOUR & SECURITY



4

PROF. LESLIE JOHN
Why people divulge
confidential information



12

PROF. MORAN CERF
Hacking into the brain to change
human behaviour



24

DR PATRICIA LEWIS
Protection for
critical infrastructure



36

DORON BERGERBEST-EILON
The evolving threat from
cyber terrorists

LOOKING BACK



40

DR DAVID KENYON
How World War Two code-breaking laid the
foundations for today's cyber warfare



18

GRÉGOIRE RIBORDY and KELLY RICHALE
A foolproof method of preserving data security



30

MÅRTEN MICKOS
Bounties for bug-hunters make the internet safer

ENCRYPTION / CYBERSECURITY

VERIFICATION



8

JEAN-LUC DE BUMAN
The importance of independent validation

DATA DESTRUCTION



50

SIDDIK APAYDIN and YARON OPHIR
Ensuring the protection of confidential
data until the end

SOCIAL ENTREPRENEURSHIP



46

OREN YAKOBOVICH
The power of film to expose
human rights abuses

PICTET'S VIEW



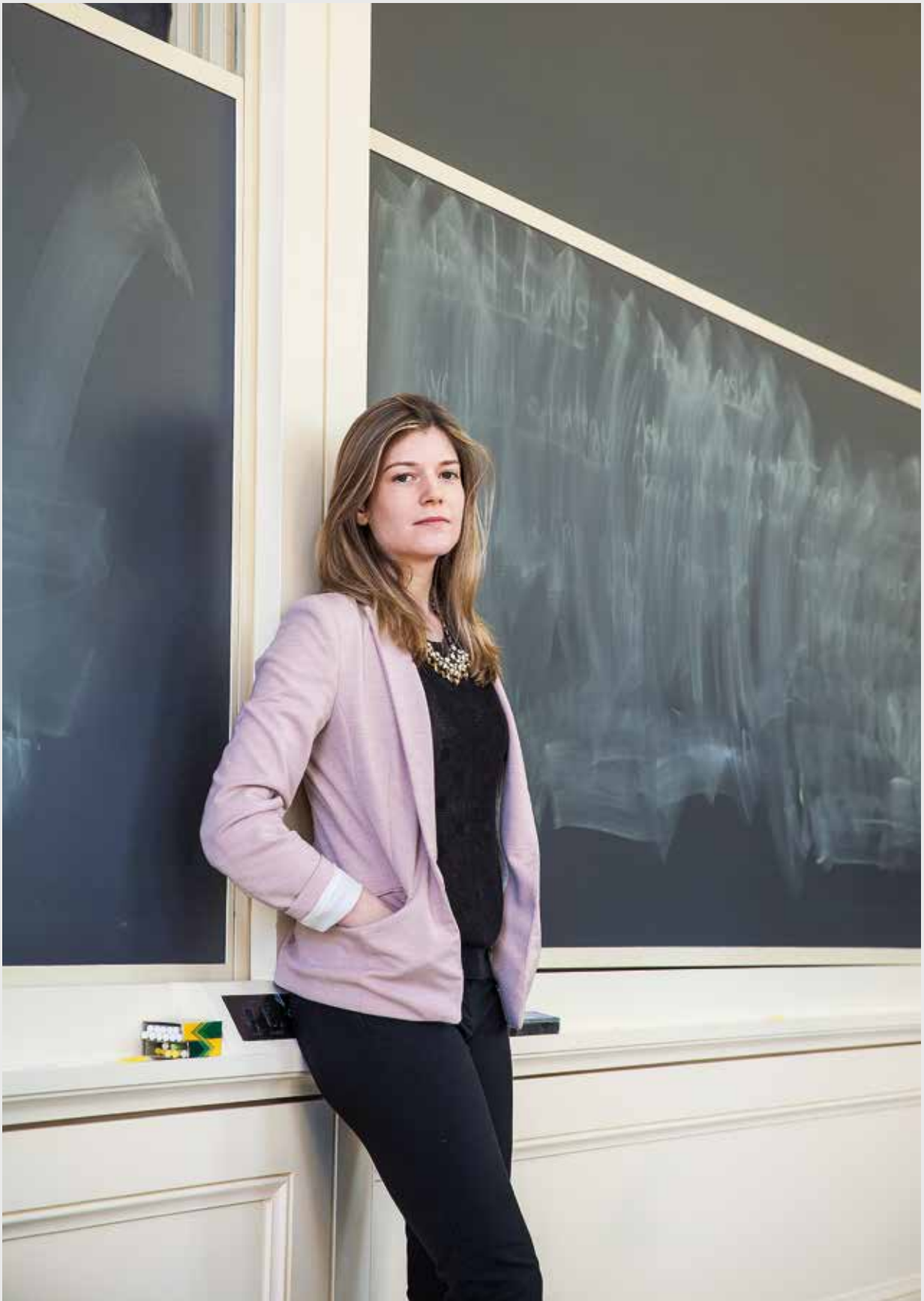
54

YVES KRAMER
Strong earnings growth from an industry
which is expanding fast



Locations

- 1 UNITED STATES**
Prof. Leslie John
Mårten Mickos
Prof. Moran Cerf
- 2 UNITED KINGDOM**
Dr Patricia Lewis
Dr David Kenyon
- 3 SWITZERLAND**
Jean-Luc de Buman
Grégoire Ribordy and Kelly Richdale
Siddik Apaydin and Yaron Ophir
- 4 ISRAEL**
Doron Bergerbest-Eilon
Oren Yakobovich



WHY PEOPLE DIVULGE CONFIDENTIAL INFORMATION

Most people say they want to keep their personal information private, according to Professor Leslie John of Harvard Business School, but in practice they will reveal it for often trivial reasons or to win the approval of others

Privacy is an issue of great sensitivity in a digital age. Many people go to considerable lengths to protect their personal information from online access by strangers, commercial enterprises and public bodies. And users of most social media have to sign up to complex agreements setting out their rights to privacy and how the companies can use their personal information.

Yet very few people read the lengthy privacy statements before signing away rights to the highly confidential information they provide online. And in practice, it can be very easy to persuade people to disclose information which is better kept private. In 2014, for example, an installation artist called Risa Puno extracted sensitive personal data such as fingerprints, driver's licence numbers and mother's maiden names from 380 New Yorkers in return for offering them a cookie – even though she refused to say what she would use it for.

Professor Leslie John, an associate professor at Harvard Business School, calls these contrasting aspects in the psychology of confidentiality and disclosure the 'Privacy Paradox'.

'In the abstract, people say they care about privacy and oppose threats to the confidentiality of online information and private messages. But in practice, their behaviour suggests otherwise, partly because it is so difficult to put a precise figure on the material value of privacy and the damage caused by breaches. As a result, privacy isn't top of mind and people's willingness to reveal confidential information can be affected by seemingly trivial factors like the offer of a cookie.'

Prof John teaches MBAs and people in executive education courses at Harvard Business School. She also carries out research into how people make decisions in fields such as healthy eating and personal privacy. Those decisions are often believed to be made rationally, but her research

reveals irrational decision-making processes, of which the Privacy Paradox is an example.

At the heart of such paradoxes is the fact that humans have conflicting motives when making decisions. They have a sincere desire for privacy, which establishes boundaries that are important to them in various ways. But they also know that disclosure of personal information can make other people like them more, because it is a key part of forging relationships.

Other researchers have demonstrated this aspect of human nature. Pairs of strangers were given lists of questions to ask each other, in order to see how much the answers affected their opinions of each other. This found that the more their answers disclosed personal information, the more the other person liked them.

In another experiment, people were asked who they would choose if one applicant said on a job application

form that the worst grade they had ever achieved in an exam was a fail and another chose the 'no answer' option. The result was that 89 per cent preferred the former – they recognised that the candidate who came clean was the worse candidate but thought them more trustworthy, and were suspicious of people who withhold information.

There is a similar reverse process: the more that people like a website or questionnaire because it appears fun, the more willing people are to disclose information about themselves and set aside privacy considerations.

'Facebook heightens the desire to divulge in a variety of ways that make you want to share,' she says. 'The more people see others sharing a lot, the more they are prepared to divulge about themselves. Meanwhile the website's privacy settings are constantly changed and typically buried under several layers of menus, making it hard for users to review them.'

Humans know that disclosure of personal information can make other people like them more, because it is a key part of forging relationships



‘Another factor that encourages disclosure is that there are often immediate and tangible benefits. As soon as you post on Facebook, you get feedback such as “likes” and comments, which psychology tells us is a form of conditioning that will encourage you to share more.

‘The dangers of sharing online are much vaguer. If compromising pictures are shared, future employers might see them some time in the future, but you don’t know who those employers are, or whether they’ll find them, or what the consequences will be. There is no clear link between your indiscretion and any bad outcome.’

Social media companies have strong motives to get as much information out of customers without alarming them, Professor John adds. It brings in more traffic, and more personal information – both of which can help in attracting advertising.

Another research project explored how willing people were to pay attention to privacy policies. Some companies give prominence to good policies, such as setting out restrictions on how they will use personal information. Others do not mention their privacy policies on order forms – an example is a company selling a car GPS system which has ‘additional features’ that effectively spy on the driver.

‘Sometimes, people are more likely to buy things from companies which do not mention privacy policies. Far from reassuring consumers, making such policies salient seems to set off alarm bells!’

A new development in social media which might help avoid postings such as embarrassing photos coming back to haunt people in later life is to make online sharing temporary. SnapChat, for example, deletes postings after 10 seconds – and while they can be saved by screen-grabs, it is not easy.

‘But if an embarrassing photo vanishes, the impression it made on the recipient may not,’ says Professor John. ‘And that impression can be shared on social media, which might not have happened if the photo hadn’t been deleted.



‘To test the impact of a deleted image, we asked people to take selfies and share them online, some to be permanently visible and others only temporarily. They were more likely to take and share indiscreet selfies if told they were temporary, yet viewers thought that those who had taken racier photographs had worse judgment – even if they were quickly deleted. In other words, the character of the photo creates an impression, even if shared only temporarily.’

People are spending more time shopping, gaming and socialising online, at a time when data-gathering technology is becoming ever more sophisticated. Yet people still divulge sensitive personal information that can be of enormous value to firms and to more malign hackers. The Privacy Paradox suggests that more needs to be done to help people understand the value of privacy and how easy it is to part with sensitive information, while recognising the value of sharing appropriate information in personal relationships. ●

Leslie John is an associate professor of business administration in the Negotiations, Organizations and Markets unit of Harvard Business School. She teaches the Negotiations course in the MBA elective curriculum, as well as in various Executive Education courses. In the past, she has taught the core Marketing course in the MBA required curriculum. She holds a doctorate in behavioural decision research from Carnegie Mellon University, where she also earned an M.Sc. in psychology and behavioural decision research. Professor John’s research centres on how consumers’ behaviour and lives are influenced by their interaction with firms and with public policy. Her work has been published in academic journals, and has featured in publications such as *The New York Times*, *Financial Times*, *The Wall Street Journal* and *Time* magazine.



The importance of independent validation

Geneva-based SGS provides teams of experts to help businesses become faster, simpler and more efficient, ensuring compliance with fast-evolving global standards and local regulations that protect customers and consumers

In the early days of SGS, the company specialised in inspecting shipments of grain arriving in large French ports from elsewhere in Europe, North America and further afield. Its network of inspectors would verify the quantity and quality of the grain which tended to shrink in volume during transit, especially on loading and unloading.

