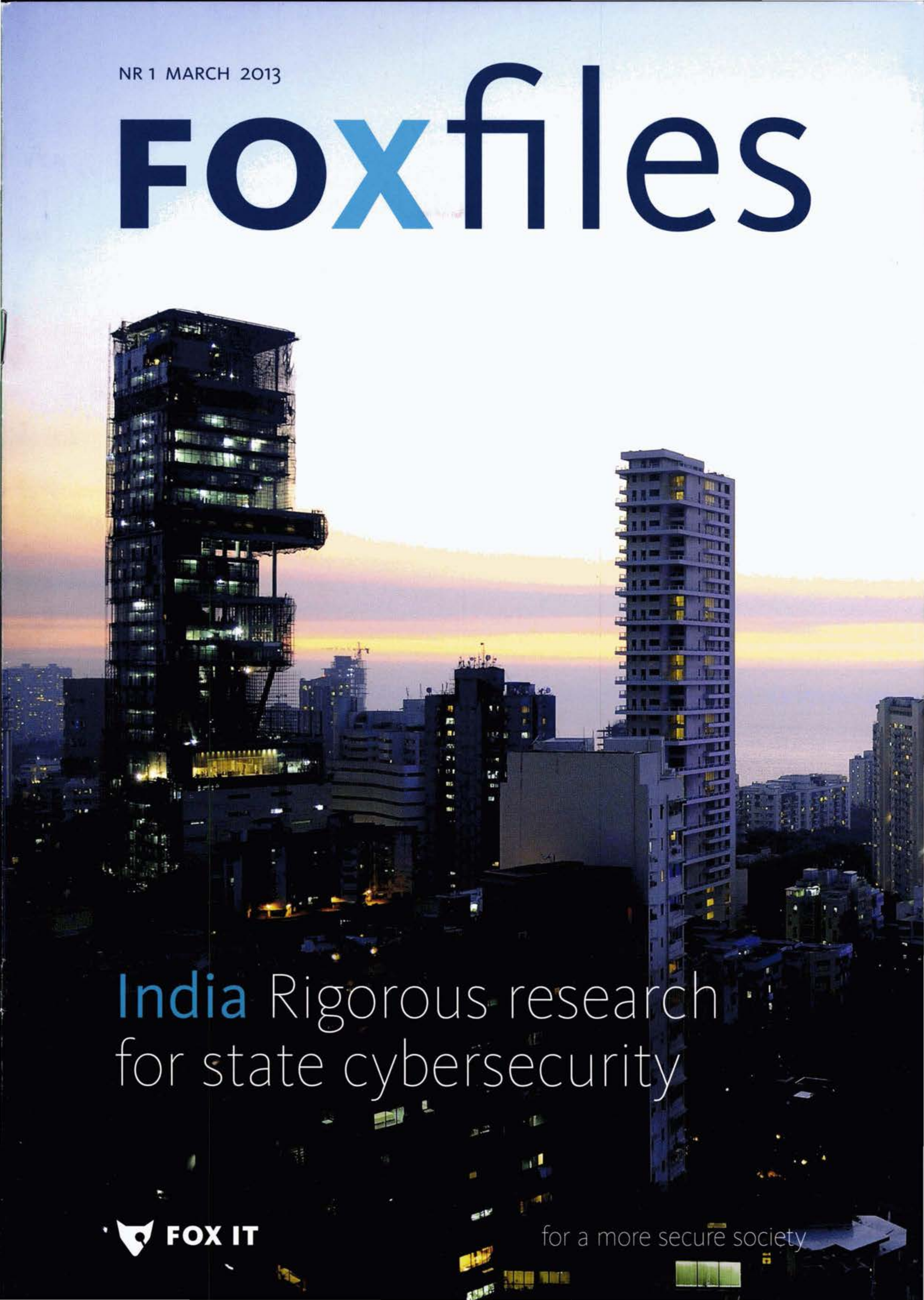
NR 1 MARCH 2013

FOXfiles



India Rigorous research for state cybersecurity

FOX IT

for a more secure society

The Hypocrisy of Ethical Hacking

It seems such an interesting idea: 'ethical' hackers who guard our vulnerable databases containing privacy-sensitive data. Surely there is no objection to that?

The Netherlands' so-called 'Lektober' (literally, leaky October) in 2011 witnessed a number of incidents and demonstrated that data security needs to be improved in our country. It was a wake-up call. After that, Robin Hood stories about hacks moved from tech news to the front pages.

Fortunately the appreciation for ethical hackers has grown. However, they still run the risk of being prosecuted. Even if a hacker himself believes he is engaged in ethical work, the affected companies and the law often hold a different view.

Two issues recently hit the headlines. At two medical institutions in the Netherlands, the 'Groene Hart' hospital and 'Diagnostiek voor U', patient details became accessible to hackers, who sought publicity through the media. In both instances the Public Prosecutor opted to institute legal proceedings. On first glance, this appears to turn the world upside down: if someone made a mistake here, then surely it was the organizations which were negligent in safeguarding the details of their clients?

There is certainly something to be said for that. But on closer examination the hackers appear to be less ethical than thought. In the case of the hospital, the hacker went straight to the media rather than to the hospital itself. Ethical hackers raised a number of questions about the time between discovery and notification, the means used and the volume of data which was stolen. At 'Diagnostiek voor U', Dutch MP Henk Krol broke into an Electronic Health Record using a stolen password. He looked up friends in the database, and soon after notifying the organization he approached the media. I learned the significant reasons for prosecution from the public gallery of the court, not from the otherwise well-informed media.

The media's pillorying of companies which have fallen victim to hacking, without any reasonable discussion about the ethics of the hacker, misses the point. It is time for all of us to take a good hard look in the mirror. And there, alongside the ethics of hackers and companies, are also the ethics of the media.

Ronald Prins, CEO FOX-IT

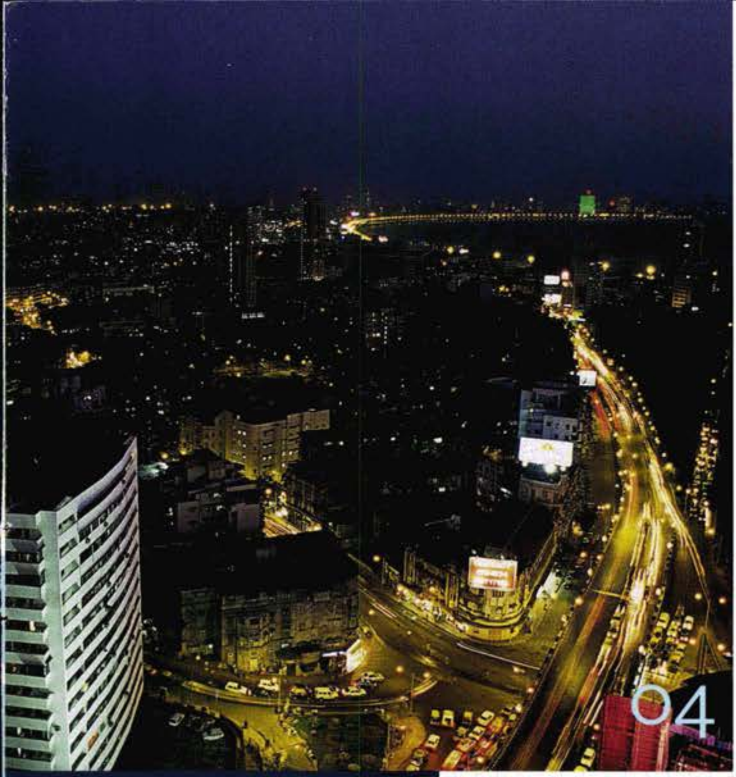
COLOPHON

Editorial address
FOX-IT Marketing Department
PO Box 638
2600 AP Delft
+31 (0)15 284 79 99
marketing@fox-it.com
www.fox-it.com

Concept and design
viervier

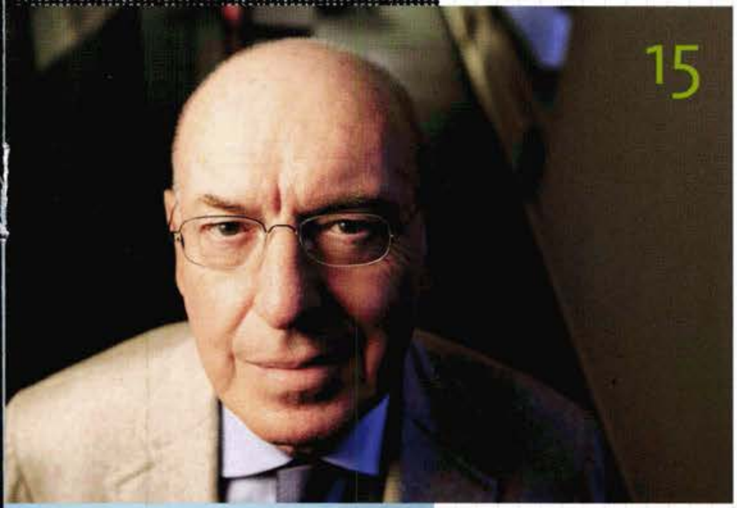
Interviews and articles
Sabel Comunicatie
Full Circle Communications
FOX-IT

