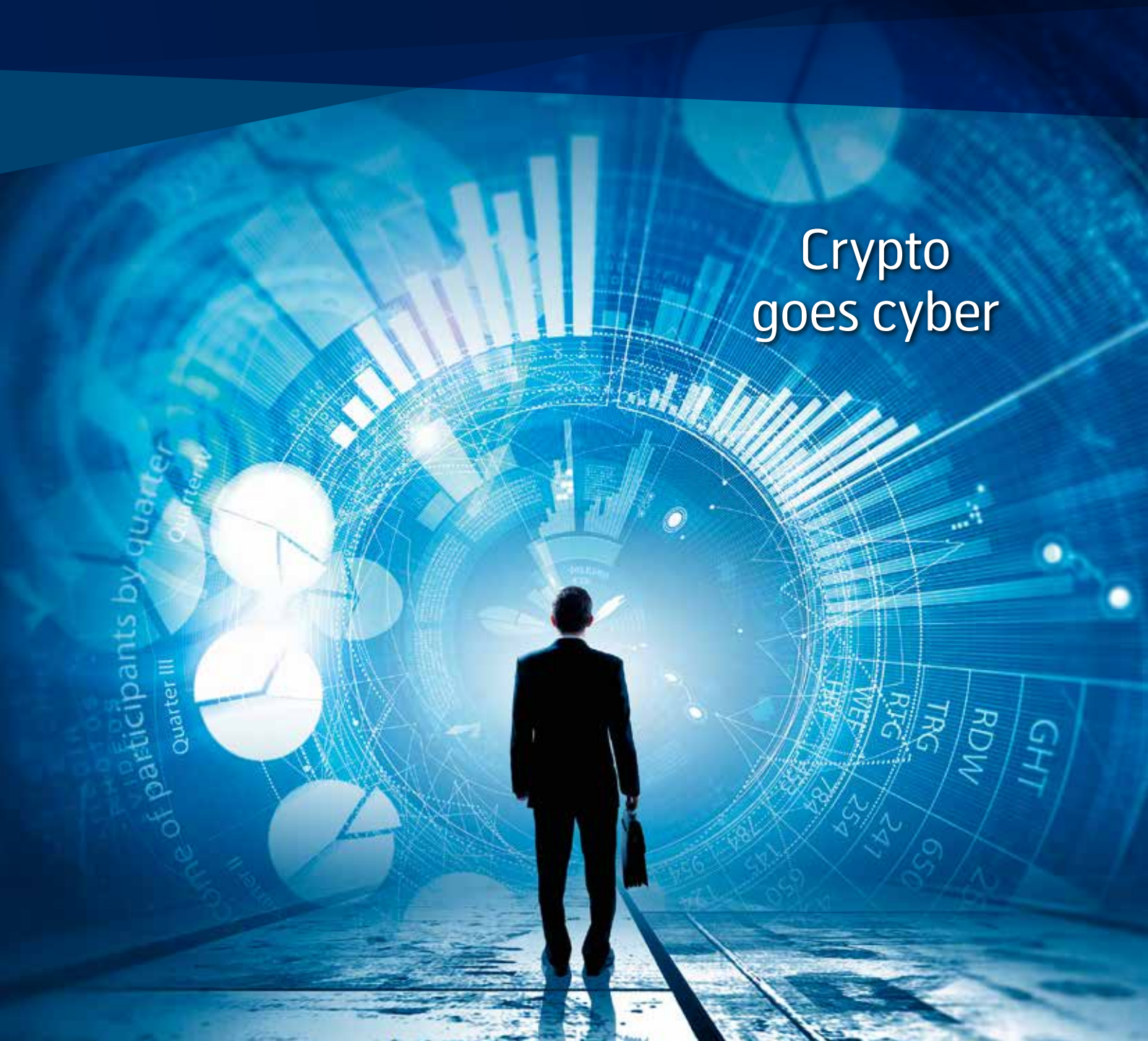
CRYPTO

CRYPTO MAGAZINE

Nº 2 | 2018



Dear Readers

Cyber threats are everywhere. In the event of an attack, sensitive information can be misused. Cybersecurity is becoming increasingly important. Therefore, the vision of Crypto is to offer holistic cybersecurity solutions to contribute to a more stable world.

As an independent supplier of cybersecurity and encryption solutions, we can use our expertise to offer advice and collaborate with our customers to develop solutions that are perfectly matched to their specific requirements.

What challenges do public authorities face within cyberspace and how can Crypto provide advice and support? Read more about this topic in this edition of CryptoMagazine.