From its launch in 1878, the company grew fast: by 1913, it was inspecting 21 million tonnes of grain a year from a network of 45 offices throughout Europe and had become the leader in the grain inspection business. Today, it has become an industry leader in a much wider range of inspection activities, with around 90,000 employees and 2,000 laboratories operating in nearly every country in the world.

The nature of its business has changed considerably over the years, and now covers ten industrial sectors. And in addition to inspecting a wide variety of goods in transit, it tests their quality, safety and performance, verifies that they comply with global standards and local regulations, and certifies them to reassure consumers and other purchasers.

‘Our services were initially based on the physical nature of the products that we inspected,’ says Jean-Luc de Buman, Senior Vice-President of

Corporate Communications, Investor Relations and Corporate Development. ‘That is still part of our work, but we have moved from physical activity to knowledge-based expertise – from blue-collar to white-collar work that covers the entire supply chain from raw materials to final consumption.’

A banker for 20 years, Jean-Luc de Buman joined SGS in August 1998 when it was still mainly focused on inspection, effectively acting as a customs office for countries which had no customs services of their own. It would value export goods at the port of departure so that the importing country could levy the right amount of import duty.

However, he found out within three months that SGS had lost two large contracts – with Indonesia and Pakistan. This resulted in the loss of 90 per cent of its earnings, making the company almost bankrupt. It decided to re-engineer the business. In 2001–02 Baron von Finck, a key shareholder, brought in a new chief executive, Sergio Marchionne, the Italian-Canadian executive who has since become chief executive of Fiat Chrysler.

The central move in reshaping SGS was to move upstream systematically. It kept the import-export trade inspection but started looking at the origins of the goods – seed manufacturers for grain, exploration activities for oil

and minerals, design for consumer products. In doing so, it has created the biggest laboratory network in the world which now employs 90,000 people along the supply chain across the globe.

‘We have effectively moved from physical activity to laboratories, and the next step will be more data-based consultancy. From our laboratories, we have data on almost everything and conceptually we can make use of it by analysing and interpreting it for customers.

‘Many of those customers are well-known listed businesses – we work for people with cross-border interests who are producing here and selling there. We are an agent of globalisation, working closely with clients to ensure their success. They have thousands of suppliers which must be compliant throughout the supply chain with the requirements of governments, NGOs and consumer organisations, as well as our clients’ values.

‘Regulation is at the centre of our activity, and it is changing all the time. We are well-placed to advise on it because we have been in so many countries for so long and our people follow developments country by country and business by business. We also have access to the technical bodies that draft the regulations: they need to draw on our expertise.’

One of Jean-Luc de Buman’s responsibilities is corporate development, in charge of acquisitions for what is a highly complex business. For example, SGS has recently acquired a company which specialises in molecular biology and DNA sequencing services in the food sector. It has invested in an Industry 4.0 startup, developing solutions for transforming food regulatory compliance. And it adopts the latest machine-learning techniques with the support of Swiss Artificial Intelligence Lab IDSIA.

The skills needed by SGS are constantly evolving, and not easily found in Europe. ‘We join forces with universities in Asia, mainly in China, and much of the training is done on the job with targets for each employee of required

‘We are an agent of globalisation, working closely with clients to ensure their success’



days of training – in some cases, months of it. We are also working with academics much more: in China, 80 per cent of our recruits are now graduates. To be a good auditor on our huge range of activities, we need the very highest quality of training.’

The industries that are most sensitive to regulation and inspection are those where safety is a key requirement. ‘We sell trust to consumers who lack trust in products such as food, drink and cars. Our role is to give them confidence in the safety of those products.’

The company is a global firm, which aims to provide services all over the world. ‘We have more growth today in Asia and Africa than in Europe, but our strategic priorities for investment to drive growth are China and North America. Years ago, China was seen as mainly a manufacturer, but today it is also a consumer market. Around half our business there is in domestic activities, in supporting local services for Chinese people.’

Serving large multinational companies involves building deep and diverse relationships with different parts of their business, such as the quality department and the production department. There can be two SGS people waiting to see the customer at the same time, unaware that they are both in the waiting room. ‘It is a team approach, and we try to bundle services as much as we can.

‘But if we find an instance of non-compliance with standards, we have to say so and tell them to stop. Clients expect us to tell the truth, but sometimes it has financial consequences and the client doesn’t want to hear it. It’s non-negotiable, though: if we don’t say it, our business will be dead.’

For the future, Jean-Luc de Buman sees SGS using tech and data for consultancy and prediction, to serve clients better. The company will also have to adapt to digitisation as a different way to deliver the service: inspectors used to

submit written reports, but the group must now report online and as events unfold. The challenge for the company will be to retain the opportunity to explain and interpret the data and its consequences.

‘Even if technology appears to remove the need for independent verification, there is still a role for giving external assurance to the public. Many industries are setting up online platforms which make decisions on procurement of supplies based on information the suppliers provide.

But someone should independently verify the process by which the platform makes the decision.

‘In ten years we will continue to inspect grain and containers, we will continue to inspect cargoes. Sensors and drones may replace the eyes of physical inspectors where they are quicker and more efficient. And the service may move online. But independent verification and certification are still essential.’●





HACKING INTO THE BRAIN TO CHANGE HUMAN BEHAVIOUR

A former hacker has become a neuroscientist whose research into the human brain is revealing how memory works, the meaning of dreams and the role of the subconscious in making decisions and shaping human behaviour

Professor Moran Cerf began his career in the Israeli military intelligence as a professional hacker. After four years in the army, he set up a company to use his skills commercially, working for companies and government organisations to help find vulnerabilities in their computer systems. As is common in Israel, he continued his studies while working, graduating in physics and taking a masters in the philosophy of science.

When his business was acquired by a larger company, he decided to continue with his studies and consulted one of his scientific heroes on the options. The elderly scientist had helped break the German Enigma code before going into science where he was involved in the discovery of DNA. His advice was to move into neuroscience, where the human brain could be seen as a black box like a computer. Today, Professor Moran Cerf is involved in ground-breaking research into the nature of memories and the unconscious part of the brain.

‘He thought that my experience as a professional hacker would be ideally suited for studying the working of the human brain. Successful hacking involved the understanding of the minds of

users of computer systems and I might be able to use my hacking skills to do the same for academic research into the human brain. He wrote a letter of recommendation for me, and within 18 months I was studying for a neuroscience doctorate under one of his former students at Caltech, the California Institute of Technology.’

What he had learnt from his ten years of hacking was the mentality of a hacker, which is working out how your targets think. If you can do this, it helps to identify their mistakes and the weaknesses of the systems they design and operate – whether they are the good guys being attacked or the bad guys doing the attacking. Hackers have to experiment to learn about the black boxes they are trying to break into, using psychological insights into how people think.

‘Today this research on the dark side of people – cheating, lying, misbehaving – is used to help improve our understanding of the mind by testing extreme moments of conflicts within us. An example of how this works was a job that my company once did for a big phone company to test how secure their online systems were.

‘Successful hacking involves understanding the minds of users of computer systems’

‘We knew that it was easier to persuade people to disclose passwords at the end of their working day when they were ready to go home. So I rang the secretary on the security desk late in the day, saying that we were working for the company on a failing antenna and had forgotten the system password. I told her the last five passwords and said

she could check that there was a failing antenna where I said we were, but she still wouldn’t tell us the password.

‘Next morning, she was called by the Chief Security Officer who congratulated her on seeing off a hacker, and got her to tell him the full story for a case study – the details including the right password. In fact, we had

pretended to be the CSO and that is how we got the password on the second day. We knew from our understanding of human psychology that her guard would be down: people’s defences drop with a second attack, something that real hackers will also know.

‘This is not magic – it’s how people think, and now I study what it is in the



brain that makes people behave like that.’ He does so at Northwestern University’s top-ranked Kellogg School of Management in Chicago, where he is Professor of Neuroscience and Business. And his pioneering research over the last 12 years has established a new way of investigating the human brain, by peeking directly inside humans’ brains.

Traditionally, neuroscience has done research on the human brain using imaging tools such as MRI or EEG, along with experiments on animals that plant electrodes in their brains. ‘I work with surgeons who have human brains exposed for clinical purposes. We put electrodes in their brains during surgery to monitor individual brain cells. We will ask the patients questions, show them movies and talk to them about their choices to learn how the brain works.

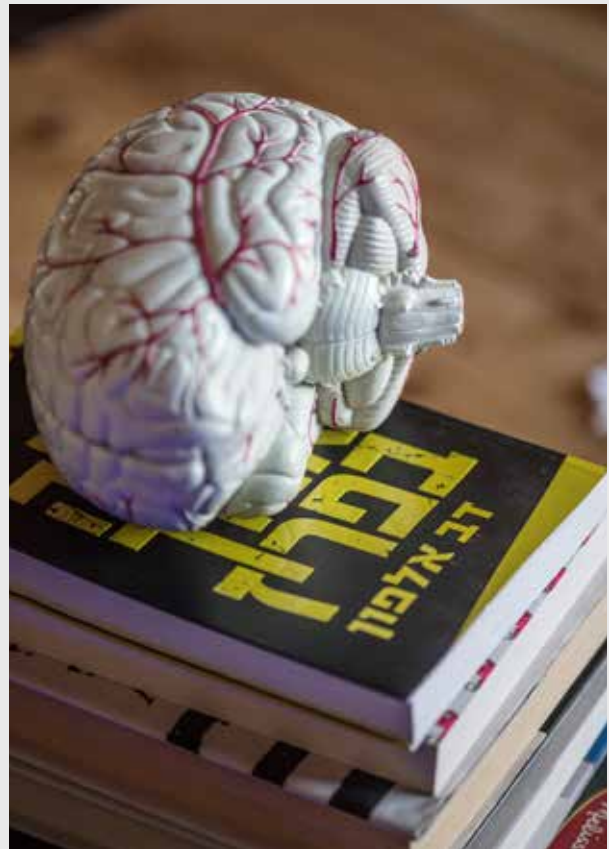
‘Very few people in the world get to study the human brain in this way, and we have carried out a variety of studies which have allowed us to do two things. First, we can find the cells of the brain that allow us to stimulate memories, decode them and see what patients are thinking about and imagining. Second, we can put our electrodes into the unconscious parts of their brains that people cannot access, and we can see how they make decisions before they know what they are.’

‘Last year, for example, we were looking at how patients dream – they forget most them as they wake up. We have found that the residues of dreams retained on waking are very different from what they have seen in their dreams while deeply asleep. We can show the patient images of those dreams and analyse what is happening in dreaming.

Hackers have to experiment to learn about the black boxes they are trying to break into, using psychological insights into how people think

‘Another study a few years ago asked people to play a game which involved pressing a button, in order to see how they decide their moves. By monitoring the unconscious part of the brain, we could see that they had decided what to do seconds before pressing a button. We can even make it possible for a patient to move a screen cursor in a particular direction by thinking about it.’