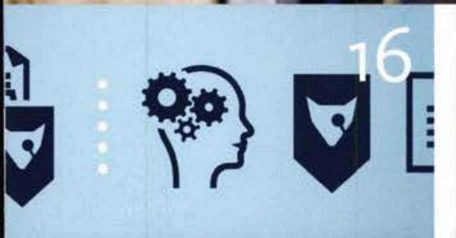
Free subscription
Register on fox-it.com

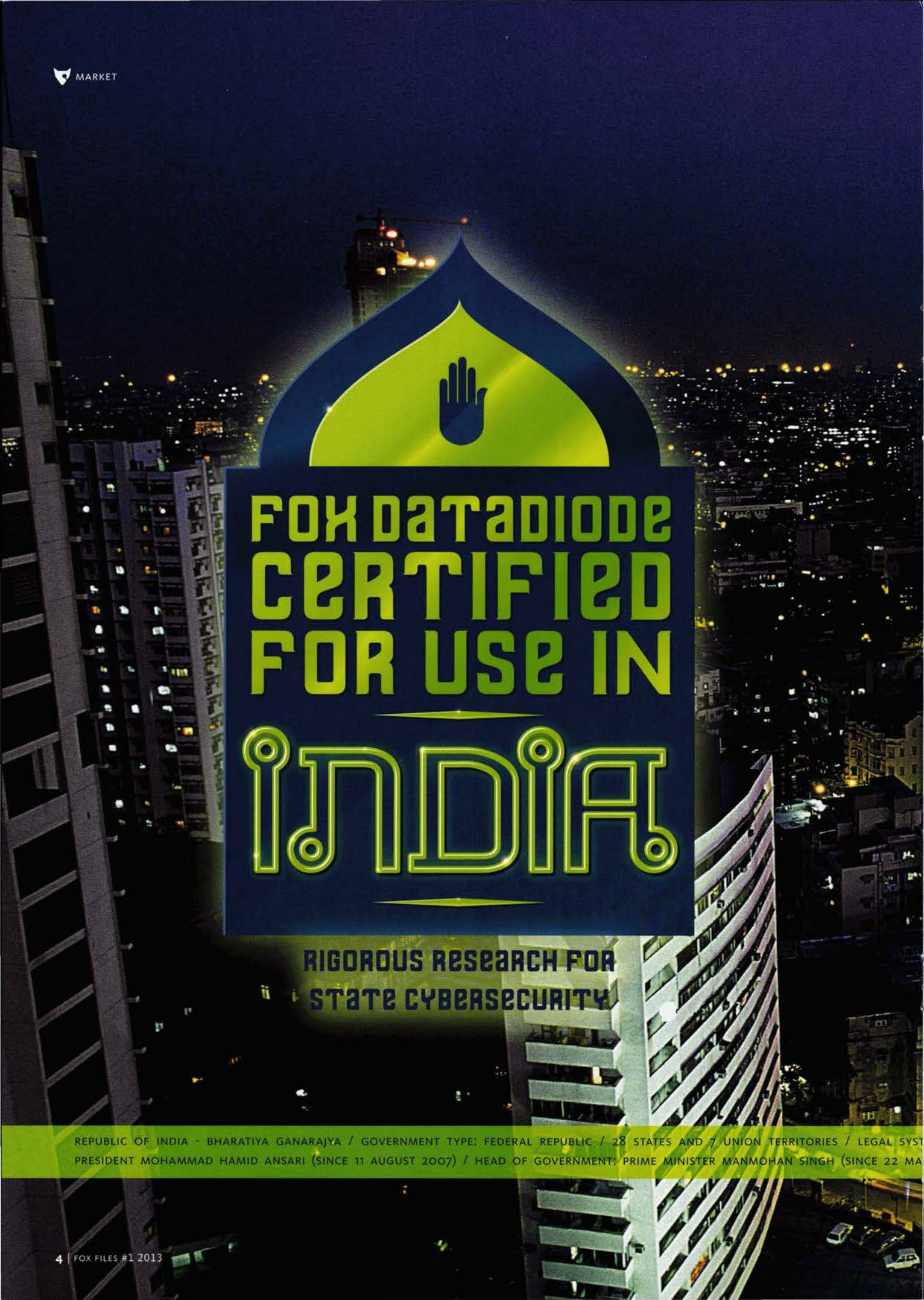

04

10

12


15

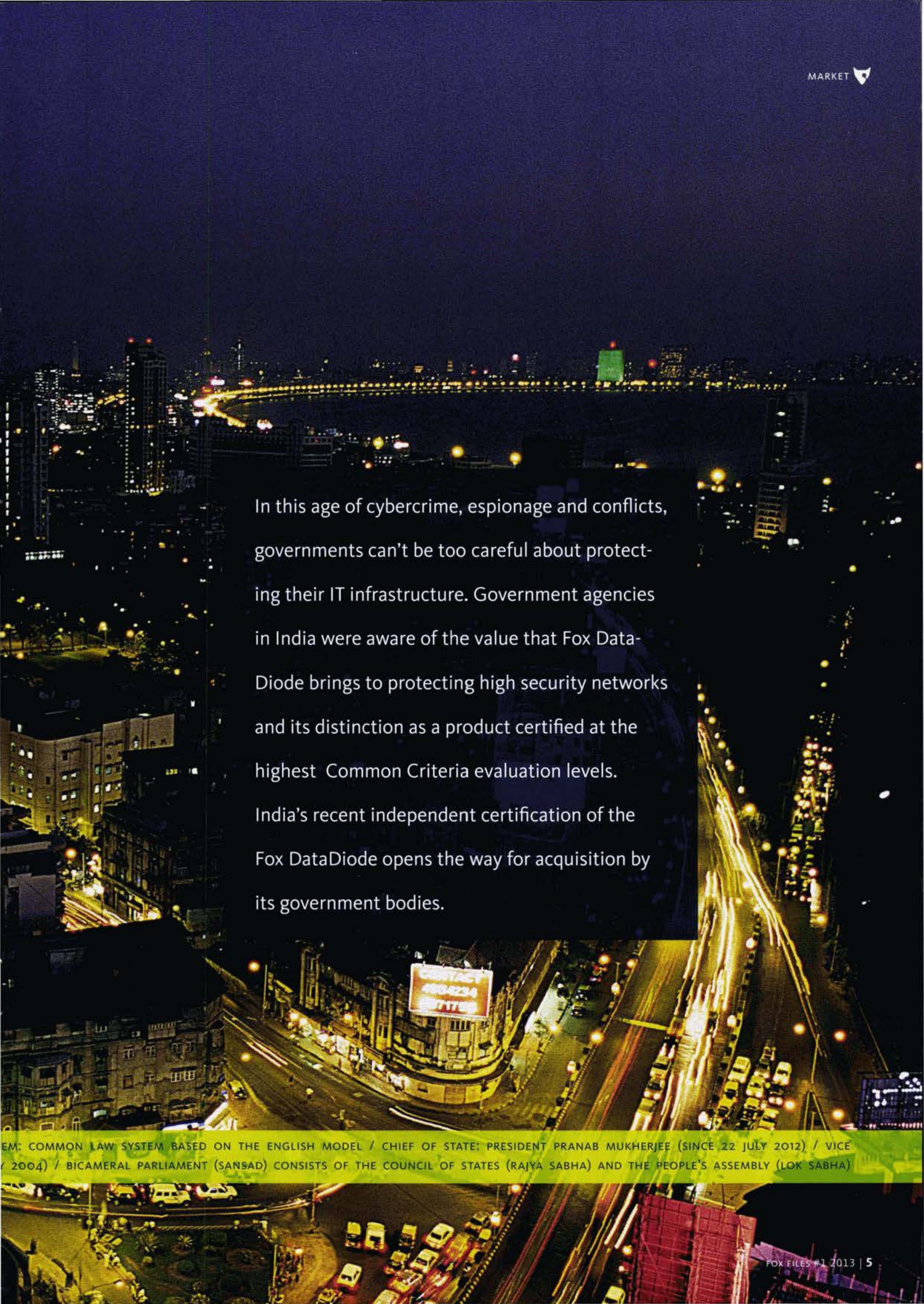

16



FOX DATADIODE CERTIFIED FOR USE IN INDIA

RIGOROUS RESEARCH FOR STATE CYBERSECURITY

REPUBLIC OF INDIA - BHARATIYA GANARAJYA / GOVERNMENT TYPE: FEDERAL REPUBLIC / 28 STATES AND 7 UNION TERRITORIES / LEGAL SYST
PRESIDENT MOHAMMAD HAMID ANSARI (SINCE 11 AUGUST 2007) / HEAD OF GOVERNMENT: PRIME MINISTER MANMOHAN SINGH (SINCE 22 MA



In this age of cybercrime, espionage and conflicts, governments can't be too careful about protecting their IT infrastructure. Government agencies in India were aware of the value that Fox DataDiode brings to protecting high security networks and its distinction as a product certified at the highest Common Criteria evaluation levels. India's recent independent certification of the Fox DataDiode opens the way for acquisition by its government bodies.