Anders Platoff
CEO
Crypto International Group

Publication details

Published twice a year | **Print run** | 3050 (English, French, Spanish, Russian, Arabic)

Publisher | Crypto International AG, Zugerstrasse 42, 6312 Steinhausen, Switzerland, www.crypto.ch

Editor-in-chief | Tanja Dahinden, Crypto International AG, T +41 41 749 77 22, F +41 41 741 22 72, tanja.dahinden@crypto.ch

Illustrations / photo credits | Aekkaphob/Shutterstock: p. 17 | Crypto: pp. 2, 5, 19 | Shutterstock: Cover, pp. 3, 4, 6, 9, 10, 12, 14, 15, 17, 18

Crypto goes cyber

As Crypto now focuses exclusively on international operations, it can respond to its customers' needs and requirements even more effectively than it already did. The company is now strengthening the crypto offering and developing a comprehensive cybersecurity portfolio tailored to the increasingly complex cybersecurity needs of international customers.

The topic of cybersecurity is becoming increasingly important, especially in the governmental sector. Effective cybersecurity is an absolute must to preserve and protect the sovereignty, security and stability of a country. There is an increasing awareness of that, as well as of the prevalence of attacks and their likely consequences. "We are seeing rapid growth in the cybersecurity market, and our customers in the governmental sector are leading the way. It has become obvious that there is no longer any other option, cyber threats and attacks are an increasing reality and without sufficient protection against them, you will endanger the most valuable asset you have as a country – your sovereignty, your security and your stability", says Anders Platoff, CEO of the Crypto International Group.

As an independent supplier of cybersecurity and encryption solutions, Crypto uses its expertise to advise customers and work with them to develop solutions that are perfectly matched to their specific requirements in order to preserve and protect those assets. This is the company's vision.

> Crypto can provide comprehensive solutions including encryption, which is a core element in effective cybersecurity.

The uniqueness of Crypto
Crypto is the world leader in high-end information security, and has been leading the way in the related area for more than half a century. This competence, experience and customer focus makes Crypto an exceptionally strong brand. Customers trust Crypto because of their experience with Crypto's products over time. They are also aware of the unique knowledge of its longstanding staff and the effectiveness of its systems and products. Platoff is positive: "We can – in contrast to our competitors – provide comprehensive solutions including encryption, which is a core element in effective cybersecurity. We understand the technical requirements that need to be met in the governmental sector." These factors have rendered outstanding relationships with customers all over the world. With a clear and experienced management structure, in addition to a clear focus on the international market, Crypto is now delivering even better products and services.

Crypto will further strengthen its offering, and develop a comprehensive cybersecurity portfolio tailored to the increasingly complex cybersecurity needs of our international customers. The fusion of our unique high assurance expertise and cybersecurity will be highly valuable for our customers, who understand the true value of protecting their nation and citizens against attacks.

> Crypto acts as a partner to its customers, advising and assisting them in all cybersecurity and encryption matters.

Dialogue is key
Crypto is intensifying its dialogue with existing and potential customers to respond to their cybersecurity requirements more effectively and with greater agility, developing and delivering tailor-made solutions. It is essential to anticipate cybersecurity trends at an early stage and to offer our customers state-of-the-art solutions at all times.

Therefore the company is expanding both its product and service portfolio to meet customers' cybersecurity requirements more effectively. Dialogue with our customers is vital in the context of developing new solutions. Crypto acts as a partner to its customers, advising and assisting them in all cybersecurity and encryption matters. The fundamentals of the strategy are the excellent relationships and partnerships with its customers all over the world.

About Anders Platoff
Anders Platoff is the CEO of the Crypto International Group and a proven manager with extensive experience across multiple industries. Platoff started out as a fighter pilot in the Swedish Air Force. He left the Air Force in the late 1990s to join Ernst & Young Management Consulting as a manager. Thereafter leadership positions followed for several years before Platoff joined the highly successful Gaia leadership as a managing partner. He then left the management consulting firm in order to take on the role as CEO of the Crypto International Group.

As a managing partner at Gaia Leadership, he worked closely with Andreas Linde and his former management team for several years.

Anders Platoff is 50 years old, married and a father of one daughter and two sons, 20, 18 and 11 years old.

Threats in cyberspace – and how to protect against them

The list of digital threats is getting longer by the day, with professional cyber criminals subjecting global organisations to constant digital bombardment. To protect themselves, organisations must implement IT security consistently and recognise what is often the greatest weakness of any IT system: the people.

Cyberspace is the virtual space made up of every IT-networked system in the world and therefore incorporates practically all modern information and communications technology. The constant stream of new applications for information technology means that cyberspace is getting bigger by the day and is becoming increasingly interconnected with the non-virtual world. Organisations operating in cyberspace edit and store their data digitally and delegate control of their processes to software applications.

This digitalisation and networking brings enormous benefits to organisations – in terms of efficiency, for example – but it also exacerbates the very real threats they face. Although all organisations have access to comprehensive cybersecurity measures, cyber attackers are also constantly professionalising their operations. Whereas attackers often used to work alone, today they operate systematically as groups with military, political or economic motives – or a combination thereof.