Professor Moran Cerf describes this approach as a new tool which can change behaviour. ‘People can be helped to stop smoking if we look at their

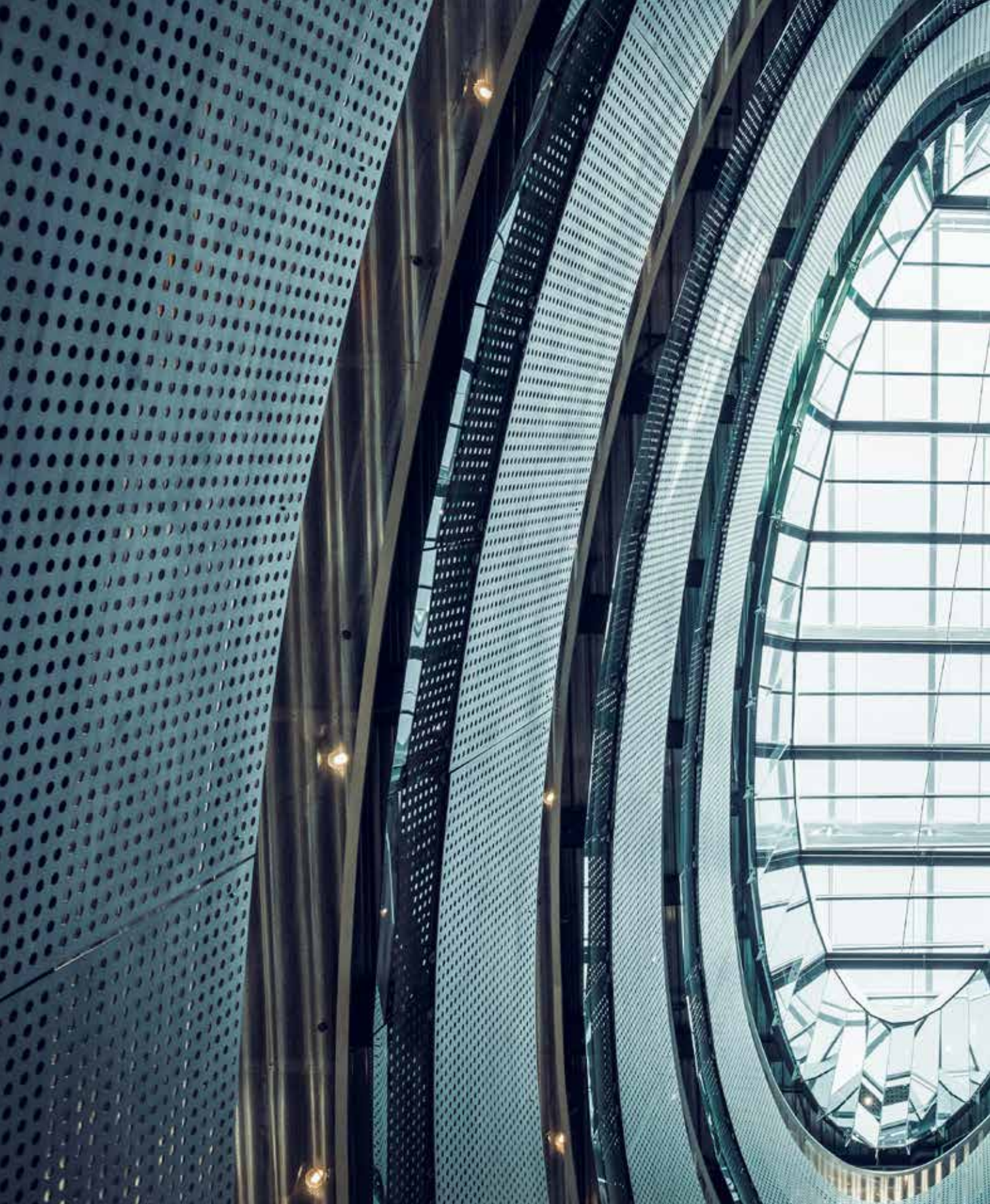


brains when their guard is down – when they are asleep, for example – so that when they wake up, they won’t want to smoke any more. We can also help people understand when is the best time for them to make decisions, by profiling their brains: is it in the morning or the evening; or when they are hungry or full?’

A lot of this is of interest to companies, so he spends a third of each year in the business school trying to pass on the knowledge he has gained from neuroscience to people who have not been patients. This covers how to think better when engaged in business activities such as making decisions, assessing risk and planning marketing campaigns.

He has also been working with the White House to apply his knowledge on behaviour to the implementation of new policies, by understanding biases and helping fix them. And he is Alfred P. Sloan Professor at the American Film Institute, teaching an annual screenwriting class in Hollywood on science in films, helping TV studios to make science more accessible.

‘My three aims as a neuroscientist are to learn more about how the brain works, to apply our findings beyond neuroscience to human behaviour, and to help people understand the consequences of our work.’ ●







A FOOLPROOF METHOD OF PRESERVING DATA SECURITY

In the battle to protect the security of digital information, a Swiss company has used quantum mechanics to develop a new form of cryptography which makes decoding data impossible – even as computers become much faster

The increasing processing power of computers is making it easier for hackers to decipher encrypted information by finding the keys at the heart of traditional coding techniques. That task will become much easier when quantum computers arrive, hugely accelerating processing speeds and making it possible to break codes very quickly.

However, the quantum mechanics science behind the new generation of super-fast computers has already generated a new form of cryptography which is impossible to decode – not least because any attempt to intercept changes the data. A leader in the field is ID Quantique, a company created in 2001 by four scientists at the University of Geneva who had identified the potential of quantum cryptography to revolutionise data security.

‘Quantum encryption technology has been around for a while,’ says Grégoire Ribordy, a physicist who was one of the founders and became the company’s chief executive in 2001. ‘But all the big IT groups have begun to enter the quantum computing field in the last two years. And the US National Security Agency (NSA) announced in 2015 that it was planning to upgrade its cryptography techniques to make them quantum safe.

‘We may have been early into the field, but people now understand the challenge. Quantum computing is no longer science any more, but engineering – it’s not a question of if, but when. So quantum encryption has become a priority for protecting the security of data when today’s conventional coding techniques become too vulnerable.’

The development of quantum mechanics came in the first 30 years of the 20th century when physicists found discrepancies between the results of their experiments and the then theory. Quantum mechanics described a new way of looking at the world of atoms, particles and other very small things. It was initially purely theoretical, but gradually led to the first quantum revolution with the development of lasers, microchips and other new technologies.

This first wave did not use the full potential of quantum physics, says Dr Ribordy. But a second quantum revolution has begun as it has become possible to use much smaller devices and control individual elements. And the emergence of quantum computing is one consequence of that, because it will be able to process the calculations needed to break cryptographic codes so fast that traditional encryption techniques will be ineffective.

‘Quantum encryption has become a priority for protecting the security of data when today’s conventional coding techniques become too vulnerable’



‘The idea of quantum cryptography is not to use quantum physics to create a problem, but to solve this problem by improving the security of communications.’

Even before quantum computing has developed, far-sighted organisations are already using quantum-safe cryptography techniques to provide long-term security of their data. An adversary can record information encrypted using traditional codes today and decrypt it in the future when quantum computing becomes available. Using quantum cryptography now protects critical data such as client portfolios, as well as information about clients and the employees of the organisation.

A more common use today of ID Quantique’s quantum-safe techniques is to secure communications between data centres – between head office computers and back-up facilities, for example. An attraction for users is that the information cannot be decrypted when quantum computers arrive, because of the Heisenberg Uncertainty Principle. This central tenet of quantum mechanics, says that if you try to read and measure a quantum object such as a photon that carries the encryption key, you change its state.

Kelly Richdale, a seasoned entrepreneurial executive brought in to help transform ID Quantique into a more commercially minded organisation, sees this as a strong selling point. ‘If someone tries to intercept information sent over optical fibres – for example between two data centres – it creates physical proof of the attempt. It is an anti-eavesdropping mechanism, as well as giving protection in the future world of quantum computing.’

The company has other products using quantum mechanics principles, such as the Quantis, a small random number generator, which harnesses the random nature of the universe to generate encryption keys for security products. It is also used in the online gaming industry, which is highly regulated and needs to be able to demonstrate that its games use genuinely random numbers.

**‘In times of uncertainty people
buy Swiss francs, and they also buy
Swiss encryption devices’**



An attraction of ID Quantique’s security encryption products for potential customers is that it is a Swiss company. ‘One of our logos is Swiss Quantum,’ says Kelly Richdale. ‘The most famous examples of security breaches were those highlighted by the whistle-blower Edward Snowden, who revealed the surveillance of digital communications by governments and their insistence that manufacturers install back doors in devices to give them access to transmissions of encrypted data.’

‘Switzerland doesn’t have that kind of strong government pressure – indeed, we have data protection and privacy as fundamental rights. When countries such as the US force disclosure through back doors, it hugely undermines trust in their products. It’s a bit like the flight to the Swiss franc: in times of uncertainty people buy Swiss francs, and they also buy Swiss encryption devices.’

Dr Ribordy says he hopes to broaden the company’s range of products, to position it as the leader in quantum-safe long-term security. These include new solutions for email encryption and storage encryption, where he expects demand to grow as the arrival of quantum computers approaches.

‘We are looking for partners to bring our quantum products into completely different markets, such as smartphones. You could just take a picture on your smartphone which would generate high quality random numbers for codes and encryption keys for security purposes.’