EM: COMMON LAW SYSTEM BASED ON THE ENGLISH MODEL / CHIEF OF STATE: PRESIDENT PRANAB MUKHERJEE (SINCE 22 JULY 2012) / VICE
2004) / BICAMERAL PARLIAMENT (SANSAD) CONSISTS OF THE COUNCIL OF STATES (RAJYA SABHA) AND THE PEOPLE'S ASSEMBLY (LOK SABHA)

The Fox DataDiode is a hardware device for use at that boundary of two computer networks. It allows data to travel in only one direction. For its use to protect secrets, information can be passed from a lower security network to a higher security secret network, but not vice versa. For its use to protect critical infrastructure like energy plants or water facilities, selected information can be pushed from a trusted Industrial Control System (ICS) to an external network, while the facility remains digitally inaccessible from the outside. Many prime government organizations in India are interested in deploying the Fox DataDiode to protect classified data and critical infrastructure networks. While the Fox DataDiode would be a major security and productivity upgrade over bidirectional fire walls and 'air gap' techniques to transfer sensitive data involving high-security networks, it could not be implemented until approved for use by India's Standardization Testing and Quality Certification (STQC) Directorate - the Indian Government's certification body.

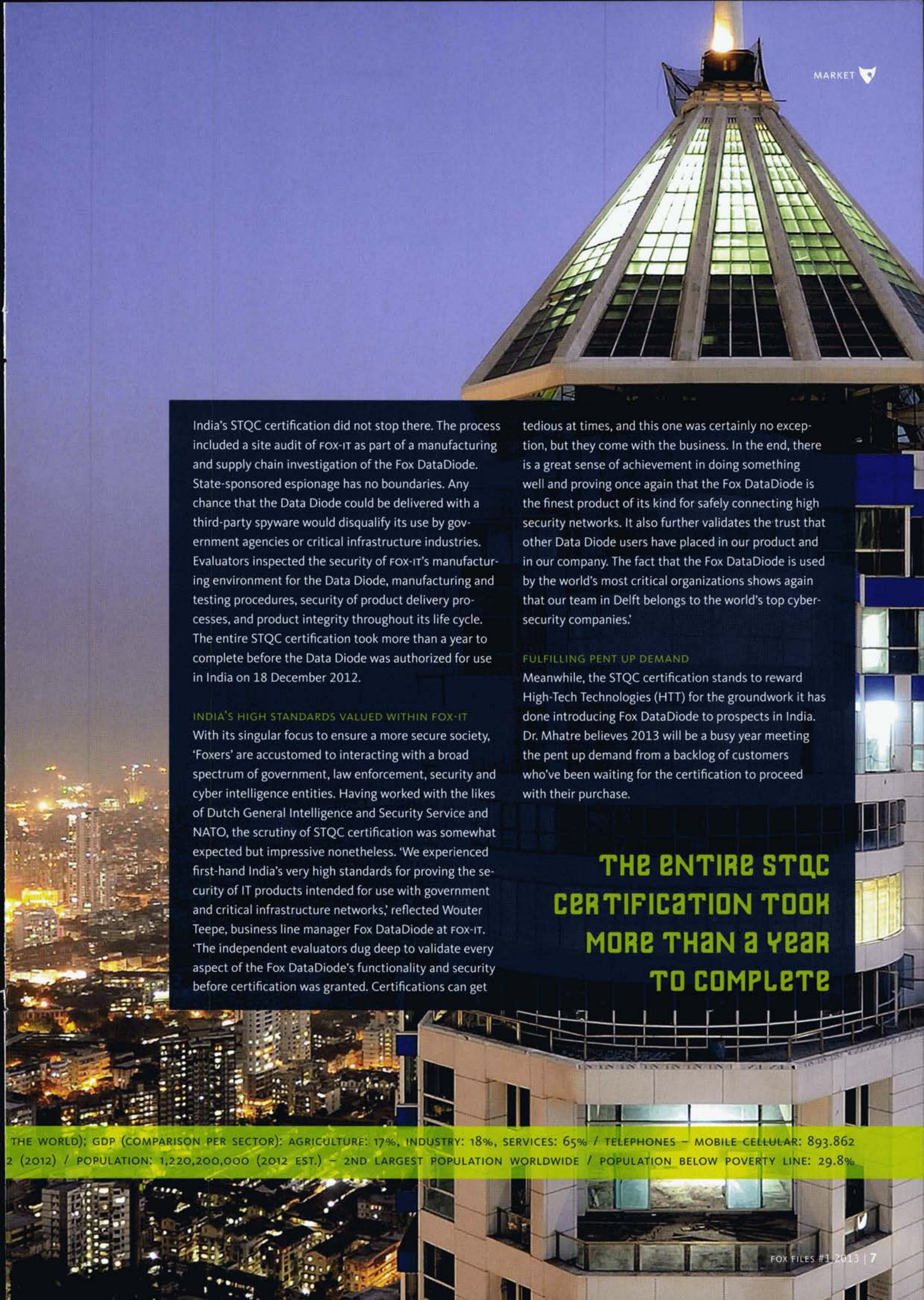
RIGOROUS CERTIFICATION PROCESS

Certification would seem to be a relatively simple process. The Fox DataDiode is already recognized internationally with the highest Common Criteria Evaluation Assurance Level certifiable in India (CC EAL4+). In fact, it has achieved CC EAL7+ certification in Europe; is approved for network connections up to and including NATO Secret; and is deployed in many countries around the world. But, in the words of Dr. Dinesh Mhatre, CEO of FOX-IT partner High-Tech Technologies in Mumbai, India: 'Prospects are very keen on the product but the Indian Government needs proof that the box shipped performs as specified and that the claims made on paper are actually true.'

India is after all a founding member of the International Organisation of Standardisation and responsible for the development of many ISO standards. Validating and documenting products and processes for the exchange of goods and services are ingrained in the country's business culture. In addition to its leadership role in the ISO, the Bureau of Indian Standards has published more than 18,000 standards for domestic use. More than 300 new Indian standards and 300 amendments to existing standards are published every year.

In India's view, the Data Diode's Common Criteria compliance does not necessarily mean secure until evaluated by its own Indian Common Criteria Certification Scheme (IC3S). This meant reviewing all procedures and documentation provided by FOX-IT on previous testing and certifications, duplicating tests in its own Common Criteria Testing Laboratories, and conducting additional tests on Fox DataDiode's functionality and security, which included vulnerability assessments and hypothetical attack scenarios. All testing planned and performed by the independent evaluators had to be documented to a level of detail that would ensure repeatability of testing procedures and the capability to reproduce results.

NATIONAL SYMBOL: BENGAL TIGER / NATIONAL ANTHEM: 'JANA-GANA-MANA' / CURRENCY: INDIAN RUPEES (INR) / GDP: $4.735 TRILLION (4TH IN
MILLION (2011) – RANKING 2ND IN THE WORLD / INTERNET USERS: 61.338 MILLION (2009) – RANKING 6TH IN THE WORLD / AIRPORTS: 35



India's STQC certification did not stop there. The process included a site audit of FOX-IT as part of a manufacturing and supply chain investigation of the Fox DataDiode. State-sponsored espionage has no boundaries. Any chance that the Data Diode could be delivered with a third-party spyware would disqualify its use by government agencies or critical infrastructure industries. Evaluators inspected the security of FOX-IT's manufacturing environment for the Data Diode, manufacturing and testing procedures, security of product delivery processes, and product integrity throughout its life cycle. The entire STQC certification took more than a year to complete before the Data Diode was authorized for use in India on 18 December 2012.