Cyberattacks are one of the greatest dangers of the future.

In the World Economic Forum's Global Risks Report 2018, cyberattacks are cited alongside natural disasters as one of the greatest dangers of the future: they have a high likelihood of occurring, and the potential for damage is huge. According to the study, companies reported four billion incidents of data theft in 2016 – more than in the two previous years put together. However, the most frequent and fiercest cyberattacks are directed at governments and armed forces. These organisations are under almost constant attack because they hold highly sensitive data, which potentially relates not only to the security and sovereignty of the country but also to the private lives of its citizens. Public infrastructure is also becoming increasingly vulnerable as a result of advancing digitalisation.

The arsenal of cyber criminals

Although cyber criminals focus on organisations as a whole, attacks are often directed at employees' devices, which can serve as a "springboard" for penetrating deeper levels of the IT infrastructure. These attacks aim to exploit carelessness on the part of staff. If cyber attackers send 100 emails a year to 10,000 employees of an organisation, this corresponds to a million infiltration attempts. For the attackers, an operation of this kind requires relatively little effort. However, a single successful attempt is enough to penetrate an organisation's IT system.

Numerous methods are available to cyber attackers in order to gain access to an IT system via a device. The practice of "phishing", whose name derives from the words "password" and "fishing", seeks to obtain users' passwords by sending fake enquiries by email or short messaging service. If the attempt is successful, a cyber attacker can commit identity theft and tamper with the IT system.

An alternative approach is to smuggle in malicious software. Known as "malware" for short, these programmes are installed unwittingly by employees and then spread throughout an IT infrastructure. Until now, fake emails were a common method for deliberately spreading malware. Clicking on an inserted link or opening an attachment caused the malware to start installing in the background. However, growing awareness of suspect emails means that cyber attackers are now increasingly opting to infect websites instead. They do this by exploiting weaknesses in their security infrastructure. Simply visiting an infected website is enough to trigger the downloading of malware.

Once installed, malware often goes unnoticed for years, which is problematic for two reasons: on the one hand, it can be used to monitor and spy on an organisation. On the other hand, increasing knowledge of internal processes can be used to determine the optimum time for an attack. Malware can also be smuggled into a system using "social engineering" – and there has been a recent spate of such cases. Phone calls from people claiming to work for manufacturers of operating systems seek to convince device users that their operating system is damaged. However, the "repair software" they are supposed to download afterwards turns out to be malware.

Another method involves disrupting the availability of IT infrastructures, typically using denial-of-service (DOS) attacks. These are often expanded into distributed denial-of-service (DDOS) attacks, in which a group of computers infected with malware come together to form a "botnet" and bombard the target – a website or IT network – with requests. The target is then of only limited use – if any – to its users. Attacks involving "ransomware" have a similar purpose. Cyber attackers first smuggle the malicious software into an IT network and then block access for all other users. The system is not unlocked until the affected organisation pays a ransom. However, the data may also be lost forever.

The rapidly expanding arsenal of cyber weapons also responds to specific trends – here, the buzzword is cryptocurrencies. Since the increase in bitcoin's market value, users with crypto portfolios have also become the target of cyberattacks. An even more frequent practice is to infect computers' processors with malware so that they can be used to mine cryptocurrencies, a task that requires huge amounts of processing power.

Cyber protection: an end to compromises
IT security managers face a difficult task. They must ensure that the confidentiality, integrity and authenticity of sensitive information remain intact. Attacks should be identified promptly and appropriate countermeasures initiated. Furthermore, the security architecture should be designed so that a successful cyberattack on a device does not leave the entire IT infrastructure exposed. However, it is also important to take devices – as high-risk gateways into an IT system – out of the line of fire by ensuring their comprehensive protection. To this end, it must be ensured that employees understand all of the cybersecurity measures and apply them correctly.

> The security architecture should be designed so that a successful cyberattack on a device does not leave the entire IT infrastructure exposed.

Until now, this task often presented IT security managers with a dilemma: comprehensive cybersecurity required protection measures that also influenced staff's digital working environment, such as the frequent entering and regular changing of passwords. However, an organisation's success is dependent on fast access to information and the ability to edit and share it efficiently. If complex security measures make access more difficult, employees will not implement these measures adequately or may even bypass them altogether, leading to a greater risk of attacks. Previously, physical separation of public and protected IT systems was the only secure solution. However, it is neither efficient nor user-friendly for staff to use separate laptops or PCs.