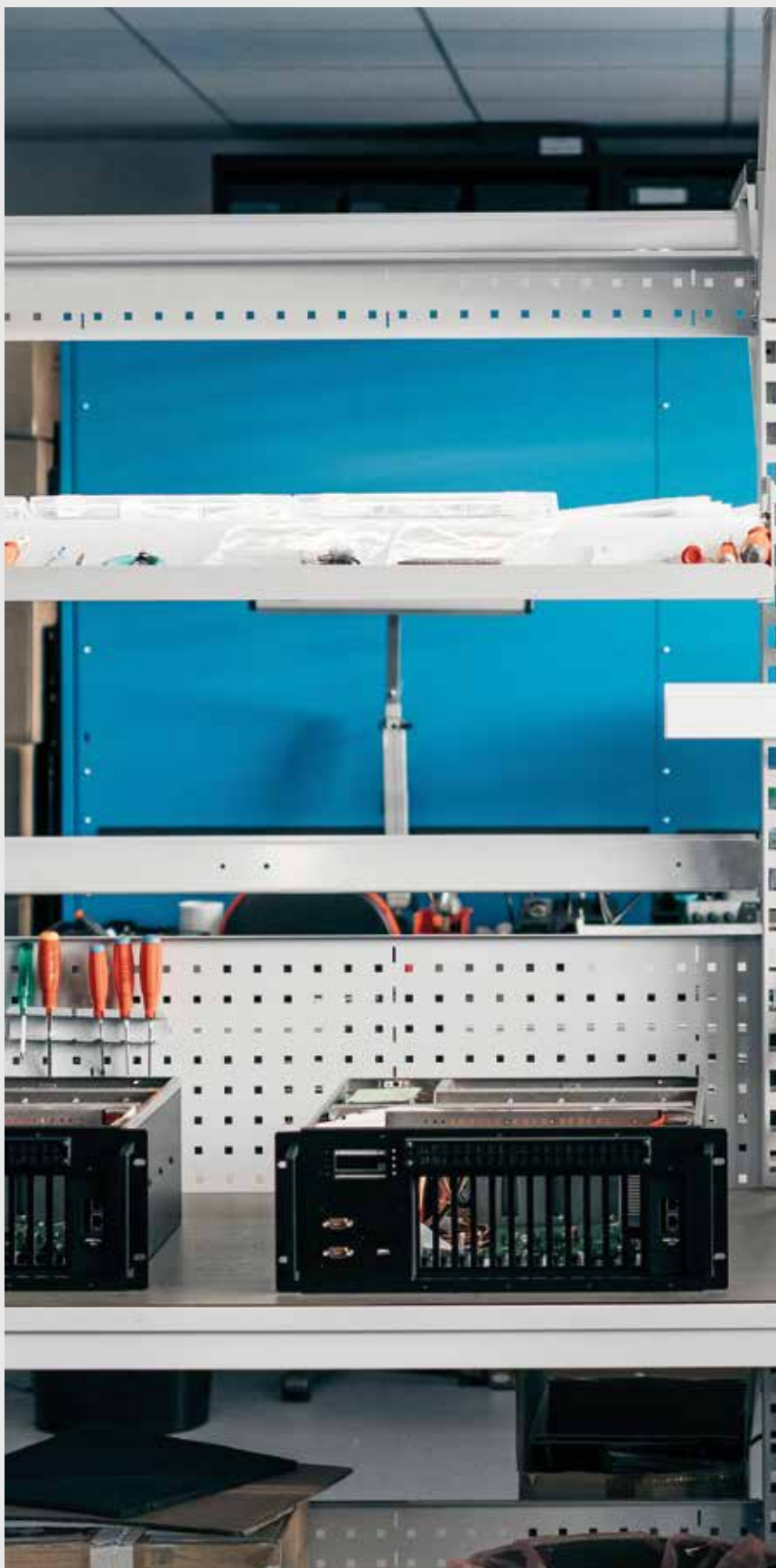
The company has started to grow fast, doubling its staff to 50 in the last year. One factor that is increasing demand is the new focus on cyber attacks. Traditionally it has been on data theft, and that is expected to continue. But increasingly cyber attacks are being used for political purposes, such as influencing elections or attacking critical infrastructure.

‘If you look at what happened in Ukraine, the Russians hacked into the electricity grid,’ says Kelly Richdale. ‘They took out part of it and the only thing that saved the Ukrainians was the age of their grid and its poor connectivity which stopped the whole network from being brought down.’

**The beauty of
quantum-safe encryption
is that it has guaranteed
forward security built in**

‘The first such attack came in Estonia, which has now become a leader in developing cyber defences. And Switzerland is a good example of how organisations can work together to defend their critical infrastructure, which includes the banks as well as the electricity industry, the water grid and other networks. There is a very strong coordinated response if there’s an attack on a Swiss infrastructure company, but there are countries where cyber defence is not so well coordinated.’

And the beauty of quantum-safe encryption is that it has guaranteed forward security built in, says Grégoire Ribordy. ‘It’s based on the laws of physics and they can’t be changed. Quantum cryptography has the potential to end the race between code-makers and code-breakers. We can improve the performance of our system, reduce its cost and maybe its size, and move into new application areas. But the security of quantum cryptography will not change – and that’s what makes the technology interesting.’ ●





PROTECTION FOR CRITICAL INFRASTRUCTURE

Increasing concerns about potential cyber attacks on satellites, energy installations and defence systems call for more creative threat responses, according to an expert in international security at a leading UK think-tank



The enormous growth in the processing power of computers has put great connectivity in the hands of users, but it has also offered great opportunities for cybercriminals to exploit their vulnerabilities. This has raised concerns over the privacy of digital communications and the security of personal data held on computers.

But a relatively new set of concerns is developing over the increasingly apparent links between cyber security and physical security in fields such as defence, the space industry and critical infrastructure. Dr Patricia Lewis, a research director at an independent think-tank based in London, has called for a radical review of cyber security in space to avoid potentially catastrophic attacks.

‘We’re looking at the moment into the cyber security of missiles and defensive systems, so many of which are now connected to the internet at some point. And we are reliant on space in our societies to a degree that many people are unaware of, but in ways that are essential to everyday life. The creation of a cyber-security regime is urgently required to develop effective threat responses.’

Dr Lewis works at the UK’s Royal Institute of International Affairs – commonly known as Chatham House – whose mission is to help build a sustainably secure, prosperous and just world. A nuclear physicist by training, she is Research Director, International Security for the organisation, with responsibilities that cover all aspects of protecting humans so that they can live safe lives to the full.

Her responsibilities fall into three areas: traditional defence and security issues; societal aspects of security; and the scientific and technological aspects of security including artificial intelligence and robotics in conflict; and the scientific and technological aspects of security. The latter includes cyber security, where the challenges have grown fast since the early days of modern computers, creating opportunities for criminal activity of increasing complexity and danger to society.

‘We know, for example, that criminals have been hacking into satellites; and we know they’ve been hacking into energy installations, including nuclear installations. This raises worries about threats to the critical infrastructure that supports utilities such as electricity, water, transport and communications. And there are similar worries about data protection – the vulnerability to attack of the large amounts of information stored on computers.’

‘When it comes to space, satellites play a variety of roles including providing signals for television and telecommunications around the world. Ships and aircraft depend on satellite global positioning and timing data for their navigation. And such data also plays a vital role in financial transactions which could be manipulated to carry out large thefts.’

‘The airline industry is one of the few that has been really out ahead in terms of cyber security because of worries about aircraft crashes. They have to always transmit and receive signals wherever they are, so they’ve been introducing authenticity checks of those the signals as part of their normal practice. Other industries need to increase the authentication of their digital information – its provenance and activity.’

‘This needs to be replicated in the many different sectors of critical infrastructure on which we rely – including energy, transport, food production, sanitation and banking. These are part of how we live now, but we take them for granted.’

The human-cyber interface is also important, she adds. ‘Human judgment plays a vital role in these systems, and whether artificial intelligence can replace it is hard to know. But human decision-making can be a vulnerability when there are insider threats that lead to people deliberately doing things wrong, which certainly happens. And there are people who use the technology but don’t understand it – another very big risk.’

‘We are reliant on space in our societies to a degree that many people are unaware of, but in ways that are essential to everyday life’

Cyber threats have become a global problem, she says. And it is not just a government problem; it is also a non-state actor problem. Governments have more resources at their disposal and therefore have greater capabilities, such as having more people able to break into systems. But non-state groups can sometimes spot a vulnerability that someone else hasn't spotted. Individuals and teenage kids have done unexpected things with cyber attacks – it is not impossible for a non-state group to make quite a major gain in that respect.

All governments are involved in cyber threats, she admits – partly as a defensive measure, partly to understand what cyber attacks can do. So if they are looking at bio-terrorism for example, they have to make those pathogens to understand their impact and to work out how they can defend their countries against them. It is the same with cyber viruses: they have to make them to see what they can do.

'The best-known cyber attack on critical infrastructure was the Stuxnet worm attack on the centrifuges used by Iran to enrich uranium for nuclear fuel. This was, from all reports, a collaboration between three western powers, Israel and the United States, with some assistance from Germany. I'm sure that some other countries were involved, as well as a major corporation. It allowed them to show what they were capable of.'

At the moment, we are often protected by what Dr Lewis calls 'the wisdom of engineers'. They design things with the assumption that they will go wrong, building in resilience, backup systems and some redundancy.



Cyberattacks will keep on coming and going. We need resilience in the system so that when they occur it won't matter

So when there are cyber attacks, the resiliency of their systems means there is not always the major impact expected.

She says that this should lead us not to worry so much about cyber-attacks. 'They will keep on coming and we will keep on trying to defend against them, but some will get through. The priority should be to make sure that we have the resilience in the system so that when they occur it won't matter.'

'A good example of this approach is the handling bio-terrorist threats. The one thing you can do to prevent the use of a particular pathogen is to vaccinate your population against it. The bio-terrorist can deploy the threat but if it doesn't affect people it is pointless. We need to think more like that with cyber security – if there's no impact, there's no payback for cyber terrorists.'

'From other security work, we know that countering a threat with the same threat is not helpful. It just becomes an arms race: you do one thing, they do the same thing back and it carries on without end.'

'We need to be smarter and more creative. If they do one thing, counter it in a completely different way that they don't expect, so they can't achieve their aim.'

She also says that talk about cyber wars is unhelpful: as with every tool of warfare, cyber will be a component of all attack and defence practices. 'People get very excited about cyber attacks and devise theories about hybrid warfare and the like. But the truth is that warfare is always mixed. It's not a football match with rules – it is war.'

'We have always attacked energy systems and communications networks. If we panic and feel powerless to do anything about cyber, we'll end up paralysed. If we think about cyber as just another tool, we can deal with it.'

'It's human behaviour. There's nothing new under the sun, unfortunately. We are primates. This is what we do.' ●









Bounties for bug-hunters make the internet safer

HackerOne's network of more than 100,000 ethical hackers can help online organisations eradicate vulnerabilities in their internet systems that could be exploited by criminals, says Mårten Mickos, its Chief Executive Officer

Barely a month goes by without reports of large companies and government bodies suffering cyber-attacks by criminal hackers and other hostile organisations. A USD92 billion cyber-security industry has grown up which tries to fend off such attacks by building walls and gates. But such strategies are easily outpaced by hackers – frequently proving inadequate and undermining the confidence of online users.

However, a California-based company has developed a revolutionary new approach that invites ethical hackers to detect vulnerabilities in the computer systems of its clients. HackerOne, founded in 2012, has already attracted more than 1,000 companies, including well-known dotcom businesses such as Twitter, Yahoo!, AirBnB and Uber. Its bug-hunters, who now number more than 100,000, are paid bounties for their successes – and more than 4,000 have already shared USD14 million for finding over 28,000 vulnerabilities.