INDIA'S HIGH STANDARDS VALUED WITHIN FOX-IT

With its singular focus to ensure a more secure society, 'Foxers' are accustomed to interacting with a broad spectrum of government, law enforcement, security and cyber intelligence entities. Having worked with the likes of Dutch General Intelligence and Security Service and NATO, the scrutiny of STQC certification was somewhat expected but impressive nonetheless. 'We experienced first-hand India's very high standards for proving the security of IT products intended for use with government and critical infrastructure networks,' reflected Wouter Teepe, business line manager Fox DataDiode at FOX-IT. 'The independent evaluators dug deep to validate every aspect of the Fox DataDiode's functionality and security before certification was granted. Certifications can get tedious at times, and this one was certainly no exception, but they come with the business. In the end, there is a great sense of achievement in doing something well and proving once again that the Fox DataDiode is the finest product of its kind for safely connecting high security networks. It also further validates the trust that other Data Diode users have placed in our product and in our company. The fact that the Fox DataDiode is used by the world's most critical organizations shows again that our team in Delft belongs to the world's top cybersecurity companies.'

FULFILLING PENT UP DEMAND

Meanwhile, the STQC certification stands to reward High-Tech Technologies (HTT) for the groundwork it has done introducing Fox DataDiode to prospects in India. Dr. Mhatre believes 2013 will be a busy year meeting the pent up demand from a backlog of customers who've been waiting for the certification to proceed with their purchase.

THE ENTIRE STQC CERTIFICATION TOOK MORE THAN A YEAR TO COMPLETE

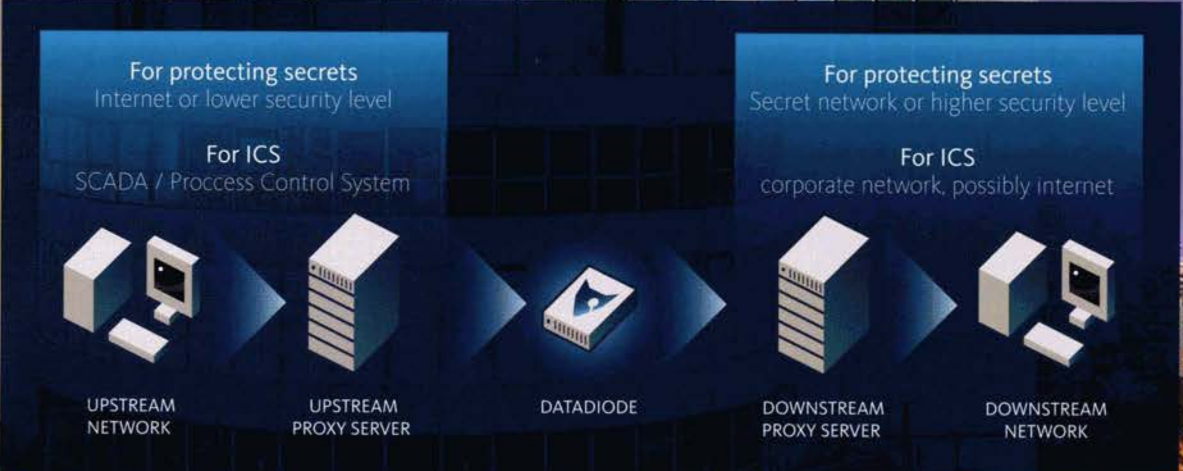
THE WORLD); GDP (COMPARISON PER SECTOR): AGRICULTURE: 17%, INDUSTRY: 18%, SERVICES: 65% / TELEPHONES – MOBILE CELLULAR: 893.862
2 (2012) / POPULATION: 1,220,200,000 (2012 EST.) – 2ND LARGEST POPULATION WORLDWIDE / POPULATION BELOW POVERTY LINE: 29.8%

During HTT's interactions with various government organizations, a wide variety of applications for the Fox DataDiode were discussed, such as:

- Sending emails automatically to a high security network as well as uploading files more efficiently
- Automating the distribution of antivirus, antispyware and software updates to isolated secret networks, which would accelerate updates and greatly simplify network management
- Enabling real-time communications between departments in a high security organization but ensuring that information is made available only on a need-to-know basis
- Centralizing data feeds from log files and SIEM (Security Information and Event Management) securely, so that multiple networks can be monitored from one location
- In specific cases: continuing an air gap process with USB drives, but using the Fox DataDiode between the computer where the drives are inserted and the rest of the high security network-to ensure that the network cannot leak information back to the USB drives

'Organizations can use the Fox DataDiode in many innovative ways to improve the security and efficiency of processes involving networks with sensitive information and supervisory controls,' said Dr. Mhatre. 'We expect this area of our business to surge now that the STQC certification is in hand.'

THE WORLD'S MOST CRITICAL ORGANIZATIONS USE THE FOX DATADIODE



MEDIAN AGE: 26.5 YEARS / 0-14 YEARS: 31.1%; 15-64 YEARS: 63.6%; 65-OVER: 5.3% / URBAN POPULATION: 30% OF TOTAL POPULATION / TO
TOTAL: 14,103 KM / COASTLINE: 7,000 KM / ELECTRICITY PRODUCTION: 880 BILLION KWH (2010 EST.) - 7TH IN THE WORLD / ELECTRIC

KEEPING STATE SECRETS SECRET

Isolating high security networks from the outside world is difficult, since their purposes are to manage data and control processes, however sensitive the information may be. While networks can be protected with a range of cybersecurity tools to keep intruders out-from firewalls to SIEM -vulnerabilities exist. Firewalls and data access permissions can be configured incorrectly (human error) or an adversary can develop a clever new exploit to evade cyberdefences and surreptitiously penetrate the network with malicious intent. Firewalls and SIEM are reactive defence measures that will always trail the first encounters with new types of malware. Even when the integrity of cyberdefence is fully intact, data from a high security network can 'leak back' to a lower security network during data transfers.

One way security experts eliminate these issues is to deploy air gap techniques where the high security network is never connected to another network. Instead, data transfers are done using portable media such as USB flash drives. But vulnerabilities exist here as well. Portable media can be lost or infected with malware. The well-publicized Stuxnet computer worm originally proliferated in this way. Air gap techniques also impact timely access to information. Data must be copied onto portable media and the media scanned for malware before transfer to a high security network.
The Fox DataDiode not only eliminates all of the security risks described above, but improves the ease of use over the airgap scenario by protecting information transfers in real time. It enables safely connecting high security networks with networks and devices at lower security levels by allowing information to travel in only one direction. It also prevents data leakage from a high security network during data transfers.

HOW FOX DATADIODE WORKS

The Fox DataDiode is a hardware device that allows data to travel in only one direction by using a fibre optic connection. It does not contain decision logic, software or firmware and cannot be misconfigured, eliminating any chance of software malfunctions, malware, tampering, online attacks or human error. The one way physical connection transfers information optically using a light source and corresponding photocell to ensure data can pass in only one direction. Fibre-optic cables minimize electromagnetic radiation when the device is connected between low and high security servers.

Typical IT protocols are bi-directional and hence cannot be transmitted over a one-way connection. Therefore proxy servers are installed on either side of the Fox DataDiode. On the sending upstream network a proxy server receives all the information to be transferred using bi-directional protocols. It passes the information on via a one-directional protocol through the Fox DataDiode. On the receiving downstream network a proxy server translates the uni-directional protocol back into a bi-directional protocol. Each proxy has an easy-to-use web interface that allows authorized users to configure what information is to be transferred. A transfer can contain files, streaming video, or incoming email.

TAL AREA: 3,287,263 SQ KM – THE WORLD'S 7TH LARGEST NATION / LAND: 2,973,193 SQ KM / WATER: 314,070 SQ KM / LAND BOUNDARIES:
ITY (INSTALLED GENERATING CAPACITY): 189.3 MILLION KW (2009 EST.) – 6TH IN THE WORLD / ELECTRICITY FROM NUCLEAR FUELS: 2.2%

Source: CIA World Factbook

VPN SITE-TO-SITE

INTERNET CONNECTIVITY IN ALL OF EUROPE

Dutch regional police deploy special van

Digital forensic investigation at the crime scene

It's like a scene in a crime movie: a van is parked at the crime scene, with police inside conducting forensic digital investigation. In the Dutch region of Twente this is not fiction, but reality. At the initiative of a number of digital investigators, the so-called Specialist Investigation Vehicle (SIV) has been on the road there since February 2012.