Highly secure working in a familiar IT environment
This "convenience or security" dilemma can easily be overcome with the technology provided by Crypto. Tailor-made combinations of software and hardware components provide comprehensive protection against cyberattacks and can be integrated into existing user environments. The Crypto SmartProtect computing platform allows highly secure working in a familiar IT setup and on a single device thanks to its isolated Compartments. It allows the user to edit and share data with different levels of security simultaneously, enabling efficient and convenient working in a familiar user environment.

A click of the mouse is all it takes to switch between the protected and public user environments. The cryptographic protection measures operate unnoticed in the background. Crypto SmartProtect can be deployed on both stationary and mobile devices and therefore responds to the needs of many organisations to ensure secure location-independent access to data at all times. In addition, the computing platform can be used both as a non-networked stand-alone device and as a component in a complex system.

Crypto SmartProtect makes working with sensitive information not only highly secure but also efficient and convenient. This unique combination is only possible because the technology's security elements are all perfectly matched to one another. Thanks to an impenetrable security barrier, users are protected against cyberattacks at all times and can concentrate on their work with confidence. In view of the growing number of devices worldwide, particularly in the mobile sector, it is also important to incorporate privately used devices into the cybersecurity architecture of governmental organisations. This neutralises even the tiniest "springboards" that attackers can use to gain access to an IT system.

> It is important to know what is going on in the dedicated network and thus to prevent, detect, analyse and respond to cybersecurity incidents.

> Crypto SmartProtect makes working with sensitive information not only highly secure but also efficient and convenient.

In addition to prevention, increasing importance is also attached to the continuous monitoring of IT systems. Their automated monitoring in real time is essential for the collection and correlation of data and for triggering a response to attacks, and is therefore a key factor in averting cyberattacks. Monitoring identifies suspicious patterns in the data streams and detects attacks at an early stage.

Cybersecurity requires not only ICT security walls but also more intensive monitoring of security systems and the early detection of attacks. In this context, detection is paramount – and Crypto is the ideal partner for this challenge.

Hardware protects software

Protection mechanisms in software cannot provide sufficient information security. Reliable encryption must be based on hardware components. These modules are also characterised by their compatibility and durability.

Software is an all-purpose weapon in the world of information technology. Nowadays, almost every workplace activity can be supported – or in some cases completely replaced – by intelligent software. Programmes are constantly advancing into other areas and taking on control functions. Just as personal fitness programmes are now software-based, so too are some monitoring tasks in infrastructure facilities such as nuclear power plants, for example. Regular updates ensure that software is optimised and adapted as necessary. However, when it comes to the security of information technology, the focus shifts to another element: hardware modules. Indeed, hardware components are explicitly required by international cybersecurity standards such as ISO/IEC 19790 for a higher level of security.

People as risk factors

However versatile software may be, it represents the Achilles' heel in the security of IT infrastructure. This is because computer programmes that are intended for mass use, such as word processing software, must meet two key conditions in order to be successful: speed and ease of use. To this end, programmers incorporate shortcuts into their command protocols. These are often accompanied by compromises in terms of security as they expand the range of potential target spaces and provide gateways for cyber attackers to exploit. Attacks are carried out in a targeted manner, for example by implanting malware into the system. This is often done using "drive-by exploits": when a user visits a specially prepared (counterfeit) website, malware is downloaded automatically in the background – and the attack goes unnoticed.

The software industry is conscious of these dangers, and a number of software-based applications promise protection against cyberattacks. However, these applications themselves suffer from numerous vulnerabilities and can be infiltrated by cyber attackers. This often involves exploiting human weaknesses – including, for example, the careless use of passwords, which are sometimes stored in unencrypted documents. In many cases, access codes are also changed infrequently – a big mistake! Moreover, there is also a risk of cyber espionage using sensors: here, a device's microphone is activated specifically in order to eavesdrop on and record the access code entered on the keypad.

Secure encryption has to be based on hardware components. Organisations working with sensitive data at different classification levels must protect this with absolute certainty if they wish to safeguard the integrity, authenticity, confidentiality and availability of their data. Hardware components therefore represent an indispensable element of cybersecurity. In hardware-based encryption and decryption units, the cryptographic calculations are performed in a protected environment inside the hardware. Neither the encryption method nor the keys can be tampered with by software applications, malware or people.

Only hardware modules are able to generate secure keys, which must be totally random and changed on a regular basis. Even if an attacker can break into the operating system or the software applications, the keys and cryptographic parameters and calculations remain fully protected inside the hardware. This can also be "hardened" using hardware modules that regularly check whether software has been infiltrated. If this is the case, countermeasures are initiated immediately, such as by sending an alert or even forcing a system stoppage.

> Organisations working with sensitive data at different classification levels must protect this with absolute certainty if they wish to safeguard the integrity, authenticity, confidentiality and availability of their data.

Even if an attacker can break into the software applications, the keys and cryptographic parameters and calculations remain fully protected inside the hardware.