When Mårten Mickos was approached to become HackerOne's CEO in 2015, he was at first sceptical of joining: he saw the cyber-security industry as rather cynical and negative. But when

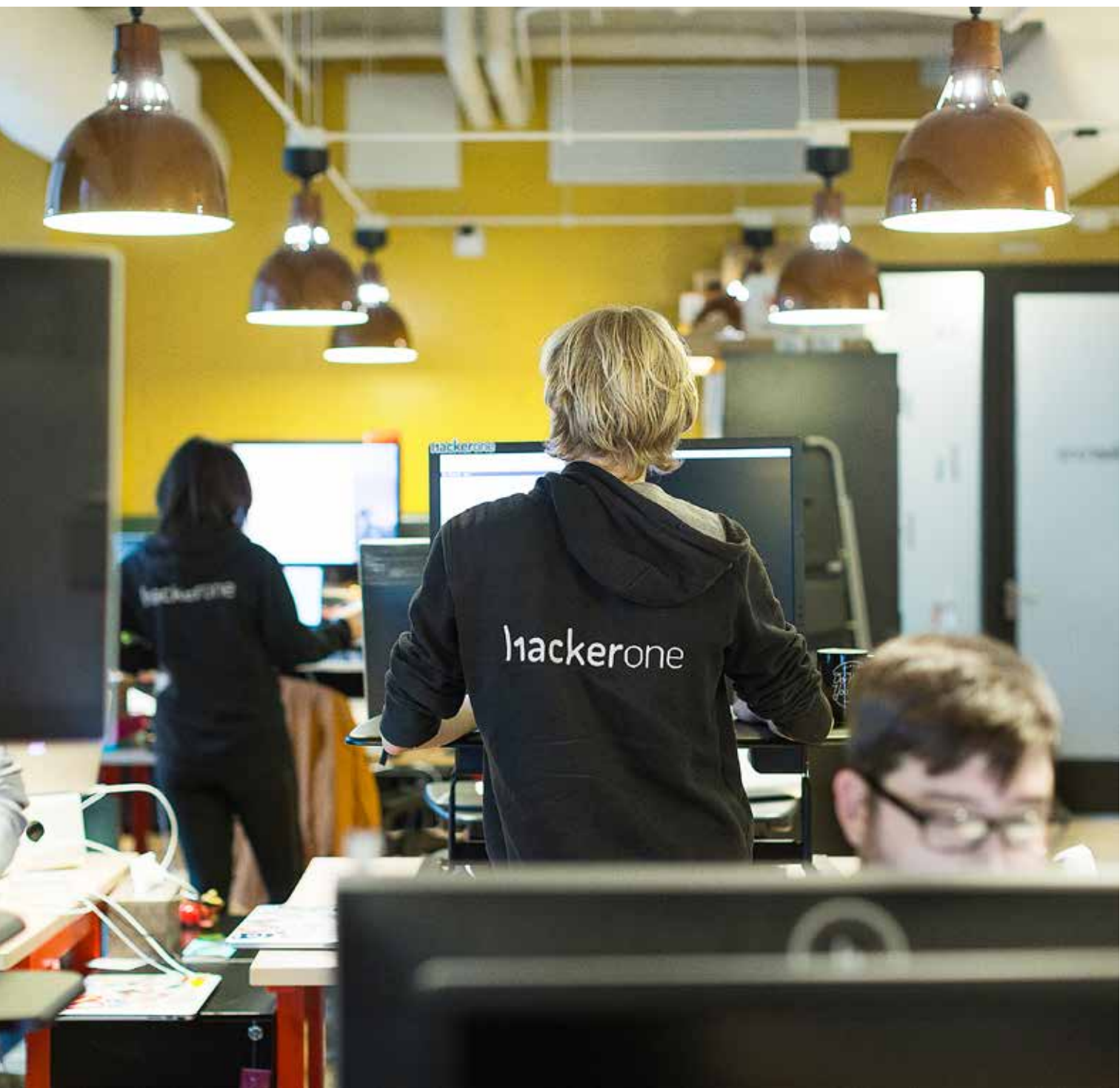
he met the founders, he found it to be a positive and constructive company which offered an enormous opportunity to build a society that could function safely and securely online.

'We're trying to turn security inside out, based on a principle which has existed for a long time,' he says. 'We're asking people to help by looking in, rather than building barriers to keep them out. It's like Neighbourhood Watch schemes which encourage people to keep an eye on their neighbours' homes when they're on holiday, to stop them being burgled.

'We are a trading platform that brings together responsible 'white-hat' hackers with responsible companies in order to make the connected world more secure. Our hackers are independent operators who are paid by our clients for the vulnerabilities they discover. We encourage clients to share on our website what our hackers have found so that others learn from their experience – which around 10 per cent do.

'We have more hacking experts than any other company in the sector and they are diverse in their backgrounds – young and old, men and women, technical and non-technical people. This makes us

‘We’re asking people to help by looking in, rather
than building barriers to keep them out’



better at finding vulnerabilities than the limited number of in-house experts working for client companies. And it is hard for humans to find flaws in the systems they have built; creative outsiders are more likely to find the “unknown unknowns” – vulnerabilities that no-one else has spotted.’

HackerOne’s typical hacker is a young man under 34 with expertise in computer sciences, for whom detecting online flaws is a hobby at college or a spare-time job. They have a cunning ability to think bad like a criminal hacker, says Mårten Mickos, but then do good by reporting the vulnerabilities to the owner of the system – the potential victim. They find chasing vulnerabilities thrilling and they can make a lot of money if they’re good – one of HackerOne’s bug-hunters made over half a million dollars on the HackerOne platform alone.

‘I see us as a bit like the Boy Scouts, whose founder created the organisation as a way of giving idle young people something to do and contributing to society. Often our hackers are super-intelligent teenagers who don’t know how to communicate with people and may be difficult to deal with. We reach out to them, giving them a meaningful role in society and bringing out the best in them – otherwise they might get up to all sorts of mischief.’

HackerOne’s approach has proved attractive to a wide variety of companies. Those which have grown up in online businesses such as Uber and AirBnB know that constantly detecting vulnerabilities is vital to their success. Older companies which have experienced their first security breach, perhaps by a criminal, quickly turn to us because they cannot afford the cost of another breach. A third group of clients comes by recommendation, often from big manufacturing companies which tell their suppliers to protect themselves against hacking so as to make the supply chain secure.

In 2016, HackerOne helped the US Department of Defense to make its systems more secure by launching the ‘Hack the Pentagon’ challenge.

**‘We have more hacking experts
than any other company in
the sector and they are diverse
in their backgrounds’**



This eight-week programme involved 1,410 hackers who found 138 vulnerabilities – the first within 13 minutes. It paid out USD75,000 of bounties to the hackers, ranging from about USD100 to USD15,000.

‘It was a huge shock for the Pentagon to find so many flaws, having previously paid millions of dollars on security protection. So they asked us to repeat the programme for the US Army with Hack the Army, and again found very serious vulnerabilities – the first within five minutes. The Department of Defense is one of the best financed organisations in the world which can pay for anything it needs, but it found it effective to turn to hackers for help!’

Big online operators often pay for continuing surveillance, while others prefer sporadic scrutiny when they launch new software. But monitoring needs to be continuous, says Mårten Mickos. ‘You can’t know when malicious hackers will find a flaw, as systems are under attack all the time from criminals, hacktivists, nation states and terrorists.’

The most common bugs are considered ‘low-hanging fruit’, he adds. Cross-site scripting (XSS) vulnerability allows hackers to get access to content on another website, for example. The most severe attacks include attackers putting software code on a system which can stop it operating or steal its data. ‘Every day, we spot new vulnerabilities which our customers must get their engineers to fix.’

Particularly vulnerable are users of old software which may have been designed before anybody thought about cyber-security, and those whose security practices have not been kept up-to-date. Organisations that do not pay attention to cyber-security in their operations are also vulnerable, and need to change their cultures. The best online companies put security at the heart of their organisations, treating it as an integral part of the corporate life-cycle.

The growing threat posed by serious hacking leads to worries that the internet is too open, and that users will move into more closed forms of online communication. But Mårten Mickos says that vulnerabilities can be greatly reduced – as happened with previous technological innovations which experienced safety issues in their early days.

‘There is no 100 per cent safety in cyber-security’

‘When cars were first made, manufacturers didn’t think about security and people died all the time in accidents. When the auto industry decided to make security a priority, it started to build safety into every car. People still die in traffic, not because cars are unsafe but mostly because of their owners’ driving practices. The same will happen with software, an industry that is only 30 years old. More companies will design security into their products and create a society where software is truly secure.

‘There is no 100 per cent safety in cyber-security but we can get closer to it – just as happens with infectious diseases which have been reduced by vaccinations and better hygiene. There will remain parts of the world where cyber-security is inferior to best practice, but in advanced societies the internet will become much more secure over time.’●

How Mårten Mickos protects his own security online

- Change passwords frequently and make them cryptic
 - Back up data at all times
 - Treat every communication as being from a potential attacker – even if apparently from a friend or colleague, it could be a phishing attack searching for a vulnerability in your security defences
 - Don’t respond to cold calls by telephone unless there is independent and reliable proof of the caller’s identity
 - Don’t allow strangers to use your phone or tablet, however good the reason
 - Make security a habit, not a burden – and don’t stop enjoying your connected life
-





- Inbox: * Sort by severity

* custom view?
(default views)

- Filter by severity

- Severity on Dashboard

- Integrations

* slack

* report escalation

Impact Requirement

- Bounty Recommendation
to use severity data.

- Severity on Hacker Profile

- badges "Big Game Hunter"
5 critical resolved

severity combined w/ CVE

severity into hacktivity weights

structured scope

vulnerability taxonomy

Spiced Apple Cider
Gato



THE EVOLVING THREAT FROM CYBER TERRORISTS

Terrorist organisations intent on destroying their enemies are using increasingly sophisticated cyber attacks to damage critical infrastructure and kill large numbers of people, according to a former Israeli security chief

Governments and large organisations trying to protect themselves from large-scale cyber attacks face two primary challenges in the modern era, according to Doron Bergerbest-Eilon, the former Head of the Protection and Security Division of the Israel Security Agency and Israel's most senior ranking security official.

The first is the constantly evolving nature of the terrorist threat. In the past, terrorists were primarily motivated politically, by the aim of ousting governments and installing new regimes. They were not looking to inflict mass damage or casualties which might have eliminated the possibility of negotiation. However, the upsurge of terrorist organisations like al Qaeda and ISIS which have set their sights on the complete destruction of their opponents has dispelled this constraint.

‘The objective of Mohamed Lahouaiej-Bouhlel, the perpetrator of the lorry attack in Nice on Bastille Day in July 2016, was to cause as many casualties as possible. A total of 86 people were killed in that attack and hundreds of others were injured.

‘And in September 2001, we know that al Qaeda sought to inflict as many casualties as possible when they carried out multiple attacks on US targets. The two World Trade Center towers at 110 storeys each could accommodate up to 50,000 workers and an additional 200,000

visitors daily, an extraordinarily large number of potential casualties to target.’

The second challenge is the evolution of cyber warfare itself. When it started in the 1980s, the aim of the Soviets was to steal software and information from the US. To combat the threat, the US planted malware to disrupt its use.

‘Today, cyber warfare is increasingly aimed at damaging a country’s or company’s critical infrastructure, and in some cases to cause mass casualties. For example, cyber attacks can cause massive damage, loss of life and widespread confusion and panic by shutting down cellular services, switching off power plants or water treatment plants, corrupting ATMs, rerouting train lines or switching off traffic lights – just to name a few.

‘In fact, many reports today go so far as to indicate the likelihood that future wars may be predicated upon cyber attacks involving communications, energy or financial services.’

During Doron Bergerbest-Eilon’s distinguished career with the ISA, he held a number of senior positions, including responsibilities over securing Israel’s air, land and sea borders. In addition, he was in charge of the protection of national classified information and national critical infrastructure. He founded the National Cyber Authority for the Protection of Israel’s Critical Infrastructure, the first agency of its kind in

the world, and was actively involved in developing a national strategy for information security and critical infrastructure against cyber threats.

After retiring from public service in 2005, he founded ASERO Worldwide, which offers a wide range of consultancy services for private and public sector clients on relevant homeland security topics. These include preparing for, mitigating and recovering from terrorist threats, and critical infrastructure protection with an emphasis on cyber threats. ASERO lists among its prestigious clients government agencies in the US, Canada and Singapore as well as private companies such as Mars Incorporated, the AES Corporation and Delta Air Lines.

He says that the key principles for securing any infrastructure or facility can be broken down into three interconnected sectors: physical security, cyber and IT security, and emergency and recovery preparedness. 'Security often fails when we focus our efforts or our resources too strongly on one principle while neglecting the others.