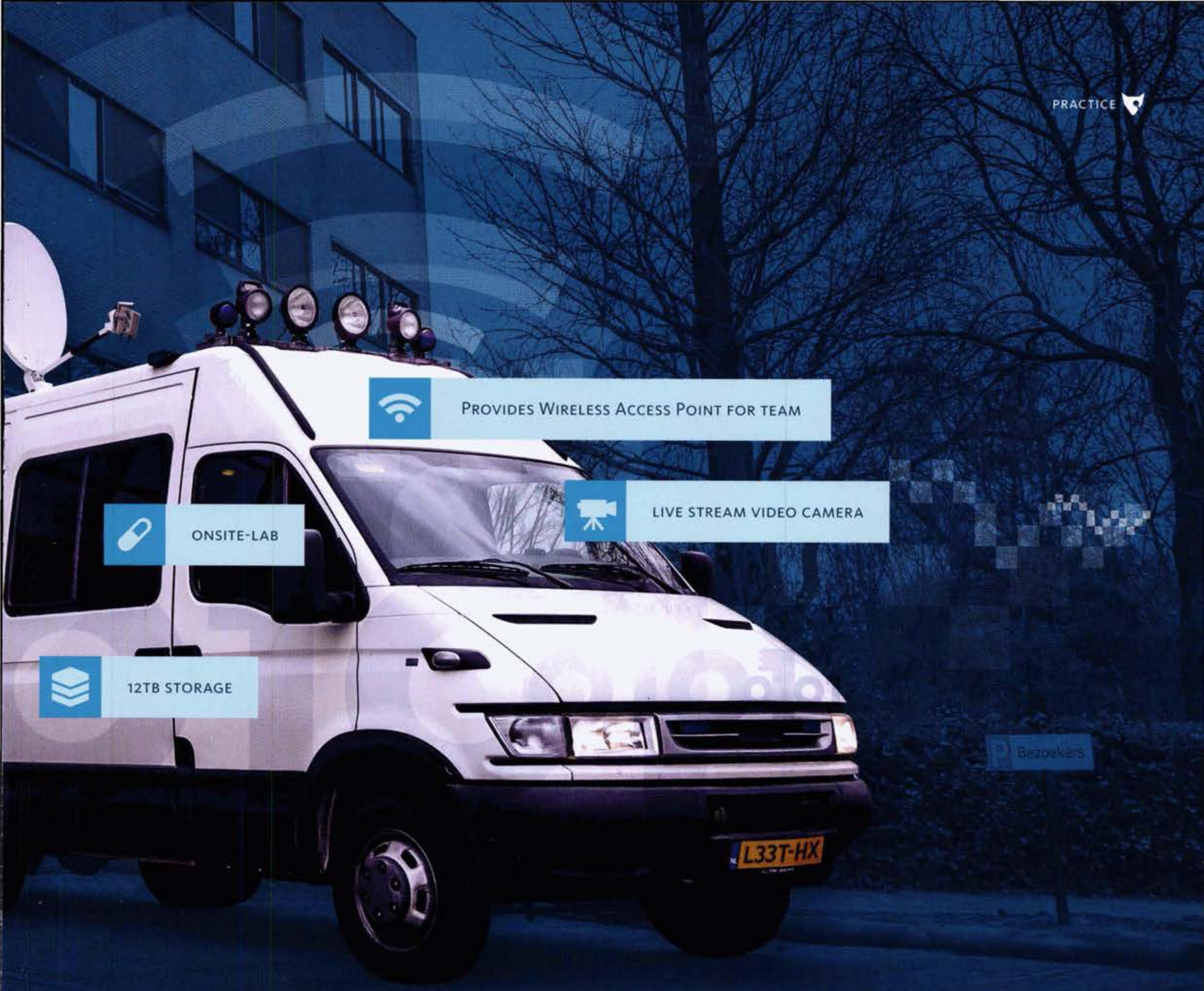
Text Nina van der Knaap en Brendan van der Maarel, FOX-IT

Police in Enschede needed a quality investigation performed on-site for speediness and a means to facilitate such an investigation. Back in 2010 the digital investigators in the police unit of the Netherlands East district of Twente were on the hunt for examples of mobile digital solutions. Digital investigators took a look at the police of Miami-Dade in the USA. They incorporated the technical ideas they saw there into the development of the SIV, the Specialist Investigation Vehicle.

A mobile solution like the SIV offered an answer, because the detectives did not have to drive to the lab with the digital data carriers, but could conduct forensic digital investigation right at the crime scene. Triage (prioritizing the most important items) was also possible, so that the detectives would not take too much evidence with them too readily. The advantage of the SIV is that the digital investigators of a large region such as Netherlands East could save a great deal of time by working on-site.

INVESTIGATION TYPES

The vehicle met a number of important criteria: it wasn't too big, could be driven with a so-called 'B' driving license (i.e. up to 3.5 tons), and was equipped with power outlets and an internet



connection. In the SIV forensic digital experts support the tactical investigation team with digital investigation, for example by examining data carriers, internet use, social media etc. So they can conduct all investigations on digital trace material, in this van. The tactical investigator determines when this is needed. Over the past 12 months the SIV has been deployed every week for a variety of issues, ranging from murder to traffic checks and from environmental crimes to missing persons.

PERFECT TEAMWORK

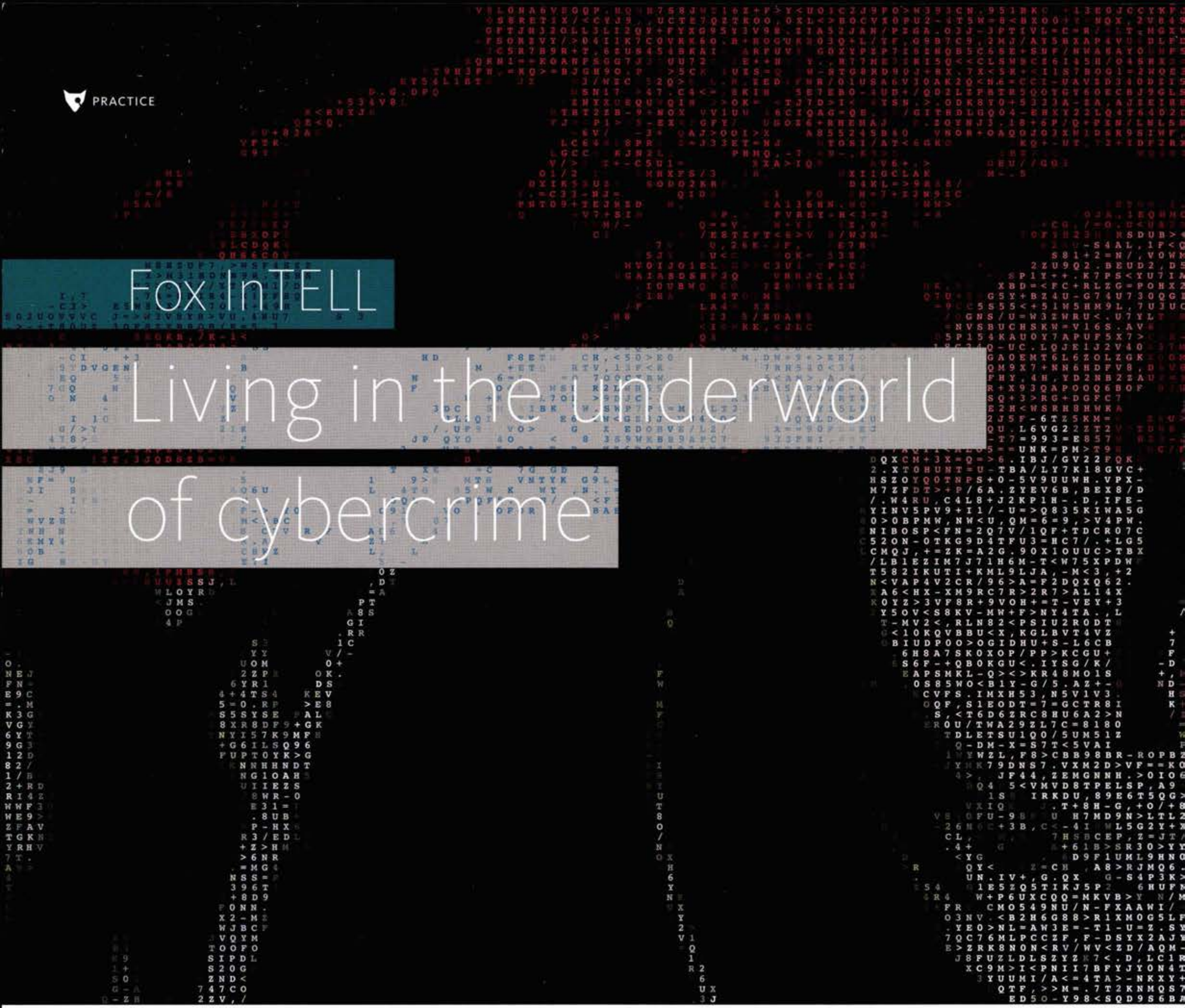
So the police deploy the SIV regularly and the digital investigators continue to expand and improve the possibilities. Thus the vehicle can also be used as part of an incident response team. Digital experts in the lab are then in internet contact with the incident response team at the crime scene, and examine the data remotely.

One of the advantages of the special police van is that the tactical investigators see the added value of their digital colleagues. These two specialist teams move closer together and thanks to short lines, they can collaborate more efficiently. Conversely it is useful for the digital experts to be able to switch directly with their tactical colleagues. Perfect teamwork, in other words.