The combination is crucial

There are various ways to implement hardware into an IT system: on add-on cards for a PC, on single-chip processors, or in stand-alone devices with a single IT-related application, such as network encryption. A further advantage of hardware components is their speed. In addition, hardware modules can be used for decades – even as the software applications they protect continue to evolve.

Hardware modules ultimately represent a static security measure as part of an overall cybersecurity strategy. However, an intelligent IT security system can call upon not only defensive measures but also preventive and offensive capabilities. It spots attacks at an early stage, tracks and destroys malware within the system, and entices attackers with so-called "honeypots": as seemingly easy prey, these simulated IT infrastructures lure in cyber attackers and then collect information about them while the actual IT infrastructure remains protected. Software forms an essential part of these capabilities. For effective protection against cyberattacks, therefore, the combination is crucial – but hardware remains indispensable.

Cyber warfare: conflicts in the fifth dimension

Cybersecurity is an absolute must to preserve and protect the sovereignty, security and stability of a country.

There is a tendency in information societies for all players to be totally networked with each other digitally. Organisations, both private and governmental, therefore face the huge challenge of protecting their infrastructures and particularly their strategic knowledge from daily cyberspace attacks, one of the most serious threats to national security today.

Conflicts in the future will increasingly be waged in the worldwide data networks, detached from any geopolitical borders. Warfare no longer revolves exclusively around the conventional dimensions of land, sea, air and outer space. Indeed, cyberspace has been added as a new component to the combat zone. In this new logic of asymmetrical warfare, the comparatively clear-cut distinction between the military sphere and the civilian sphere has lost its validity. It is not at all rare for cyberattacks to be launched by civilians with no actual power status, who operate covertly and strike anonymously.

The new digital forms of warfare are highly complex and multifaceted because information and communication technologies are constantly advancing and with them the range of potential attack possibilities. Of course, not every cyber activity carried out with the intent to do harm is akin to an act of war. On the less dangerous end of the spectrum are harmless attacks by individual criminal hackers devoid of political, ideological or strategic aspirations, e. g. entailing phishing or social engineering to obtain credit card numbers. However, beyond this, there are various kinds of attacks that can cause major damage to an economy and seriously endanger the security of the population. This category includes denial-of-service attacks such as the often cited ones launched from a botnet against Estonia in 2007 that paralysed the entire country. Attacks of this kind have a painful effect on public life or involve infiltrating other people's operating systems by means of malware with an eye to manipulating or even destroying an entire infrastructure.

Critical infrastructure is an especially endangered target of cyberattacks because supervisory control and data acquisition (SCADA) systems are centrally organised in most cases and depend on high-tech networks. Although these attacks do not involve physical violence but are carried out instead by planted malware such as Stuxnet, Duqu or Flame, the damage they do is nonetheless horrific.

The defence sector is also extensively confronted with massive cyberattacks as various armed forces continue their visible efforts worldwide to deploy the tactical Internet for network enabled operations.

Legal situation still not clarified

The law of war consists of the internationally applicable principles "ius ad bellum" (acceptable justifications to wage war) and "ius in bello" (limits to acceptable wartime conduct). Experts in international law around the globe are wrestling with the urgent question of whether these principles apply to cyber warfare and to the current basic situation with its implicit changes. The focus is on massive attacks that go far beyond the usual Internet crime being prosecuted under criminal law. This discussion is thus clearly associated with a number of

questions that are difficult to answer: What criteria have to be met to have a cyberattack be considered an act of war justifying a military retaliation? Is a conventional military response a reasonable and legitimate course of action and one on which consensus can be reached? To exacerbate matters, it is complicated to identify the attackers and their motivation quickly and unequivocally and to assess possible diffuse consequences of the attacks. And not least, politics and policy play a role, not just technical aspects. How should a country defend itself against a cyberattack verifiably brought about by another country without endangering economic relations, for example?

NATO commissions research on precisely these kinds of issues at its Cooperative Cyber Defence Centre of Excellence. They were the subject of the "Tallinn Manual on the International Law Applicable to Cyber Warfare". The manual is controversial because critics say it sets the hurdles for a military response too low. The nearly 100 rules in the manual are intended as a guide for member states of the NATO alliance and are not legally binding. Tallinn 2.0 was released in February 2017 and is designed to expand the scope of the Tallinn Manual.

In recent years, a massive build-up of capacities in the fight against cyber warfare has been observed in the form of national cyber defence centres.

> The new digital forms of warfare are highly complex and multi-faceted because information and communication technologies are constantly advancing and with them the range of potential attack.

A massive build-up of capacities in the fight against cyber warfare has been observed in recent years in the form of national cyber defence centres. Nearly every European country now has a computer emergency response team (CERT) and a national cyber defence strategy aimed at being able to protect the national infrastructure from cyberattacks. Certain countries such as the United States and Germany also rely on offensive defence that does not preclude the possibility of actively attacking an adversary's networks.