'For example, we estimate that 60 per cent of cyber attacks are caused by 'insiders' such as disgruntled current or former employees. If we secure computer systems only, we neglect to vet employees properly, install and safeguard passwords, or secure server rooms to prevent unauthorised access. In addition, non-cyber threats such as the air conditioning inside a server room can be manipulated to corrupt or disrupt data services.

'It is also necessary to understand the specific needs of a client and the threats they are facing – defining the threat criteria. To do that, we have to look first at who and what we are trying to protect against, such as an attack by a country, specific organisation or individual, and their capabilities and likelihood to carry out different types of threats.'

It is increasingly difficult to prevent or deter cyber threats, says Doron Bergerbest-Eilon. Unlike conventional warfare or terrorism in which the enemy or attacker can be seen, it is often difficult to identify the source of cyber attacks, making it difficult to retaliate.

When the need for cyber security first emerged, security practitioners attempted to mirror best practices from

Security challenges fall into three broad groups: physical security, cyber and IT security, and emergency and recovery

the physical domain by isolating and safeguarding critical data and information infrastructure. But with up to 60 per cent of attacks coming from within, attempts to isolate infrastructure from outside enemies are futile – while infrastructure relies on communication with other systems for efficiency and maintenance.

'So security practitioners responded in the same way as people attempting to thwart attacks since the Middle Ages have, by constructing walls – firewalls for the cyber domain. However, we have learned throughout history that an adversary will find a way to circumvent security measures, including bypassing firewalls.

'Antivirus software was then introduced and widely installed. Yet this did not provide the level of security originally envisioned, as an adversary could develop new viruses capable of evading anti-virus software.'

It is clear, he says, that attempts to defend against cyber threats have largely failed, as new ways are continually found to circumvent measures or attack infrastructure. Since focusing on defence will always fail against a determined adversary, a new cyber protection paradigm is needed.

For critical infrastructure, that is provided by industrial control systems (ICS) which have evolved to become some of the most sophisticated technologies available. If ICS can protect against all known scenarios, there should be no real threat from nations, hostile groups or individuals to critical infrastructure managed by those systems.

'For example, driving a car without coolant could eventually destroy the engine. But if the car is managed by a control mechanism, a warning that the car is overheating should appear on the dashboard indicating that you should refill the coolant. Even if you ignore the dashboard warning, more modern cars will take measures automatically to prevent you from destroying the engine.

'The same principle may be applied to critical infrastructure. If a threat is detected, the ICS has the capability to alert relevant channels to take appropriate countermeasures. However, this measure is only successful if the ICS accurately understands the threat and not been fooled into believing that there is no actual threat.'



For example, Stuxnet, a malicious computer worm, was used in 2010 to target the industrial computer systems of Iran's nuclear programme. It is likely that this worm had the capability to deceive industrial control systems and malware detection, making it virtually undetectable. While this capability was once in the hands of cyber superpowers only, today it is probably in the hands of hostile countries, entities and other radicals looking to carry out large-scale infrastructure attacks.

Doron Bergerbest-Eilon argues that not only have adversaries proved their ability to consistently

breach cyber defences but that they may also be able to circumvent the most advanced technologies, specifically industrial control systems. This could allow them to destroy infrastructure and cause mass casualties, with serious economic consequences.

His new paradigm would therefore always assume that malware is already inside a system and take steps to protect the integrity of information fed into the ICS – in order to prevent deception that could stop the system from providing optimal cyber protection.●



HOW WORLD WAR TWO CODE-BREAKING LAID THE FOUNDATIONS FOR TODAY'S CYBER WARFARE

British code-breakers gave the UK and US a vital advantage in the second world war by deciphering the enemy's secret communications with techniques that were the precursors of modern computer technologies



Bletchley, an unremarkable town north of London, was known until the 1970s mainly as a railway junction. But a book published in 1974 revealed that it had played an essential role in the second world war by intercepting and decoding secret communications between Berlin and the commanders of Germany's armed forces.

Slowly the full story began to emerge. At the start of the war, the British Government's Code and Cipher School had relocated from London to Bletchley Park, a mansion on a 21-hectare estate beside the town's railway station. There it devised code-breaking techniques that gave the allies an immense advantage in the war against Germany, supporting operations on land, at sea and in the air – especially on D-Day.

But the impact of Bletchley Park reached much further. By industrialising the code-breaking process and creating the world's first electronic computer, it heralded the birth of the information age. After the war, its alumni were involved in developing the earliest true computers through laboratory research at universities such as Manchester.

'The machines built at Bletchley Park were precursors of the computer, rather than computers themselves,' says Dr David Kenyon, the organisation's Research Historian. 'But I like to describe Bletchley Park as a computer system, in which some parts were done electro-mechanically and some by humans, in a process that took data in at one end and disgorged information at the other end.'

'The people on the site were mimicking some of the components of modern computers, such as data processing, data storage and communications. Data was stored on card indexes, for example, for search and analysis using machines.'

'It was not a static organisation – its technology and processes evolved at a tremendous rate. Staff numbers at Bletchley Park rose from 180 in September 1939 to almost 9,000 in January 1945. At its peak, the punch-card operators were getting through two million cards each week, searching them for repeated patterns in intercepted communications that could help decode them and link them to other messages.'

British code-breaking had effectively got going systematically in first world war, with at least one major success in the decoding of the Zimmermann telegram in January 1917. This secret diplomatic communication sent to Mexico by the German Foreign Office proposed a military alliance if the US entered the war against Germany. The proposal enraged US public opinion and generated support for entering the war in April 1917.

After the war, British code-breaking was passed to MI6, the Secret Intelligence Service, with a staff of around 70 who intercepted telegrams sent by the Bolsheviks and some other countries. They extended their activities to the Italians in the 1930s after the rise of Mussolini, and to Germany later in the decade after Hitler came to power.

Most of the early cipher systems were pen and paper based, but electro-mechanical systems began to appear after the first world war. German engineer Arthur Scherbius invented the Enigma machine which used a keyboard with several rotors to encrypt messages. The rotors continuously changed the code by rotating after each keystroke, and if the receiving machine was configured in the same way, it could decipher the message.

Scherbius hoped to sell it to banks and companies to keep telegrams confidential, but it was not a commercial success. However, the German armed forces adopted Enigma for military use in the 1930s, which prompted other countries to develop decoding capabilities. One which was successful in cracking the Enigma code was Poland, which feared a German invasion.

Assuming that a war would lead to bombing attacks on London, MI6 looked for somewhere to evacuate the Government Code and Cipher School and bought Bletchley Park, 80 kilometres north of the capital. When the war began, its staff moved there, along with people previously identified as promising code-breakers – mainly male British citizens with degrees from Oxford and Cambridge in subjects such as languages, mathematics and engineering. Later in the war after women were conscripted, many arrived at Bletchley Park and eventually made up 75 per cent of the staff.

By industrialising the code-breaking process, Bletchley Park heralded the birth of the information age



‘There were 150 million million million possible key settings’

The School had acquired an Enigma machine in 1926, and had also been sent information on how to decode its messages from the Poles shortly before the war began. Meanwhile Alan Turing, a brilliant Cambridge mathematician who had already devised a ‘universal computing machine’, moved to Bletchley Park where he quickly invented the electro-mechanical Bombe machine which could help break Enigma much faster than its Polish equivalent.

‘If the Enigma machine had been used correctly, its codes should have been virtually unbreakable,’ says Dr Kenyon. ‘There were 150 million million million possible key settings on the German machine. A brute force attack trying every combination would take an impossibly long time, even with a modern supercomputer.’

‘But British decoders identified weaknesses that came from the interaction between humans and the machine, developing methods still used today with cyber security. One was the requirement for code books so that both sender and receiver used the same settings – these could be stolen or captured. Another was the need to create additional settings to strengthen security, generated at random for each message. These could often be identified, since humans find it hard to be random (which is why they often cannot devise secure passwords).

‘Turing’s Bombe machine also exploited cribbing, widely used to decode older cipher systems. If you can guess the content of an encoded message, you can extract the message key and read other messages with it. Germans often used similar text in messages such as the weather forecast, which could provide the key for that network on that day.’

The Bombe was not a computer, but a single function machine which used telephone exchange technology. So was Colossus, a semi-programmable electronic machine devised by a Post Office engineer to speed up cryptanalysis. By that time, 7,000 messages were coming in daily from intercept stations, and the emphasis was on decoding them quickly for indexing and analysis to find patterns.

When the US entered the war, close cooperation developed with the UK over code-breaking, which continued until the D-Day invasion of Normandy. A special Western Front Committee was created to collect information for the invasion, which was so successful that it had the complete order of battle for the German forces in France by 1944.

When the war ended, most of the staff were discharged from the armed services, instructed under the terms of the Official Secrets Act to

keep what they had done confidential. The Colossus machines and many documents were destroyed, to maintain secrecy about work that became important during the Cold War, which was why it took so long for Bletchley Park's role to emerge.

The Code and Cipher School continued as GCHQ, the UK Government Communications Headquarters which is now based in Cheltenham. It still works closely with the US National Security Agency on signals intelligence, monitoring communications which have grown enormously in volume and complexity. The methods used to identify transmitters and U-boats during the war can now do the same for mobile telephone SIM cards.

Bletchley Park had several uses after 1946, but was scheduled for housing development until a trust leased it