The Specialist Investigation Vehicle is deployed every week, from murder to environmental crimes

WORKING WITH TRACKS INSPECTOR

The Specialist Investigation Vehicle (SIV) also incorporates FOX-IT's Tracks Inspector, software with which tactical investigators can read digital evidence material relatively easily. With Tracks Inspector the tactical investigator has direct access to the digital information and can apply relevant findings immediately in the investigation at the crime scene. Cooperation with the Specialist Investigation Vehicle in Twente thus also appeared to be a good combination. Tracks Inspector is user-friendly, intuitive and runs in a web browser. This is exactly what the tactical investigator needs to be able to conduct digital investigation easily himself.



Fox InTELL

Living in the underworld of cybercrime

If an enterprise's information security team doesn't know about a new cyber threat, they can't defend against it. Fox InTELL provides a way to see into the dark underworld of cybercrime so companies can protect their customers and their brands from cybercriminals' pending exploits and targeted attacks.

Underlying FOX-IT's network security and breach mitigation services is expert cyber intelligence. It's ingrained in so many things that the company does, offering Fox InTELL as a standalone product first in Europe and now in the U.S. was inevitable.

For years, FOX-IT has grown a world-class organization to continually gather, process and leverage actionable intelligence, both to fulfill client-specific requests and to innovate new products and services. In addition to its own Internet monitoring, Fox today works with a network of partners doing their own monitoring as well as intelligence, security and law enforcement agencies worldwide.

Through Fox InTELL, the information gathered by FOX-IT internally and from across the cyber intelligence community is made available to any enterprise on a subscription basis. The value to subscribers' information security (InfoSec) teams is an early warning of emerging threats and even pending attacks targeting their organization. With Fox InTELL, financial institutions, e-tailers and other high-profile enterprises can dramatically improve their cyber intelligence position, which enables situational awareness, deploying better security controls, and making more informed risk decisions to protect their customers and their brand online.

Fox InTELL improves situational awareness, enabling better security controls and risk decisions

SKILL SETS THAT AREN'T TAUGHT IN SCHOOLS

Long before governments began hiring hackers to strengthen their cyber security defenses, FOX-IT had already pioneered the concept. In their younger years, many Fox InTELL experts were already demonstrating their computer savvy and out-of-the-box thinking. FOX-IT is one of the few places in the world where they could channel their unguided curiosities and talents into productive careers that protect society today. For them, fighting cybercrime is not just a job but a lifelong passion.

There is no formal classroom for their skill sets, only years of computer time exploring code and researching exploits and intrusions. As the use of viruses, worms, Trojans and botnets grew, so did their expertise. At FOX-IT, their job is to infiltrate the underworld of cybercrime for surveillance, reconnaissance, counterintelligence and pre-emptive threat mitigation. 'To work here is an enormous rush,' says a Fox InTELL operative. 'We monitor so much of the dark corners of the Internet, I learn so much that almost no one else knows.'

PORTAL-BASED ACCESS TO CLIENT-SPECIFIC PROTECTION

Fox InTELL is delivered to subscribers through a secure web portal accessible from any web-capable device. Quarterly reports cover the most relevant threats and underworld trends over the last three month period. When Fox InTELL reveals an urgent threat, alerts are issued via email and RSS feed, as well as an ad hoc report via the portal to each affected client with specific information for their organization. Subscribers can follow threat evolution in real time through the portal, instead of receiving lengthy reports with delay.

For brand protection, Fox InTELL scours the Internet with its unique client-specific threat monitoring and tracking feature. Fox InTELL analysts scour the Internet looking for any appearance of the client's brand in malware configurations, command and control infrastructures, spamming emails and underworld forums. Confirmed threats are followed to see if and how they develop, while Fox InTELL's cybercrime and security experts stand ready to assist the client with appropriate countermeasures.

PORTAL-BASED COLLABORATION INCREASES PROTECTIVE AGILITY

The Fox InTELL portal includes a Collaboration area, which has proven to be an important feature for client interactions with each other as well as with Fox InTELL experts. Community discussions on new threats and countermeasures raise questions and provide answers on issues faster than intelligence reports can be generated. A Fox InTELL subscriber could well be experiencing or has experienced an identical situation and post valuable information before anyone else.

INNOVATIVE TOOLS THAT HAVE TO BE HOMEGROWN

To do their job well - the way they think the job needs to be done - Fox InTELL experts design their own stuff, such as:

- Fully automated tools to initially process the copious amounts of raw and semi-processed intelligence collected from internal and external sources
- Malware recovery tools to reverse-engineer threats and devise mitigation solutions
- Modus Operandi Engines to automatically filter all the false positives that choke a company's SIEM strategy

Innovations such as FOX-IT's DetACT for Online Banking service to stop online fraud before real damage is done and FoxCERT to rapidly mitigate data breaches and conduct follow-on digital investigations spring from applying the ingenuity of Fox InTELL experts to real-world problems.

KNOW YOUR ENEMY

Countries cannot properly defend themselves without intelligence, whether it's conventional or cyber warfare. Neither can enterprises in today's world. Fox InTELL gives InfoSec teams the precise intelligence they need to properly defend against threats that they otherwise could not see coming.

CLIENT-PREFERRED ACCESSIBILITY TO INTELLIGENCE

Fox InTELL is designed to meet each client's precise threat protection needs. Features include:

- Access to the Fox InTELL Portal
- Quarterly reports on malware and underworld developments
- A knowledgebase for ad hoc searches into information about past and ongoing threats
- Alerts and ad hoc reports for clients susceptible to a specific threat detected
- Client-specific threat monitoring and tracking
- Portal collaboration, where subscribers can share information with peers
- Access to real-time threat evolution monitoring

All of the above intelligence is organized within the portal for quick subscriber access to specific information of interest. Areas dedicated to the Knowledgebase, ongoing Live Incidents (anonymized), and Collaboration serve all subscribers. Each subscribing organization also has their own client-specific space, where confidential information can be exchanged between the client and Fox InTELL experts.

Fox InTELL delivers intelligence according to the needs of each cybersecurity stakeholder - from C-level management summaries to the raw data. InfoSec teams with the interest, time and resources can perform their own analysis, compare their findings with Fox InTELL results and even discuss methods of analysis and data interpretations with a Fox InTELL analyst.

If an actual attack is so new and unique that the threat evaded the world of cyber intelligence, Fox InTELL includes malware recovery from clients to reverse-engineer it. This feature not only speeds incident mitigation and prevents a recurrence for the affected client, but helps to protect other Fox InTELL subscribers from the same threat. In addition to all of the above, FOX-IT with FoxCERT provides the expertise to assist with mitigation and forensic investigation.

Vacant: the CCO position

Ad Scheepbouwer joined FOX-IT in October 2012 as a member of the board and as a shareholder. With his experience in the boardrooms of major exchange-listed companies, he is unrivalled in knowing just how the rabbits run there. Now it is time that sly foxes enter the boardrooms, he proposes, turning their eyes and their thoughts to cybersecurity. Where are the Chief Cybersecurity Officers?

It used to be said of generals that they were always busy with the previous war. You certainly can't say that about the cybersoldiers who protect our computer networks. It is in fact their ambition to always be a step ahead of the hackers. How might they be able to infiltrate our systems? That is the question constantly on the minds of crime-fighters, which is why they sense trouble when others still believe that everything is just hunky-dory. Distrust is second nature to them.

TRUSTING DISTRUST

Of course that is not the attitude with which most of us approach our work. I do not think a little distrust is a bad thing, and at certain times I prefer knowing for sure to trusting. Nevertheless: in my career I have particularly had to call on the latter. As someone in charge you must ultimately be able to count on the people around you: the employees, the partners and so on. I would be seriously mistaken if my fellow board members do not share that approach to the (corporate) life. To the extent that I have been able to sense the atmosphere in the boardrooms of Corporate Netherlands, it is one of trust.

You simply need to be able to assume that many things are correctly organized. So if people turn up with wild tales of cybercrime, about Mafia leaders preparing attacks from Ukraine, viruses which spread themselves rapidly and hard-disks which have become infected in China, initially the temptation is to take it all with a pinch of salt.

FATALISTIC THOUGHTS

By now many managers have realized that a hack could have dramatic consequences. However they still cannot imagine that they might also be targets. 'That won't happen to us – what are the odds?' That is probably a very normal or even natural reflex, but it is not the right reaction. An essentially correct but at the same time fatalistic thought may limp along just behind that: 'A hundred per cent secure really isn't feasible, is it? So therefore...'
And so cybersecurity is not given the attention it deserves, while the risks become greater and more plentiful thanks to the continuing growth of Internet traffic and the increasingly intensive use of mobile devices such as tablets and smartphones. We can do more with the Internet year by year, but that also makes us increasingly vulnerable. And so, for the time being, there appears to be no end in sight for the series of incidents we have recently experienced in the Netherlands: the malware on the major news portal nu.nl, the Diginotar hack, the hack of Dutch telecom provider KPN, the DDoS attacks on the websites of MasterCard and the Public Prosecutor, the Dorifel virus, etc.