The national guidelines must be consolidated based on a comprehensive international cybersecurity policy and aligned with each other. There is close international cooperation in Europe, for instance, on devising joint strategies and policies. The European Union Agency for Network and Information

It is difficult to define what criteria have to be met to have a cyberattack be considered an act of war justifying a military retaliation.

Security (ENISA) assists member states of the European Union with developing and implementing strategies of this kind and also with sharing expertise.

Ultimately, governmental and military organisations as well as private businesses are called upon at organisational level to tackle the issue of protecting their infrastructure from cyberspace attacks. To analyse a given threat situation, technical experts employ what they call honeypots, i. e. systems intentionally configured to be insecure. They give the impression of being real control systems in order to lure potential attackers, whose attacks are then recorded and evaluated.

The Organisation for Security and Co-operation in Europe (OSCE) issued a "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace" in 2013. This comprehensive framework contains strategic measures to protect critical infrastructure from cyberattacks and to counter possible attacks proactively. Most of the procedures described in it are also certainly relevant to other organisations with high protection requirements. The guide points out a need for action in three areas among others, calling for cybersecurity to be defined as an integral part of specific risk management, for security standards to be improved and for investments to be made in sensitising employees.

The OSCE framework also considers the use of cryptography to be one of the good practices for improving cybersecurity and for protecting higher security zones. The use of hardware-based encryption and a proprietary algorithm can thwart especially perfidious cyberattacks involving activities such as infiltrating and spying on computer networks by means of masquerading, manipulating and eavesdropping on classified data and planting malware. The confidentiality, authenticity and integrity of the data warranting protection are always ensured in this approach. The OSCE plays a major role in this topic and is working on implementing UN guidance with groups of governmental experts.

The UN – a textbook example of cybersecurity

It is not only states and armed forces that are dependent on highly secure communication channels. International organisations such as the United Nations (UN) also represent potential targets for cyberattacks. In addition, the UN acts as a global discussion platform for new threat scenarios.

The task of making the world a more peaceful place is anything but straightforward, and negotiations between parties involved in a conflict often drag on for many months or years. The UN frequently plays a central role as a mediator in such talks. As a neutral party, it is tasked with listening to the parties to a conflict, communicating proposals and offers, and conveying counteroffers until both sides come to the table and, ideally, reach an agreement.

In the early stages of negotiations, UN mediators are often required to engage in open discussions with the various parties – either in person or by telephone. This is only possible if the parties can be certain that the UN will ensure the security, confidentiality and integrity of information entrusted to it at all times. A breach of information security would lead to an almost irreparable loss of trust. Peace talks would be discontinued if either party suspected that the opposite side was eavesdropping on their discussions with the mediator.

The technological capabilities now exist to listen in on confidential discussions, and the use of such technology cannot be ruled out even in conflicts between parties with limited financial resources. For example, this may be facilitated by friendly relations between one party and a great power that is sympathetic to its cause.

Over 110,000 peacekeepers

Political negotiations are not the only area in which the UN is dependent on highly secure communication channels. The same is true of the organisation's peacekeeping missions. At present, over 110,000 "peacekeepers" are deployed on behalf of the UN in around a dozen conflict areas. These peacekeepers include Blue Helmets from numerous countries, as well as police officers and civilians. Areas of deployment include conflicts centred in the Middle East, which make headlines on an almost daily basis. However, the organisation also maintains a presence in crisis areas such as Kosovo, which has largely disappeared from media coverage almost 20 years since the war ended. UN troops have been stationed for an even longer time in India and Pakistan (since 1949) and in Cyprus (since 1964). The list of completed missions now includes deployments in numerous civil wars, such as in Angola, Yugoslavia, Rwanda or East Timor, and UN peacekeeping forces have attended to over 70 missions in total. The UN's missions can incorporate a variety of tasks, such as delivering humanitarian aid, monitoring ceasefire agreements, and disarming rival factions in civil wars. Furthermore, the UN is able to set up Commissions of Inquiry in conflict areas, mediate in the field, establish buffer zones, and supervise conditions and sanctions.

Deployment is not without risks

A UN peacekeeping mission requires the approval not only of the countries in which it will take place but also of all parties to the conflict. The aim is to prevent UN troops from getting caught in the crossfire. Nevertheless, Blue Helmets carry weapons and are permitted to use them in certain circumstances – in particular for self-defence. It is clear from these safety precautions that peacekeeping missions are often risky and dangerous. Especially in the field, it is therefore essential to ensure effective and tap-proof communication channels – just as for regular armed forces. This is the only way to protect UN soldiers and to ensure the credibility and neutrality of peace brokers.