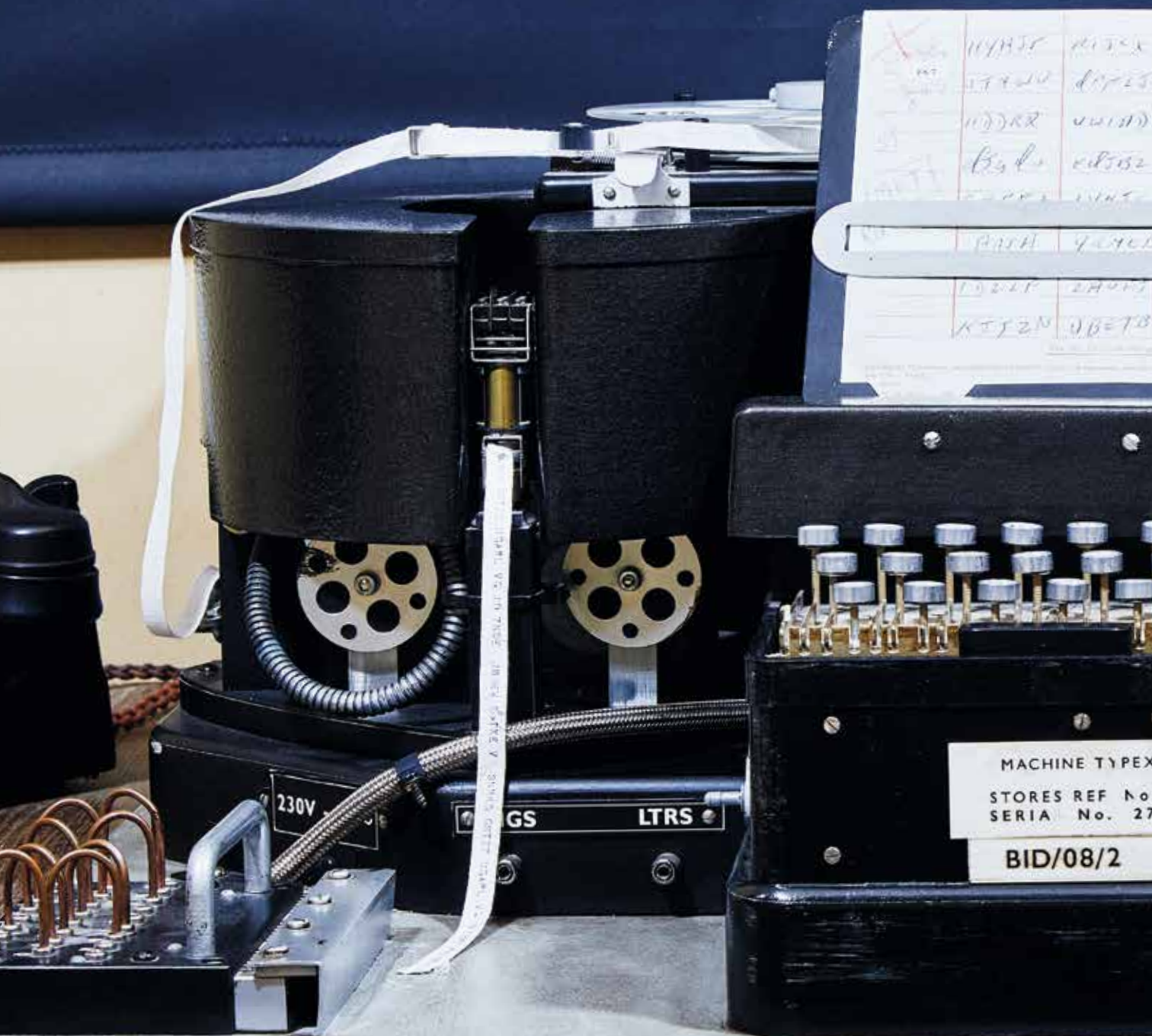
to preserve its heritage. It has now been restored as a visitor attraction which attracts 250,000 visitors each year.

'What Bletchley Park achieved is hard to quantify,' says Dr Kenyon, 'but the impact on the second world war was significant. It helped win the Battle of the Atlantic by tracking down U-boats, and that made it possible for the Americans to get their weapons to the UK for D-Day. And the intelligence advantage it gave the allies for D-Day was immense, probably shortening the war.

'For the legacy afterwards, a lot of things were done here for the first time, but the secrecy meant that they had to be rediscovered in the 1970s. However, when people are looking back now at how IT works, how information is managed and how companies operate, it is clear that Bletchley Park was at the forefront of these developments.' ●

At the time already
Bletchley Park
was at the forefront of
how IT works today,
how information is
managed and how
companies operate







One of the first Typex machine created in 1937, a British cipher machine



The power of film to expose human rights abuses

Israeli entrepreneur Oren Yakobovich has created Videre est Credere, a human rights organisation which helps communities to film and document the violence and corruption they experience, and distributes the material to create change

From his childhood, Oren Yakobovich had always wanted to join the Israeli defence forces. His parents had immigrated to Israel in 1967, giving birth to him a few years later and bringing him up in a very patriotic house which believed that the country belonged to the Jewish people. At 18, he joined up, first as a pilot and then becoming an infantry officer serving mainly on the West Bank.

But surprised at what he saw there, he began to understand the Palestinian cause for the first time and what Israel was doing to the Palestinian people. When growing up, he had known very little about what was happening on the West Bank and he decided that he didn't want to serve there anymore. The occupation was not strengthening Israel's security, he felt, but building up hatred for the future.

'I believed there was the potential to create peace without compromising our security. There was no need for us to be in cities intimidating youngsters and women, as happens when you give the army a policing role. I also saw what it was doing to my people – good people committing human rights violations in difficult situations.

'So I refused to go on doing it, and I was jailed for a month which gave me time to think about how I could change the views of my people. I decided to create stories explaining what was

happening on the West Bank by making film documentaries that would help my intelligent brothers and sisters to understand the need for change.'

He also made documentaries about social issues such as poverty, minority rights and the treatment of women. His films were well-received abroad and at film festivals, but he felt that he needed to do more to capture the reality of the people on the West Bank. He wanted them to be able to tell their own stories and say what they wanted to say.

'Instead of me going out there to film them, I thought I should give them the technology and training to help them tell their stories. So I analysed where there was suffering on the West Bank, where there was talent and gave 100 cameras to people living there. They came back with amazing images of violations of human rights and mistreatment in their daily lives, and the 'Shooting Back' film we made from them won awards and helped us bring perpetrators to court.

'The next step was to move beyond Israel, and give cameras to oppressed communities around the world, so they could show us what we don't see. I travelled under cover to Turkey, Africa and Asia to find out what was needed. And I moved to London where there was access to lots of resources for my research.'

He also formed a partnership with film-maker Uri Fruchtmann, a former husband of the singer Annie Lennox. They founded a charitable organisation called Videre est Credere – which means ‘to see is to believe’ – and they developed a four-step approach to their work:

1. Engage with local communities, especially in rural areas where journalists rarely get to.
2. Equip and train local activists so they can operate safely with cameras to film violations.
3. Verify the images captured by the activists to avoid creating fake news which would undermine Videre’s work.
4. Create impact by distributing the images to people who can change what is happening – whether they be decision-makers, lawyers or media organisations.

The cameras initially used in Israel in 2007 and 2008 were large – this was before everyone had smaller smartphones. The hundreds of cameras now used by Videre are even smaller still and can be hidden in everyday objects. Mostly produced in China, they can be bought online.



‘Visual images are the best method of communicating, both for the mass media and to provide evidence for legal purposes. And spy cameras are now easily hidden in objects such as car keys, screws set in walls, stones, jewellery and clothing. They have apertures as small as a millimetre and they can film in high definition, and we can also record what is said. We might use dozens of cameras for specific projects.

‘We also customise our cameras and develop new ways of concealing them, using 3D printers to make what they are hidden in. Our laboratory does other kinds of research, such as tracking the routes used by people-traffickers for bringing people across borders to do forced labour. And with big data applications, it can analyse complex information to explore the structures behind violations and corruption.’

Projects are selected where Videre can bring most added value and have an impact. Some take years to complete, creating sustainable structures, training people and using their skills in different ways. But Videre always starts with massive amounts of research by its own research department working independently, investigating on the ground with its own cover stories.

It focuses on three issues:

- What information is needed – which might include documents, bank statements, accounts and social structures as well as visuals;
- Who will be involved on the ground to collect the information and verify it, and the techniques and equipment needed to do so;
- Which organisations should be used to distribute the information for maximum impact.

‘For example, with a corruption investigation in Africa, we didn’t need to go there because we knew people were paying massive bribes. So our researchers spent a year and a half tracking down the details of who was involved and how money was being moved around. They identified people on the ground who could collect the necessary evidence, whether film, documents or anything else, verify it and then check it in case more work was needed.’

Videre is currently working in seven countries where it believes there is the impact potential to change things. Sometimes it will identify organisations that it can work with on the ground, teaching them how Videre works and training their people so that it can increase its global impact without having to open more offices.

The organisation centrally employs around 30 people with skills in information-gathering,



‘Visual images are the best method of communicating, both for the mass media and to provide evidence for legal purposes’

communications, fund-raising, accountancy, technology and security. In local offices, people are recruited from the military, human rights and development organisations, and creative fields such as film-making. It has a £2 million budget, the majority of which is given by philanthropists. There is hardly any income from governments, except for specific projects.

A potential new source of funding is supporting investigation and audit processes used by local companies, many of whom are failing to take the right decisions in their overseas activities because they lack the right information. This makes it hard for them to uphold their corporate social responsibilities and acquire companies in places where Videre has the information and access.

‘So we are creating a social impact business in parallel with our charity. We can see what’s

happening upstream in remote areas and warn them if they’re drifting into a bad place – for example, into an area where slave labour is used. As a charity, we could increase our work if we can earn an income from this.’

One final point that Oren Yakobovich is keen to emphasise is that the organisation never takes credit for its work. ‘People see our work in the media all the time and hear of it in court cases. Often when I’m talking to people about an issue, they say Videre is not needed because work is already being done on it.

‘But what they are talking about is our work, our verification and our processes – and we never say it was us to protect the security of our teams and partners.’ ●



Ensuring the protection of confidential data until the end

Two entrepreneurs who created a service which shreds paper documents on-site for clients have developed techniques for destroying redundant hard drives, putting the information they hold beyond the reach of competitors and criminals

There is much talk in business of 'the paperless office', but as technology advances, more and more paper is used in the workplace – increasing the amount that needs to be destroyed to preserve confidentiality. That insight was what prompted Yarom Ophir and Siddik Apaydin to found Katana, a Swiss paper-shredding company that provides its services from trucks which do the job at clients' businesses where they can monitor its destruction.

'While working for a client in a previous business, we ended up using its office shredders all day,' says Yarom Ophir, Katana's chairman. 'We started imagining a truck that would come and destroy paper at the office, and realised there was a market for such a service.'

'In pre-digital days, documents were produced on typewriters, perhaps with carbon paper to produce a second copy. Today, word-processed

documents are cc-ed in emails to everybody working on a transaction, and they will often print them out – multiplying the amount of paper which needs to be shredded.'

The company started its paper-shredding operations in 2004 with a single truck that could destroy 800 kilogrammes of paper documents an hour, which is much faster than office shredders. It found a ready market among banks, insurers, government bodies and large multinational companies which produce large amounts of confidential documents. By 2009, it had expanded from Geneva to the whole of Switzerland, destroying 5,000 tonnes of paper in that year for more than a thousand customers.

But within a few years, clients began asking Katana whether it could shred the hard drives on their personal computers and servers. Since paper



‘There is a popular belief that data can be removed from digital devices by deleting it or reformatting the hard drives’

shredders were not strong enough to handle the job, the two co-founders launched Katana Digital which operates trucks capable of destroying data on CDs, DVD, back-up tapes and USB keys as well as hard drives on gadgets such as copiers.

‘There is a popular belief that data can be removed from digital devices by deleting it or reformatting the hard drives,’ says Siddik Apaydin, the company’s chief executive. ‘But that never takes the data away: it just overrides it by changing the binary code – and that can often be reversed. No specialist will say that erasing a hard drive is 100 per cent secure.’

Katana Digital has three processes for destroying digital data. One is degaussing which uses powerful magnets to permanently remove or randomise the data. The second drills a hole in the centre of a hard disc, which renders it completely unusable. The third physically shreds the hard drive by using special equipment inside the company’s trucks. Katana guarantees the total annihilation of data stored on hard drives.

Before processing, the hard drives are scanned to create a record of what has been destroyed for the client. And the whole operation is carried out at the client’s site, so that data cannot be stolen by taking it elsewhere. The process is filmed so that the client can watch and keep a copy of the footage if required. The materials used to make the hard drives – which include gold, copper, titanium and aluminium – are recycled through reputable companies.

Today, the company has grown to 30 staff with 14 trucks, and plans to expand into the rest of Europe, where 500 million hard drives have been produced in the last five years and 80 million more are now added each year. It is targeting Benelux, Germany, Italy and France by the end of 2017, and moving on to Eastern Europe in 2019–20.