Those who want peace must prepare for war

THE COMPANY'S RESPONSIBILITY

The government is not aloof from all this. At the end of last year the Dutch Lower House discussed the National Cyber Security Policy extensively and with considerable knowledge of the issues. During the debate the possibility of a 'digital fire-brigade' expressed by colleague Ronald Prins was also considered. However Minister Opstelten misses no opportunity to point out that cybersecurity is in fact the responsibility of organizations and companies. 'The government is not going to take this over from them.' So companies cannot evade it: they must take on the responsibility themselves.

TIME FOR A CCO

Right now many undertakings have accommodated the security issue somewhere within the company. For example with officials with years of experience with the police or justice systems. I believe it is important to strengthen this as soon as possible with specialists in (fighting) cybercrime. This also introduces the necessity of more focused guidance. Should cybersecurity not be at the very top of the CIO agenda? Should it not perhaps even be desirable to expand the management or the board of directors by one member? In addition to the CEO, CFO and CTO should there not also be a position for a CCO, the Chief Cybersecurity Officer? He or she could then ensure that security is high on the management agenda, and that it stays there until further notice!

It might be expected of this CCO that initially, he makes smart choices on the storage of data: the personal details (of employees and clients) and the critical company data (such as sensitive documents or intellectual property like AutoCAD drawings of innovative products). He or she will guide the IT department, but that is just one component of the job description. That is because a cybersecurity policy encompasses so much more. For instance, the CCO would also bear responsibility for awareness among employees, because if they simply use the Internet unsuspectingly and do not pay any attention to risks like phishing, then that is just mopping up with an open tap.

PURCHASING POLICY

A policy area which should also not escape his or her attention is purchasing policy. Many parties are involved in this, both internally (IT department, purchasing, marketing, sales, etc.) and externally (among others suppliers, independent consultants and experts). In an uncoordinated and impulsive purchasing policy, IT security becomes Swiss cheese. That is why it is up to the CCO to get all these interested parties along the same line and to drive the discussion. He or she needs to create the conditions in which the input of all parties can be taken into

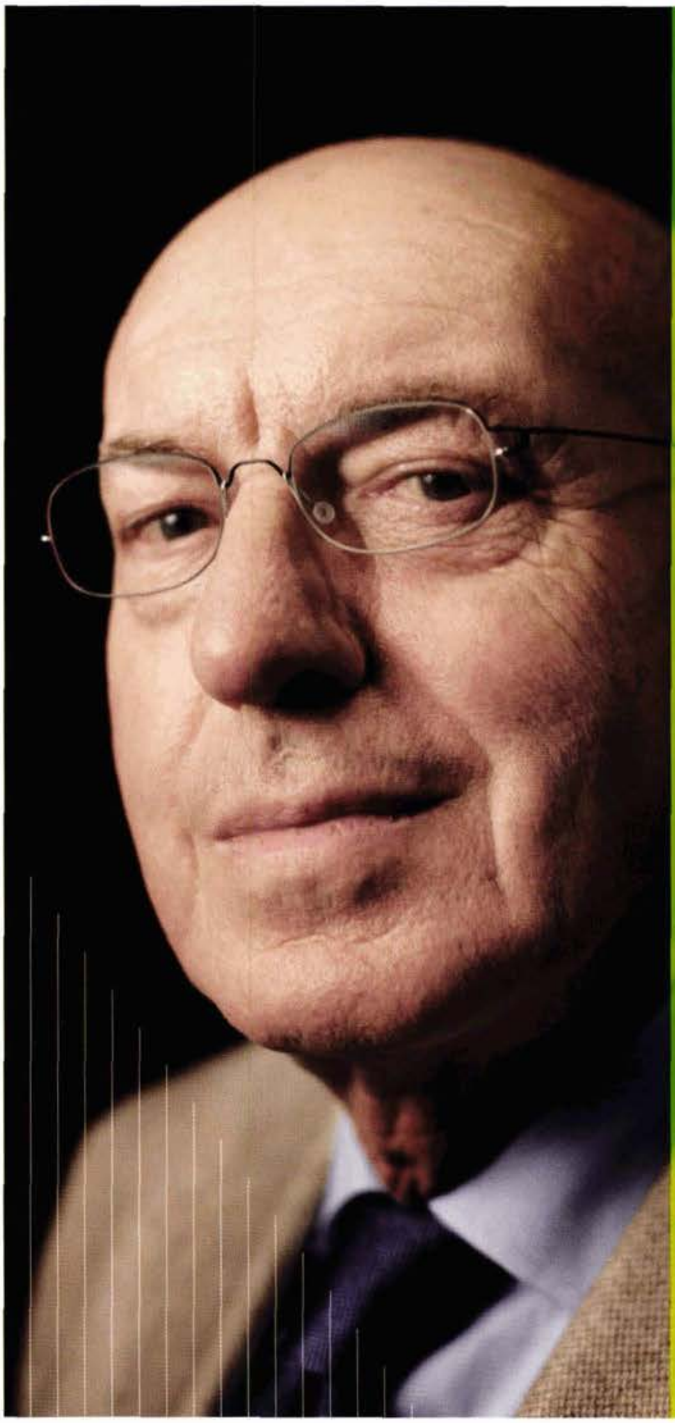
account without losing a grip on security.

CRISIS PREVENTION

In the same way that other board members monitor the price trends and sales performance of the business units, the new board member can also keep track of all the information on IT security inside and outside the company. For instance, he will have the opportunity to keep raising the security policy – or to put it better, the crisis prevention policy – to a steadily higher level.

Anyone opting to do nothing will certainly have their turn. An ancient principle is in fact more current than ever: those who want peace must prepare for war. Companies which embrace that motto can save themselves and their environment a lot of mischief. And indeed: in a timely manner they will draft in the help of the cybercrime-fighters who were appointed distrustfully because of their work, but who in fact deserve trust precisely because of it.

Ad Scheepbouwer, CEO Fox-IT



WHO IS AD SCHEEPBOUWER?

Ad Scheepbouwer (born in 1944) is a self-made top manager. He left school early, tackled every opportunity and avoided no challenge. He quickly carved out a career with various logistics companies. He gained renown from 1989, as director and CEO of PTT Post, later TNT. From 2001 he led the telecoms company KPN away from a threatened ruin following the UMTS license purchase, to an internationally respected firm. Right back in 2002 he was chosen as Topman of the Year. In May 2011 he said farewell to KPN. Since then he has made a number of investments in companies, including FOX-IT where he also became one of the three directors.

WHY DID YOU OPT FOR FOX-IT?

'When looking for investment opportunities I got into discussion with Ronald Prins and Menno van der Marel. Unfortunately cybercrime is a market which is growing strongly, and FOX-IT is ahead of the pack nationally in fighting it. The company has been growing strongly and has plenty of opportunities for further expansion. That's a favorable basis for an investment. It's also a great company to work for, with plenty of young people.'

WHAT IS IT LIKE, WORKING AMONG THE YOUNG LIONS OF FOX-IT?

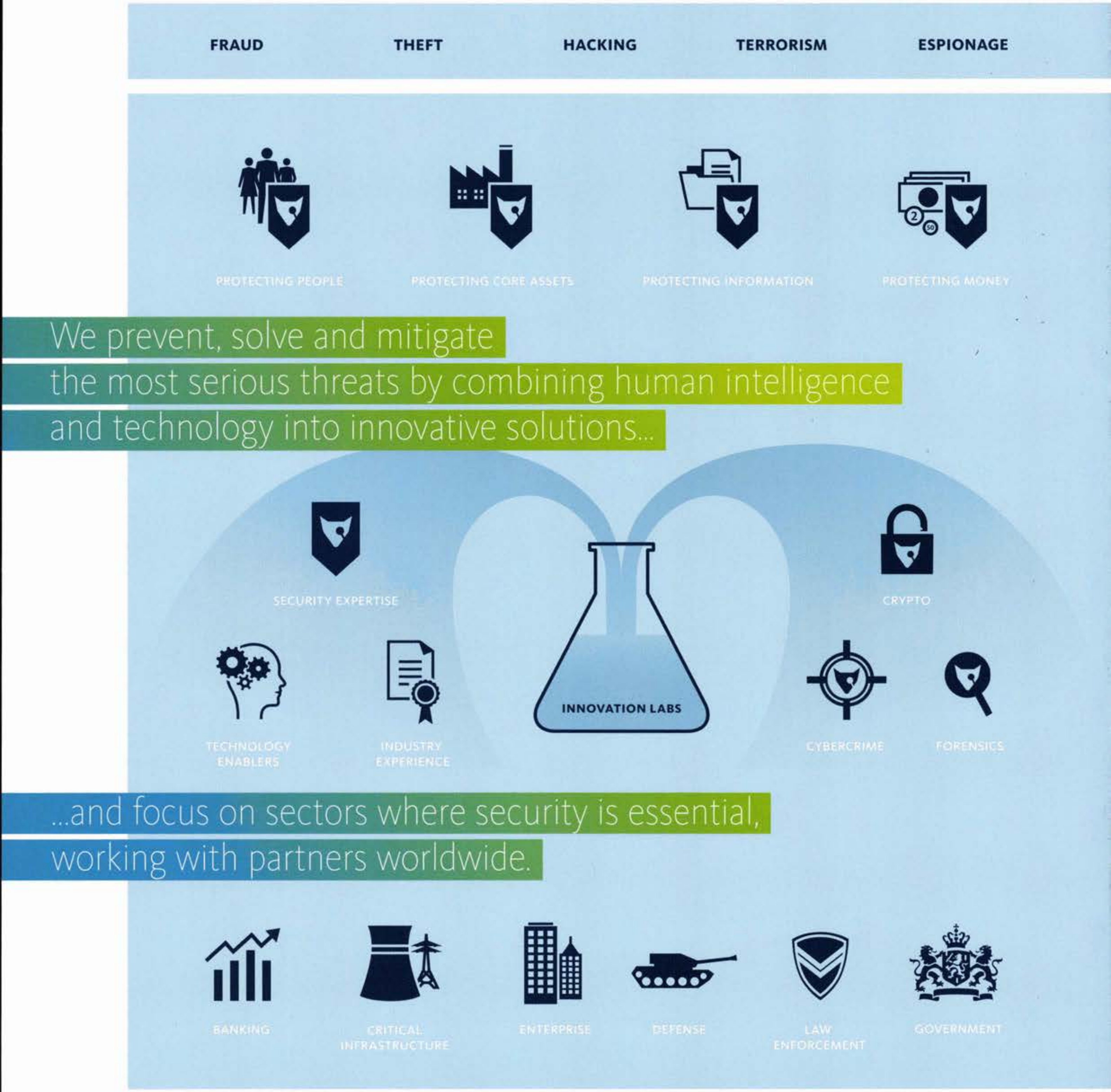
'I've always liked to work with young people. They have lots of energy, display enormous enthusiasm and are full of ambition. That attracts me. That also enables me to add another view to things.'

WHAT WILL YOU ADD TO FOX-IT?

'My challenge is to help with the company's further expansion. Growing fast brings problems with it: how do you find people, how do you safeguard the quality, how do you set up the organization, how do you fund it? I will help to manage this, with particular attention devoted to the financial side. We are also going to set up a strategy: which products and services, in which countries? What steps will we take in the years ahead? Making clear choices, not just growing. That also gives you a clear narrative for clients and employees.'

ABOUT FOX-IT

Fox-IT prevents, solves and mitigates the most serious threats as a result of cyber-attacks, fraud and data breaches with innovative solutions for government, defense, law enforcement, critical infrastructure, banking, and commercial enterprise clients worldwide. Our approach combines human intelligence and technology into innovative solutions that ensure a more secure society. We develop custom and packaged solutions that maintain the security of sensitive government systems, protect industrial control networks, defend online banking systems, and secure highly confidential data and networks.



We prevent, solve and mitigate the most serious threats by combining human intelligence and technology into innovative solutions...

...and focus on sectors where security is essential, working with partners worldwide.

A selection of products and services by FOX-IT

DETACT

DetACT prevents fraud by stopping malware, phishing and hybrid attacks on online channels. Offering real-time detection of passively monitored payment streams, it empowers Infosec teams with behavior analytics on the navigation layer, featuring unique history profiling and anomaly detection. The combination of transparent client side detection tooling and world-class cyber intelligence results in an exceptionally high detection accuracy. It's scalable and implementation neither affects the customer experience and nor the enterprise architecture.

TRACKS INSPECTOR

The volume and importance of digital information is on the rise in criminal investigations. Detectives must depend on specialists unfamiliar with their cases, to process digital information. This causes delays since there is a lack of digital forensics specialists and labs to support caseloads. Tracks Inspector offers an intuitive, web-based, collaborative and scalable solution that puts digital investigations into the hands of detectives.

FOXCERT

During a cybersecurity emergency, FoxCERT enables you to act quickly, decisively and correctly. FoxCERT provides immediate assessment and consultation, an emergency response team onsite, collaborative action aligned with your incident resolution objectives, access to Fox-IT cyber crime and digital investigation resources, assistance with PR, crisis management and law enforcement. FoxCERT is on-call 24/7 at +31 15 284 79 99.

DATADIODE

The Fox DataDiode is a unidirectional hardware device, used at the boundary of two networks. It allows data to travel - in real time - only in one direction. To protect sensitive/classified data, information is passed from a lower to a higher security network, but not vice versa. To protect critical infrastructure, information can be pushed from a trusted Industrial Control System (ICS) to an external network, while the facility remains digitally inaccessible. It's highly certified, a.o. CC EAL7+ and NATO Secret.

INTELL

If an InfoSec team doesn't know about a new cyber threat, they can't defend against it. Fox InTELL tracks and analyzes cyber threats and potential attacks in real-time as they are planned within the cybercrime underworld. Fox InTELL's portal-based service improves an enterprise's cyber intelligence position, which enables better situational awareness, security controls and risk decisions to protect their customers and their brand online. Collaboration and real-time threat tracking give Infosec teams huge advantages.

Bits

RED OCTOBER ON SMARTPHONES

In January, Kaspersky Lab published its discovery of the cyber-espionage malware virus Red October (Rocra). The attacks focused on embassies and scientific research organizations. Over the course of five years, information got stolen and networks explored by using a combination of Chinese exploits and Russian malware components. Through infected computers, Red October spread to smartphones, using Blackberry and Android operating systems. Fox InTELL did research on command and control servers and located infected smartphones across America, Africa, Asia and Europe.

DIGITAL FORENSICS ACADEMY

In digital forensic investigations, the volume and complexity of data to be examined is increasing. Globally, governmental and private organizations are struggling to find enough qualified digital forensic experts to keep up with the demand. Digital forensics is a field of rapid developments, keeping up is the challenge. FOX-IT understands these issues and can help with a complete six-week Digital Forensics Academy. This way, organizations get their less experienced staff quickly up to speed and help the experienced staff to keep up to date.

More information? See www.fox-it.com

INTERNATIONAL EVENTS

Are you coming to one of the following international events? Visit our booth for a chat and a coffee.

11 Mar 2013	Smart Grid Cyber and SCADA security Security, London, UK
12 Mar 2013	eCrime Congress, London, UK
18 Mar 2013	ICDDF, London, UK
21 Mar 2013	NextGEN SCADA, Amsterdam, NL
27 Mar 2013	Euroforensics, Istanbul, TR
22 Apr 2013	NATO NNEC, Lisbon, PT
23 Apr 2013	InfoSecurity Europe 2013, London, UK
24 Apr 2013	Expert Meeting: Using intelligence to keep ahead of online banking threats, London, UK
24 Apr 2013	Forensics Europe Expo, London, UK
01 May 2013	eCrime Congress, Dubai, UAE
19 May 2013	CEIC, Orlando, FL, USA
28 May 2013	AFCEA Technet International, Warsaw, PL
05 Jun 2013	eCrime France, Paris, FR
31 Jul 2013	OHM2013, Geestmerambacht, NL

INVESTIGATIONS ON THE INTERNET – THE BASICS

It sounds simpler than it is: investigating on the Internet. Participants in this four-day training course learn the basics of Internet Technology and a variety of methods for searching online. Many professionals, ranging from tactical detectives to information desk staff, have completed this basic training course and successfully apply their skills at work. Our trainers make the difference: they are ethical hackers and specialists in the field of digital forensics and IT security, with a teaching background. Visit fox-it.com for more information or mail training@fox-it.com

FOX-IT FIRST TO DETECT NBC.COM HACK

The Fox-IT Security Operations Centre (SOC) was the first to discover that the NBC.com website was spreading Citadel malware on February 21. Immediately NBC was informed, who mitigated the hack of the web server and stopped the drive-by download attack. A malicious iframe pointed to the exploit kit 'RedKit', which abused known Java and Adobe vulnerabilities to infect visitor's computers with a version of the Citadel Trojan. The malware is configured for stealing money from the user's accounts by manipulating online banking sessions with a number of American banks.