> The topic of cybersecurity is not only of concern to the UN in the context of its peace talks and peacekeeping missions. The organisation also acts as a global platform for discussing these issues at the multilateral level.

However, the topic of cybersecurity is not only of concern to the UN in the context of its peace talks and peacekeeping missions. The organisation also acts as a global platform for discussing these issues at the multilateral level. For Laura Crespo, who conducts research for the Swiss Cybersecurity Advisory and Research Group (SCARG), this is one of the UN's core tasks. "After all, cyberattacks that threaten international stability and peace represent a serious and steadily growing threat," she says. According to Crespo, the UN is primarily concerned with attacks that could have grave consequences in terms of the functioning of entire countries, including attacks with state backing and those targeting key infrastructure, for example.

At present, over 110,000 representatives of peacekeeping missions are deployed on behalf of the UN in around a dozen conflict areas.

Sound expertise in cybersecurity

The UN has been addressing cybersecurity for more than 20 years – since long before it became a topic of public debate. In particular, the Office for Disarmament Affairs (UN ODA) has gained in-depth expertise in this area. In concrete terms, so-called UN Groups of Governmental Experts – expert groups made up of different states – have already been convened on five occasions. Three cases led to a final report, while the other two groups failed to reach a consensus. The report by the Expert Group that met in 2014 and 2015 is considered a particular milestone. This called on states to adopt cyber defence measures, classify attacks and forge partnerships with other states. For example, specific proposals included that states exchange information on instances of cyberattacks.

Crespo emphasises that, so far, member states remain solely responsible for their own cybersecurity, although efforts are under way to create a Computer Emergency Response Team (CERT) – that is, a permanent group of experts in relation to cybersecurity – at the UN level. The cybersecurity expert is convinced that "this would also improve the organisation's technical defensive capabilities". However, she still believes that the UN's primary role is to sensitise states to the topic and motivate them to accumulate knowledge in order to counter this type of threat. After all, she is certain of one thing: "When it comes to the issue of cybersecurity, not all states have reached the same level of awareness."

SUCCESS STORY

Highly secure satellite network for global command support

Whether in strategic or operational / tactical applications, secure satellite links allow reliable and highly secure communication at all times, even in environments without adequate terrestrial communication infrastructure, meeting the needs of armed forces for total autonomy, mobility and security as well as ensuring global command support.

In principle, satellite links involve disseminating information over areas spanning entire regions of the world. Secure encryption is the only reliable way to protect sensitive information against eavesdropping or even tampering.

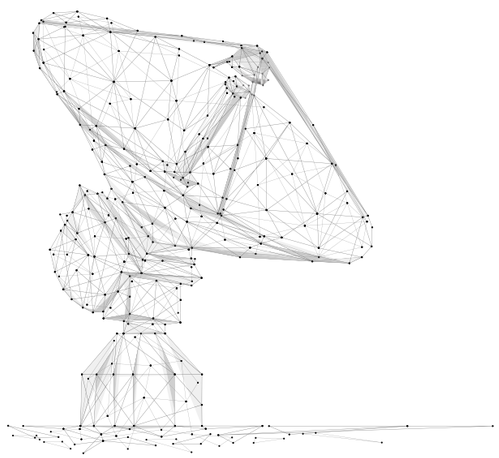
Accordingly, governmental organisations such as a foreign ministry or ministry of defence, for example, have comprehensive and extremely stringent requirements for a global satellite network. For example, highly secure connectivity must be ensured for stationary participants at all times. It is also essential to use universal technology for transmitting different services such as voice, video or data. Moreover, centralised security management is needed in order to ensure the effective administration of communication relations and user groups.