The latest concern which Katana is addressing is the growth of the internet of things – household appliances with online links which can store data. ‘We started as luxury garbage-men destroying paper,’ says Yarom Ophir. ‘But today we are a hi-tech business, working with high security people to preserve the confidentiality of data.’

‘Henry Ford advised companies never to ask their customers what they want, because they would say a faster horse. We follow his advice by using our experience to try constantly to anticipate what the client needs, and then offer it better.’●

‘Today we are a hi-tech business, working with high security people to preserve the confidentiality of data’





Strong earnings growth from an industry which is expanding fast

Stocks in businesses that provide security solutions in a wide variety of market sectors are proving to be an attractive investment theme with growth fuelled by innovation, urbanisation and regulation

When Pictet Asset Management launched the Security Fund ten years ago, the security market was not seen as a strong or growing one. But today the security industry is growing very fast, and expanding to cover many different market sectors.

Security permeates our lives, from dawn to dusk. When we rise in the morning, we use electricity, gas and water to heat our homes, shower and make breakfast – relying on utilities whose operations are securely protected. We travel to work by car or public transport, using equipment secured for our safety and under the watchful eyes of products such as video surveillance.

At work, there are plenty of cyber-security functionalities activated when working online, while the safety of our meals is ensured by testing and traceability. When we shop, we use electronic payment systems that authenticate our transactions and detect fraud. When we travel by train or plane, our safety is ensured during the journey.

The security industry is everywhere, strongly anchored in our daily life, which is why it has been growing so fast over the last few years. And what makes it attractive to investors is that there are three long-term drivers providing secular growth: innovation, urbanisation and regulation.

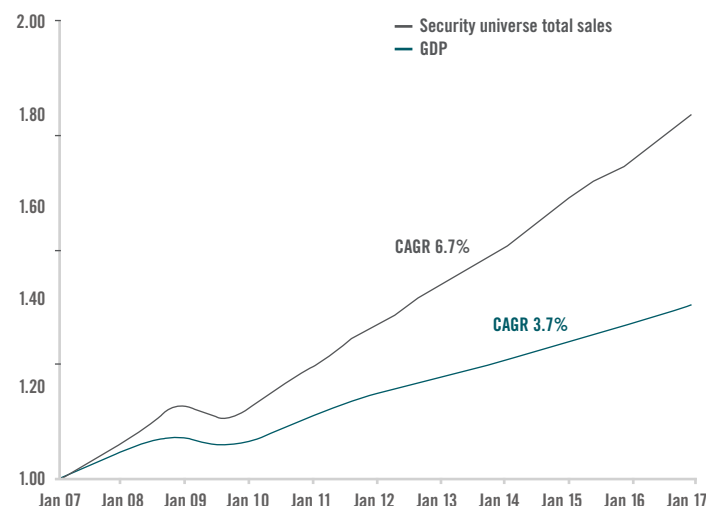
Innovation can be seen in the new security needs that have arisen from modern technologies. Let's take the automotive industry as an example. The autonomous car is no longer a dream: it will be reality in the next couple of years. To get there, the security content for each vehicle will increase significantly. It is not only about seatbelts and airbags but features such as cameras, sensors, autonomic braking systems, radar, laser and night visions systems.

There are similar demands for internet security, which was barely required 25 years ago when we mainly used phones and faxes. Now the internet connects billions of people online through many different devices. Security challenges already include data theft and hacking attacks but it is still early days for the emerging cyber-security market. Only 50 per cent of the world's population is online and connecting the rest will expose the IT infrastructure to new threats at a time when data breaches are already increasing by 60 per cent a year.

The second driver is urbanisation which requires massive investment to secure infrastructure such as power plants, mass transit systems, airports and water utilities. More than half the world's population now lives in urban areas, and that proportion continues to rise.

SECURITY SALES WILL CONTINUE TO GROW MUCH FASTER THAN GDP*...

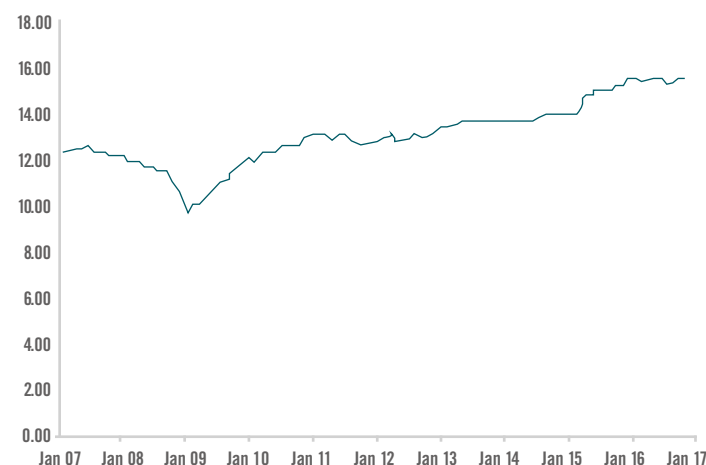
Security universe total sales, GDP real rebased, Jan 2006



*GDP OECD data G20 GDP – Constant prices, growth rate same period previous year seasonality adjusted % – World

...WHICH WILL DRIVE FURTHER MARGIN UPSIDE

Security universe EBIT margin (%)



We estimate that with the large restructurings during the last crisis and better cost discipline, a large majority of companies in the universe can expand margin above prior peaks

The security industry is
everywhere, strongly anchored
in our daily life

Security spending on urban areas in developing and emerging markets is forecast to grow at around 9 per cent a year over the next five years – more than twice the rate in developed markets. Dubai is a good example of what can be achieved when building a new smart city that did not exist two decades ago, integrating brand new security solutions into its infrastructure.

The third driver is regulation, which imposes rules on public bodies, companies and individuals that must be applied. Even in sectors such as financial services where compliance officers apply the rules, testing, inspection and certification has become big business. And new rules are coming all the time – for example, the mandatory side-airbags for every new car in Brazil recently. In France, every home has had to have a smoke alarm since 2015.

In a near future, all new vehicles in Europe must have an eCall terminal which automatically contacts the emergency services if it is involved in a crash – a rule already introduced in Russia not too long ago. Meanwhile, the EU's General Data Protection Regulation which will be enforced in 2018 will require European companies to disclose data breaches, their financial and reputational impact such as the number and kind of data stolen, and the measures taken to avoid repetition. Not complying with this new regulation will also mean the possibility of companies being sued, with fines amounting to 4 per cent of turnover or EUR20 million.

Then there are food regulations which support a large food-testing market around the world. The number of international standards rises every year, and the regulations have to be implemented.

Given this sharp growth in the security industry, Pictet has identified a universe of 330 companies with relevant theme-related activities which have a total market capitalisation of USD3.3 trillion. Applying our SRI criteria excludes any company with more than 5 per cent of sales related to defence or military equipment. Furthermore, our purity test eliminates companies with less than 20 per cent of sales in security. These criteria reduce the universe



to around 210 companies with a total market cap of USD1.1 trillion.

Next comes Pictet's investment process to manage the liquidity and share price volatility of the portfolio for risk management purposes. We visit the companies once or twice a year to evaluate their business franchise – their strategy, competitors, pricing power and similar issues. We also assess the management quality – what kind of management, track record, shareholder-friendliness and how it applies ESG factors.

We score the 210 stocks, and select the 60–75 best companies to make up the portfolio. The portfolio is solely made up of the strongest convictions without any references being made to any benchmarks – geographic exposure, for example, is the result of our conviction ideas. So in December 2016, six of the top ten stocks were US-based companies, two from Japan and one each from Sweden and The Netherlands.

When looking at the geographic breakdown of demand for security products, North America accounts for

48 per cent of sales, Europe is the second largest source of sales with 24 per cent, followed by emerging markets (14 per cent) and Developed Asia-Pacific (10 per cent – mainly Japan).

One additional attraction of security stocks is the diversity of market opportunities in the fund. Secure electronic payments products account for 19 per cent of the fund, followed by cloud computing and cyber-security (16 per cent), and occupational safety (14 per cent). Infrastructure safety is 11 per cent, environmental and food safety just under 10 per cent, as is residential and non-residential construction.

The value of the Pictet Security Fund has risen to USD1.65 billion since its launch and with excellent performance, even when risk-adjusted. The future remains bright. Since January 2007, sales growth of the security universe has averaged just under 7 per cent, compared with 3.7 per cent for global GDP. The operating margins of the fund universe have expanded as well, outpacing previous cycle highs. We expect this to continue. ●

Yves Kramer joined Pictet Asset Management in 2005 and is a Senior Investment Manager in the Thematic Equities Funds team. He launched the Security Fund in 2006. Previously, he had spent five years in Pictet's Financial Research Department as an Equity Buy-Side Analyst for European and North American software stocks. Before joining Pictet he worked as a Financial Analyst for North American equities at Union Bancaire Privée. Yves graduated from the University of Geneva with a BA degree in Finance.

Acknowledgements

We should like to thank the experts, researchers and entrepreneurs who talked to us about how they see global security threats, the solutions needed to protect society against them, and how new technologies can be used for humanitarian purposes:

Doron Bergerbest-Eilon, Jean-Luc de Buman, Professor Moran Cerf, Professor Leslie John, Dr David Kenyon, Dr Patricia Lewis, Mårten Mickos, Yarom Ophir & Siddik Apaydin, Grégoire Ribordy & Kelly Richdale and Oren Yakobovich.

Pictet Report

Pictet Report is published by Pictet Group on a periodical basis. Its contents are based on a series of specially commissioned interviews and discussions on particular investment and business themes of topical interest.

Pictet

The Pictet Group is a partnership of six owner managers. It offers only wealth management, asset management and related asset services. The Group does not engage in investment banking, nor does it extend commercial loans. With more than CHF 478 billion in assets under management at 31 March 2017, Pictet is today one of the leading Europe-based independent wealth and asset managers.

Headquartered in Geneva, Switzerland and founded there in 1805, Pictet today employs more than 3,900 people. It has 26 offices in: Amsterdam, Barcelona, Basel, Brussels, Dubai, Frankfurt, Geneva, Hong Kong, Lausanne, London, Luxembourg, Madrid, Milan, Montreal, Munich, Nassau, Osaka, Paris, Rome, Singapore, Taipei, Tel Aviv, Turin, Tokyo, Verona and Zurich.

Disclaimer

This document is not intended for persons who are citizens of, domiciled or resident in, or entities registered in a country or a jurisdiction in which its distribution, publication, provision or use would violate current laws and regulations. The information and data furnished in this document are disclosed for information purposes only and do not constitute a solicitation to subscribe to products or services of the Pictet Group*.

The content of this document is confidential and can only be read and/or used by its addressee. The Pictet Group is not liable for the use, transmission or exploitation of the content of this document. Therefore, any form of reproduction, copying, disclosure, modification and/or publication of the content is under the sole liability of the addressee of this document, and no liability whatsoever will be incurred by the Pictet Group.

The addressee of this document agrees to comply with the applicable laws and regulations in the jurisdictions where they use the information reproduced in this document. This document is issued by the Pictet Group. This document and the contents therein may be cited if the source is indicated, but the reproduction or distribution of this publication, in part or in whole, is prohibited.

All rights reserved. Copyright 2017

**The Pictet Group includes the entities mentioned in the report published under the following link: www.group.pictet/reports*