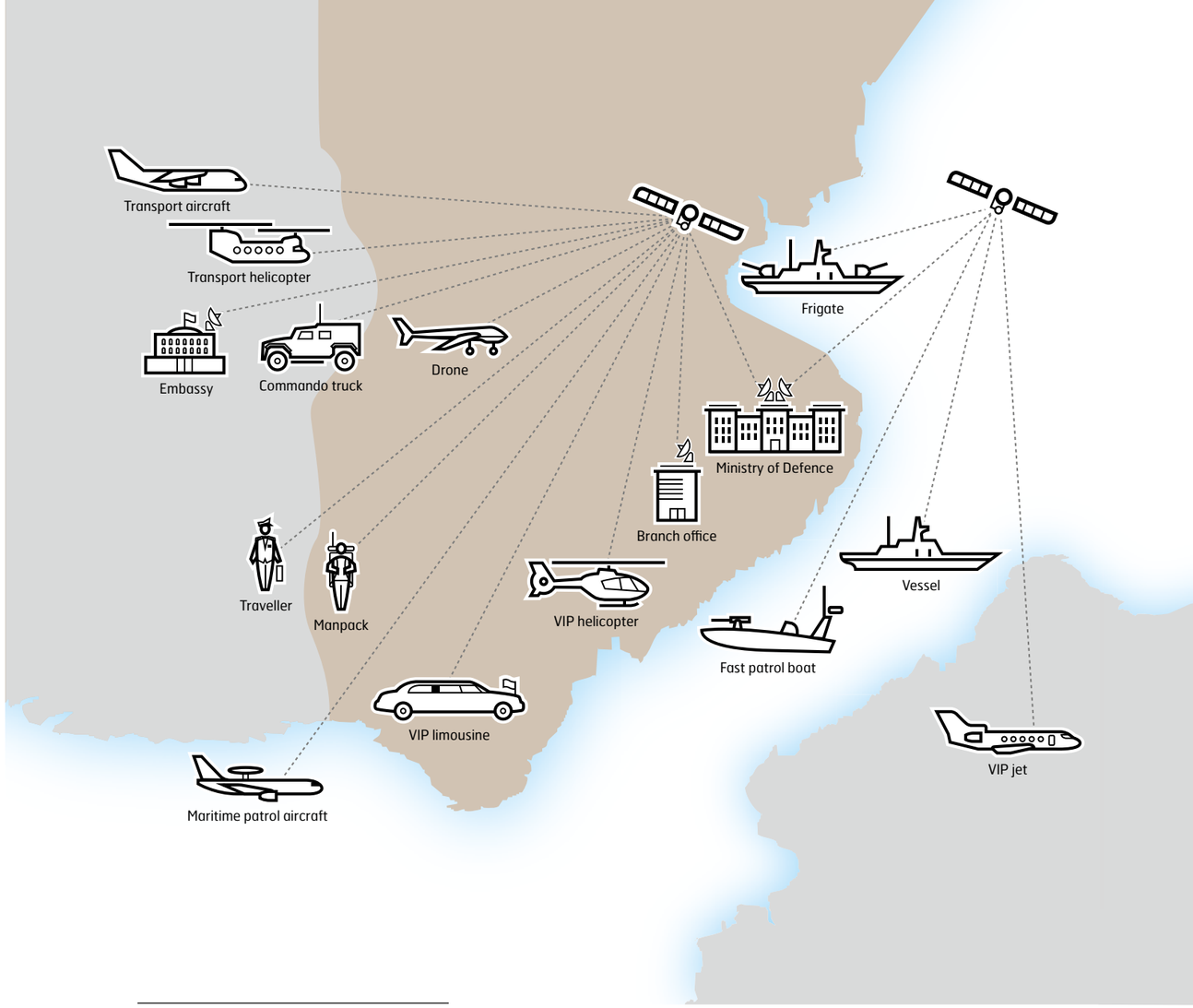
Flexible scalability and universal networking
In order to meet the catalogue of requirements and provide the customer with a comprehensive and highly secure solution, an IP-based satellite network was implemented with a view to delivering command support to armed forces leadership at the strategic, operational and tactical level. Ultimately, the IP VPN encryption solution from Crypto was integrated into the current satellite network infrastructure, incorporating the existing Network Operation Centre (NOC) and Security Operation Centre (SOC) for monitoring and operational purposes. IP VPN encryption solutions from Crypto ensure that the confidentiality, authenticity and integrity of information are protected at all times on a global basis.

> Successful command support thanks to maximum autonomy and total information security.

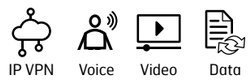
The installed solution allows the customer to scale both the network and the bandwidths and therefore to adapt these flexibly to the different deployment scenarios in the field. Furthermore, the customer enjoys access to tailor-made user and authorisation management, including the definition of communication groups. Cryptographic parameters are created and administered – both offline and online – using the centralised Security Management Centre SMC-1100. The customer therefore has an encrypted satellite network extending across all strategically important parts of the world.

With its IP VPN encryption solutions, Crypto provides highly effective protection for all common technologies in the information networks of today. Crypto's experts ensure comprehensive knowledge transfer to the local system administrators and offer a wide range of testing and training services at the Crypto Academy.





A satellite network with highly secure encryption extends across all strategically important parts of the world.



Highly secure, constant connectivity

Independent operation
The entire satellite network, which covers almost every part of the world, can be operated autonomously by the local system administrators, who act as service providers to the users.

Total security
Crypto's unique security architecture safeguards the confidentiality, integrity and availability of sensitive information – the information cannot be utilised by third parties, and any tampering is detected, logged and eliminated immediately.

Constant availability
The secure satellite network ensures constant availability and fail-safeness.

Crypto International AG
Zugerstrasse 42
6312 Steinhausen
Switzerland
T +41 41 749 77 22
F +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch