

 CRYPTO

CRYPTO MAGAZINE

N° 2 | 2017



Digital transformation in the context
of Information Security

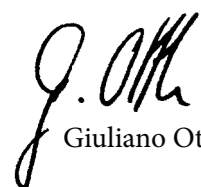


Dear Readers

The digital world has us firmly in its grasp. Many tasks call for electronic services and have become inconceivable without them. Neither companies nor governments nor public authorities can isolate themselves from these changes, as processes and procedures are in a state of constant flux in the age of digital transformation.

The digital working environment is placing new requirements on communication technologies, bringing Information Security to the fore and presenting increasingly complex challenges for IT managers. Consistent separation is the right approach to ensure that staff can handle sensitive information securely at all times.

cOffice Workplace – based on Crypto SmartProtect technology – meets these requirements and therefore provides cyber defence at the highest level. The HC-9400 Officebook is a smart device for employees and acts as the high-security component of cOffice Workplace. You will find more information on these topics in this edition of CryptoMagazine.


Giuliano Otth

President and
Chief Executive Officer

3 | FOCUS

A whirlwind revolution – digital transformation in full swing

6 | INTERVIEW

Interview with Prof. Dr. Andreas Wenger, Director of the Center for Security Studies (CSS) at ETH Zurich

9 | Risks in the digital workplace

13 | Target device – cOffice Workplace offers uncompromising protection

16 | Digital warfare: the beginning of an era

19 | E-government: towards a digital state

20 | SUCCESS STORY

Information Security concept for secure e-government

22 | How dark actually is the Darknet?

Publication details

Published twice a year | **Print run** | 3,750 (German, English, French, Spanish, Russian, Arabic)

Publisher | Crypto AG, P.O. Box 460, 6301 Zug, Switzerland, www.crypto.ch

Editor-in-chief | Anita von Wyl, Crypto AG, T +41 41 749 77 22, F +41 41 741 22 72, anita.vonwyl@crypto.ch

Reproduction | Free of charge with the consent of the editorial office. Courtesy copies requested. Copyright by Crypto AG

Illustrations / photo credits | Crypto AG: pp. 2, 15 | Prof. Dr. Andreas Wenger: p. 7 | Shutterstock: Cover, pp. 3, 4, 8, 9, 10, 13, 18, 22



A whirlwind revolution – digital transformation in full swing

Digitisation will stop at nothing: everything that can be digitised will be digitised and interconnected. Driven by innovative technologies, it opens up new possibilities that have the potential to bring about fundamental changes in society, the economy, public authorities and organisations. The digital revolution is under way and its outcome remains uncertain, but there is no doubt that digitisation also comes with a new set of security risks.

The world is undergoing a drastic transformation. It is already impossible for companies, public authorities or organisations to make do without IT. However, the rapidly increasing use of digital technologies on a widespread basis brings far more wider-ranging changes than simply the greater penetration of IT into all areas of life. Indeed, in many areas, digitisation is bringing about structural change. Although this change is characterised by unlimited possibilities, it also calls for a rethink, as well as a process of transformation within organisations, processes and working cultures.

Digitisation is taking hold at a rapid pace

A look at the world of business illustrates what significant changes digitisation has already produced in certain sectors.

According to Forbes (2015), six of the ten highest-value companies, based on their stock market value, are IT or IT-based companies. Purely digital companies such as Facebook or Alibaba have established themselves on the market in record time. Facebook, the most popular media company in the world today, produces no content of its own. Alibaba, the largest retailer in the world, has no stock. Yet both pose a threat, with their online-only business concepts, to the "traditional" business models of established market players.

This transformation benefits those who pursue a coherent digital strategy from an early stage, for there can be no doubt that digitisation is more than just a passing fad. On the contrary, digitisation is increasing at an exponential rate.



New information technologies are being adopted and applied at a rapid pace. By way of comparison, it took radio 38 years to achieve an audience of 50 million people. For TV, it took 13 years. For online media such as Facebook or Twitter, it took less than 12 months to bring the same number of people on board.¹ Moreover, the willingness of society to adopt technical innovations is greater than ever before. Whereas the proportion of people who used a mobile phone was just 1% of the world's population in 1995, this figure had risen to 73% by 2014.

Key drivers of digital transformation

The launch of the computer in the 1950s and 1960s marked the starting point for the developments we are seeing today. Since then, data processing – or information technology – has crept inexorably into almost every area of life. Its objective: to automate processes and make them more efficient. And, if anything, the phenomenon is on the increase, fuelled by constant technological development. Within this process of evolution, there are five emergent technological trends that will profoundly influence the "digital revolution"; although their impact is almost impossible to predict today, studies suggest they will contribute USD 1.36 trillion to global GDP by the year 2020²:

- Mobile technologies, which provide access to information and therefore allow people to interact or make decisions anywhere and at any time

- Social media, which transform interaction within peer groups
- Analytics and big data, which allow people to make sound decisions in real time and to develop scenarios based on actual data
- Cloud computing technologies, which provide flexible access to applications and data (on favourable financial terms)
- The "Internet of Things", which offers almost unlimited opportunities for interaction through the smart networking of autonomously controlled objects. These objects are constantly evolving thanks to new discoveries in the field of artificial intelligence (AI)

Driven by the exponential increase in processing power and the availability of huge volumes of data, considerable progress has already been made in the field of AI. Many of these algorithms learn from data traces left behind in the digital world, leading to new forms of "machine learning" and fully automated discovery that allow "intelligent" robots – so-called chatbots – and computers to program themselves and to make decisions in a matter of seconds based on defined basic principles.

All of these new developments and technologies have one thing in common: they take advantage of the pervasive power of digitisation and information technology. In this respect, the individual trends are closely interrelated. However, this intensive use of technology in a "hyperconnected world" is

also accompanied by a great many risks. When the technology fails, it tends to result in serious damage and, hence, to heightened security risks – especially for governments and other organisations.

Digital risks for states and organisations

As technologies continue to merge, along with the reciprocal learning processes of governmental and non-governmental players, the nature of security threats is undergoing a profound change. Vulnerability is generally increasing. Cyberspace is becoming another theatre of war, just as land, sea and air have been in the past. Parties to future conflicts will seek to disrupt, confuse or deactivate their adversary's sensors, communications and decision-making capabilities. In this respect, the battle for "information superiority" will emerge as one of the principal means of future military, political and economic clashes. The transformation of the armed forces will be dependent on robust, confidential, stable and comprehensive networking, as well as extensive information sharing and network-oriented investment.

Public authorities also see themselves as duty-bound: the trend towards gathering, collecting and storing extremely sensitive personal data and providing access to it in centralised databases heightens the risk of an attack on data collections of this kind, which are therefore seen to be in extreme danger in terms of their integrity and availability. Cyberattacks on the data held by

the European Central Bank (ECB) and on other organisations with high security standards have demonstrated just how vital it is to have effective security concepts in place in order to tackle such threats.

When the technology fails, it tends to result in serious damage.

IT security is a top priority

Data is said to be the raw material of the 21st century, and it is important to protect this raw material against unauthorised access, as companies, public authorities and institutions are especially vulnerable to the dangers of cyberattacks because of their extensive reliance on IT. Data and Information Security, as well as data protection, are therefore a matter of existential importance. Particular attention must be paid to the way that sensitive data is handled.

From the point of view of IT organisation, digital transformation presents challenges on various levels: first of all, it is important to keep pace with technological progress. However, questions about suitable architectures are also crucial, as IT innovations – especially those that require integration into the existing IT landscape – are easier to realise if existing architectures are designed to be flexible, modular and elastic. In many cases, this goes against the status quo, as today's Security Architectures have been built up historically and therefore tend to be highly complex. Cascades of firewalls and antivirus software are just as important here as demilitarised zones (DMZ) and inner and outer lines of defence. In this context, a network cannot trust another network unless it has at least the same level of security. Against this backdrop, the role of the IT security manager in particular is becoming increasingly important in the age of digital transformation.

Sources:

¹ https://www.mckinsey.de/files/Social_Media_Brochure_Turning_buzz_into_gold.pdf (accessed: 3 April 2017)

² <https://www.forbes.com/sites/joemckendrick/2015/03/17/digital-technologies-will-soon-add-1-trillion-plus-to-global-economy/#d49feb521b85> (accessed: 3 April 2017)

"There is virtually no political or military conflict these days that doesn't also have a significant cyber component"

The Center for Security Studies (CSS) at ETH Zurich is a centre of competence for Swiss and international security policy. Prof. Dr. Andreas Wenger is Director of the CSS and provides comprehensive information on trends relating to digital transformation in the context of Information Security.

Digitisation is steadily forging ahead. Looking back, which developments were particularly important from a security policy perspective?

The commercialisation of the Internet in the 1990s led to a sudden expansion of cyberspace. This was accompanied by a similarly rapid increase in the social and economic importance of technologies that had actually been created for a different purpose. However, it soon became clear that cyberspace was fundamentally insecure and that the market did not ensure adequate security. As a result, governments increasingly began to grapple with cyber crime and cyber sabotage. Initially, governments focused their efforts on prosecuting cyber crime and protecting critical infrastructure, although this, in turn, could only be guaranteed by working hand in hand with the private sector.

What new threats have come to the fore in recent years from a security policy perspective?

In the last few years, cyber conflicts have taken on a strongly political and military aspect. Since STUXNET, i.e. the malware attacks on monitoring and control systems in the context of Iran's nuclear programme in 2010, the sabotage of critical infrastructure using cyberattacks is no longer a fictional scenario. The Arab Spring of the same year demonstrated that both public protest and state repression now increasingly take place over the Internet. The Snowden affair of 2013 underlined how widespread the practice of state espionage has become in cyberspace. The war in Ukraine in 2014 made it clear that cyberattacks are now an integral part of operations by armed forces and intelligence services. In parallel to this, the rise of Islamic State in Syria and Iraq in 2014 highlighted that non-state groups also make active use of cyberspace for recruitment, financing, communication and propaganda.

In short, there is virtually no political or military conflict these days that doesn't also have a significant cyber component.

How is digitisation changing the power political map?

That probably won't be clear for a few years yet. What is clear, however, is that there has been a wholesale increase in the opportunities to exert power by manipulating information. This is partly because it is difficult, both in a technical sense and in terms of criminal law, to attribute attacks conclusively to specific sources. In the last few months, however, attempts by states to influence elections in Western countries have shown that the strategic effects of propaganda and counter-propaganda are hard to control. Although cyber technologies are cheap and can also be used by non-state actors to exert asymmetric influence, hacking has not undermined the traditional power structures as the great powers, in particular, are massively expanding their cyber capabilities. States that are significantly inferior to other states in terms of conventional power projection are increasingly relying on cyberattacks in order to gain information superiority, at least in localised conflicts.

How are governments adapting their security strategy to these changes?

The subject of cyber warfare has, without doubt, become a top priority for global security policy. Cyberspace is extensively integrated into the existing deterrent and defence systems. Among other things, this means that governments are establishing a legal framework for the offensive and defensive use of cyber capabilities, building up additional operational capabilities in both civilian and military applications, and creating new organisational structures and command centres. Although very little reliable data is available, it can be assumed that spending has risen sharply in these areas within both the secret services

and the armed forces. Great efforts are also being made in the area of Information Security and in promoting digital literacy for all users.

What do these developments mean for multinational cooperation?

The fight against cyber crime calls for joint solutions as this is a global problem that affects everyone. Institutions such as the UN, Interpol or the Council of Europe are seeking to harmonise legislation in relation to prosecuting cyber crime. The area of cyber conflict has a more complicated starting position as states have very different interests from a power politics standpoint. The greatest progress has been made in discussions conducted within the NATO alliance aimed at applying the law of armed conflict with regard to cyber operations. However, it is often hard to define what should be considered a cyber weapon because the line between war and peace, internal and external security, political and criminal motives, and state and non-state actors becomes blurred in cyberspace.

Will we see a digital arms race in the years ahead?

If you believe all the rhetoric about building up cyber command centres, spending in this area is increasing everywhere you look. What we do know for sure is that modern armed forces see cyberspace as an operational dimension in its own right and are looking at structuring the tasks and processes in this area of operations. At the same time, the cyber dimension is closely linked to the dimensions of land, air, sea and space. Ultimately, that also means you have to assess the armament process from all angles. In the cyber sphere, there is particular uncertainty as to whether investment should be made primarily in offensive or defensive capabilities. Given the nature of the problem, this uncertainty is unlikely to be resolved any time



Prof. Dr. Andreas Wenger has been Professor of International and Swiss Security Policy at ETH Zurich since 2003. He is Director of the Center for Security Studies (CSS), which forms part of the Center for Comparative and International Studies (CIS) of ETH Zurich and the University of Zurich.

soon. It is linked to the question of whether expanding the cyber realm contributes, on the whole, to a destabilisation of strategic relations between states.

Cyber risks are multidimensional – accordingly, it is difficult to formulate a shared Security Architecture for the state, the economy and society.

Has the digital world become less secure, per se, and what are the consequences of this?

That's another tricky question, partly because insecurity is a matter of opinion and partly because the starting position for the argument is unclear. Is the world less secure today than during the Cold War? One cannot simply look at new vulnerabilities in cyberspace and conclude that "we" have become less secure. So far, there have been very few fatalities as a result of the digital world. However, both the phenomena of violence and the solutions to it are evolving in the context of digital transformation, requiring state actors to adapt their security policy strategies on an ongoing basis. For example, criminality has changed and is increasingly focusing on cyberspace. The decline in "normal" burglaries may be related to this or to greater investments in security, which might in turn be a manifestation of widespread feelings of insecurity. It is therefore also important to gain a better understanding of these connections.

What new risks has digitisation created from the point of view of Information Security?

The socio-technical context is changing both quickly and on a lasting basis. The key elements of this are more-mobile networking, the automation of industrial production, the network-based control of systems and equipment, and the resulting exponential growth in volumes of data (big data, cloud computing). This is associated with new vulnerabilities and growing challenges in terms of securing the entire value chain, bringing particular importance to various so-called critical sectors such as health, energy, finance, transport, or indeed defence. This process of digital transformation will also be associated with new challenges for security policy.

How should states, armed forces and intelligence services respond to this development?

Cyber risks are multidimensional – accordingly, it is difficult to formulate a shared Security Architecture for the state, the economy and society. Cyber security and cyber defence can only be ensured holistically and at a nationwide level. They necessitate technical, organisational, social, political and legal countermeasures. A comprehensive cyber protection strategy includes efforts in the areas of early identification, resilience, criminal prosecution, defence and governance. Until a few years ago, efforts in many countries were focused on civilian approaches and decentralised measures. In the course of the politicisation and militarisation of cyberspace, as mentioned earlier, increasing attention is now being paid to military approaches and questions of operational priorities. The key issue, with respect to a state's ability to act in cyberspace, is coordination between civilian and military bodies. However, cyber security is not simply an issue to be tackled at the national level; it is also vital to incorporate business and science and to cooperate on the international stage with regard to multifaceted cyber standards.

The Center for Security Studies (CSS) is a centre of competence for Swiss and international security policy at ETH Zurich.



Risks in the digital workplace

Digitisation is having an enormous impact on the world of work. This also applies to highly sensitive areas such as state institutions and organisations. Although this makes the workplace more agile and efficient, it also potentially makes it increasingly easier to access secret information. However, there are ways to protect against cyberattacks.

Some talk of a revolution. What we can say for certain is that digitisation is changing the world of work. Information technology is pushing forward into more and more areas, and the world is becoming increasingly interconnected. Although this creates opportunities, there are also dangers lurking beneath the surface: greater functionality and networking are giving rise to new threat scenarios.

In Diplomacy, for example, this has been clear for a long time. Communication relationships have changed dramatically, especially with regard to the internal communication between foreign ministries and embassy staff around the world. Here, information is exchanged internationally over public networks that also transmit top-secret data.

Digital Diplomacy

Ambassadors regularly inform their home country of events in their host country – usually in the form of daily and weekly reports. This exchange takes place primarily using state-of-the-art communication technologies. Nowadays, corresponding technologies are available that allow even highly classified data to be sent from a single device. This information is then forwarded, partly in filtered form, to other offices and archived in the data centre. These investigations pertain not only to matters of security but also to the image of a state, which is diminished by the activities of non-state actors on an increasingly frequent basis.

Diplomatic reports are classified because the results of the investigations provide information about individuals from the external representation's network of contacts, which has been built up painstakingly over many years and must not be made public under any circumstances. More delicate still are the personal assessments of the local situation and local issues. Indiscretions can quickly lead to serious political tension and can make the ambassador's work difficult or even impossible in future.

More and more mobile devices in use

Besides classical embassy work, day-to-day foreign policy has expanded considerably in recent decades to include other forms of cooperation. More-intensive international cooperation means increasingly frequent meetings at a multilateral level – such as conferences of international organisations. With the – typically complex – dossiers, it is often necessary to check back with political leaders during the negotiations as diplomats are obviously not in a position to reach decisions at their own discretion.

The devices used by employees are the primary target.

This communication is even more sensitive than that of regular embassy work, as diplomats are cut off from their home network and must compose their questions and receive their instructions via mobile devices. This freedom of movement requires technologies that ensure total data security even while out and about – without having to compromise on the devices' ease of use.

Intelligence services as early warning systems

Apart from that, Diplomacy often also relies on information from intelligence services, whose area of activity has also changed significantly in recent years. Specifically, the Internet has become a key element of their work, as the World Wide Web contains huge "deposits" of data that can be probed for clues. The global data network also acts as the arena for a large part of human communication, for example on social networks and all sorts of forums.

Diplomacy and intelligence services can only perform their role as an early warning system if they also carry out investigations on the World Wide Web. The Internet has also long since become a "place" where – and from which – operations are carried out or launched against states.

Combating hostile actions of this kind from the virtual sphere is placing unprecedented demands on governmental organisations. Indeed, the exchange of national security data is not restricted to internal communications; rather, it must also meet all of the criteria for maximum Information Security during cooperation with partner services abroad. Moreover, it must do so without compromising the nation's own sovereignty.

Armed forces in the digital dimension

In light of altered threat scenarios, cooperation between armed forces is also acquiring a new dimension. According to experts, the idea that each state protects itself against the diverse threats independently is outdated. There is a need, they say, for bilateral and multilateral cooperation. Even looking to the future, it is widely accepted that the battle for "information superiority" – in the broadest sense of the word – will be at the heart of future international conflicts. These conflicts might also focus increasingly on protecting critical infrastructure that is vulnerable to attacks either directly or indirectly via the Internet.

At the same time, the Internet of Things (IoT) creates an entirely new risk landscape, also for the military sector. Drones, smart helmet visors or wearable computers (wearables) for command and control information systems – these individual components communicate with one another over networks made up of various technologies. There are almost no bounds to the exchange of information. But this key benefit of the IoT is simultaneously its key danger. To ensure the confidentiality of this information, it is usually encrypted during transmission (data in transit).

In this context, special attention is paid to the IT systems of energy suppliers. As the nerve centre of a society, these systems face a particularly high risk of targeted cyberattacks, and the automation of instrumentation and control mechanisms may serve to accentuate this risk. Establishing and maintaining the cyber-secure operation of the energy supply requires various measures, such as decoupling communication and data processing from the Internet and adopting a decentralised ICT structure, as well as safeguarding communication, especially in the event of a failure of the established mobile network operators.

Devices are the primary target

As employees of public authorities are connected to the World Wide Web and use it for research and communication purposes, they are a potential target for cyberattacks. The primary target for such attacks are the devices used by employees. It is therefore important to adhere to the fundamental security principle of separating and isolating the various information systems.

There are no reliable statistics relating to cyberattacks on state institutions. However, data available from the world of business shows how commonplace these kinds of attacks have become. In a survey of Swiss companies, 54% said they had been the victim of a cyberattack in the last twelve months. A study at a global level yielded similar findings. The participants in this study agreed that cyber threats were increasing substantially.

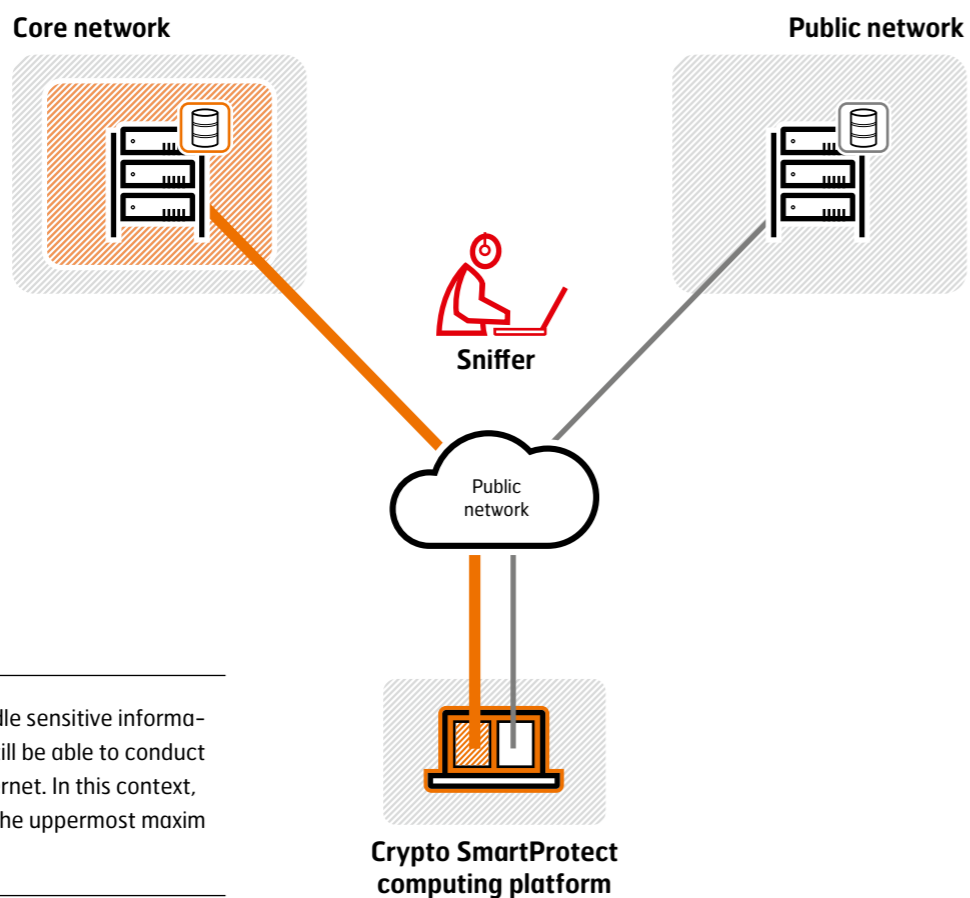
In this context, many experts fear that the risks of expanding the IoT cannot even be foreseen yet. The only thing that is certain, in their view, is that the ever-greater networking of different devices represents an "immense security risk". In particular, cyberattacks could potentially lead to damage in the "offline world". Availability is increasing because everything is interconnected and because protecting infrastructure is a very costly business.

The human factor

However, passive and active cyberattacks have already become some of the biggest threats facing governmental organisations today. Weak points in computing platforms are targeted by attackers in order to install malicious software (malware). A key part of this process is phishing, or the attempt to access an Internet user's personal data using fake websites, emails or text messages and to commit criminal acts using the stolen "identity".

In fact, hacker attacks often involve different combinations of these methods. The perpetrators typically deploy malicious software, such as Trojans, which they smuggle into a system using phishing methods aimed at careless or negligent employees. Evading classical antivirus software is the least of the hackers' problems. In other words, traditional security concepts are reaching their limits. Moreover, elaborate security solutions are often only an apparent solution, for their complexity means that they are not used correctly in day-to-day work and therefore represent an additional security risk.





Users must be able to handle sensitive information on their devices and still be able to conduct searches on the public Internet. In this context, separation is regarded as the uppermost maxim of security.

Security and ease of use combined

The prerequisites for the secure processing of information and secure communications include systematic classification and unambiguous access authorisations. However, a holistic approach is also essential for high system and platform security. Technology and user behaviour must be taken into consideration.

In the best-case scenario, highly sensitive data would never come into contact with public data traffic, as any such contact is a security risk and a potential gateway for a cyberattack.

Ideally, systems would also be built so that protective mechanisms run in the background and employees simply cannot make mistakes. They should be able to use the software they are familiar with just as they normally do. Without this ease of use, the protective mechanisms are poorly accepted or – in the worst-case scenario – may not be used at all.

The high-security computing technology Crypto SmartProtect meets all of these security requirements, providing cyber defence at the highest level for communication in highly critical areas of work. With relatively easy integration into existing IT infrastructures, Crypto SmartProtect is used by those responsible for IT security to eliminate the most serious vulnerabilities in the system – devices such as employees' PCs and laptops.

Target device – cOffice Workplace offers uncompromising protection

Information Security is a key issue in the age of digital transformation because innovative communication technologies not only throw open the doors to new applications and solutions but also present new risks. Sensitive information is subjected to targeted cyberattacks on a daily basis – and users' devices are the primary target of such attacks. Crypto AG can eliminate this risk with the use of devices based on Crypto SmartProtect technology.

A chain is only as strong as its weakest link. This is by no means a new insight, but it still rings true – both now and for the future. In the context of cyber defence, it means that IT security administrators must localise weak points and secure them appropriately. Experience shows that even localising these weak points can be a major hurdle because IT structures are often so complex and confusing that effects and dependencies are impossible to predict. It is therefore all the more important to reliably protect weak points identified as such in risk analyses – paramount among them the employees' devices.

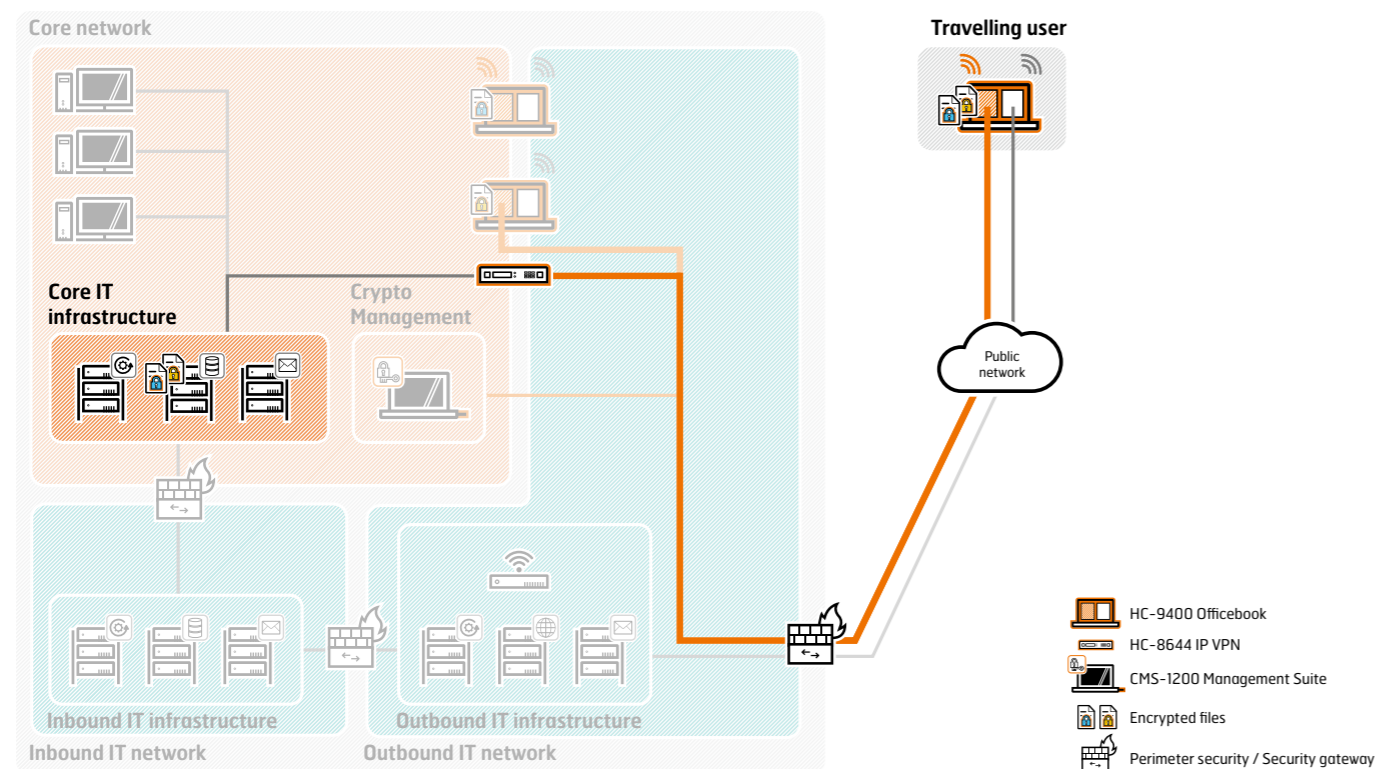
Cyberattacks affect all employees

The oft-repeated view that individuals themselves are not a potential target of cyberattacks has now been categorically disproven. Countless attacks originating in cyberspace have

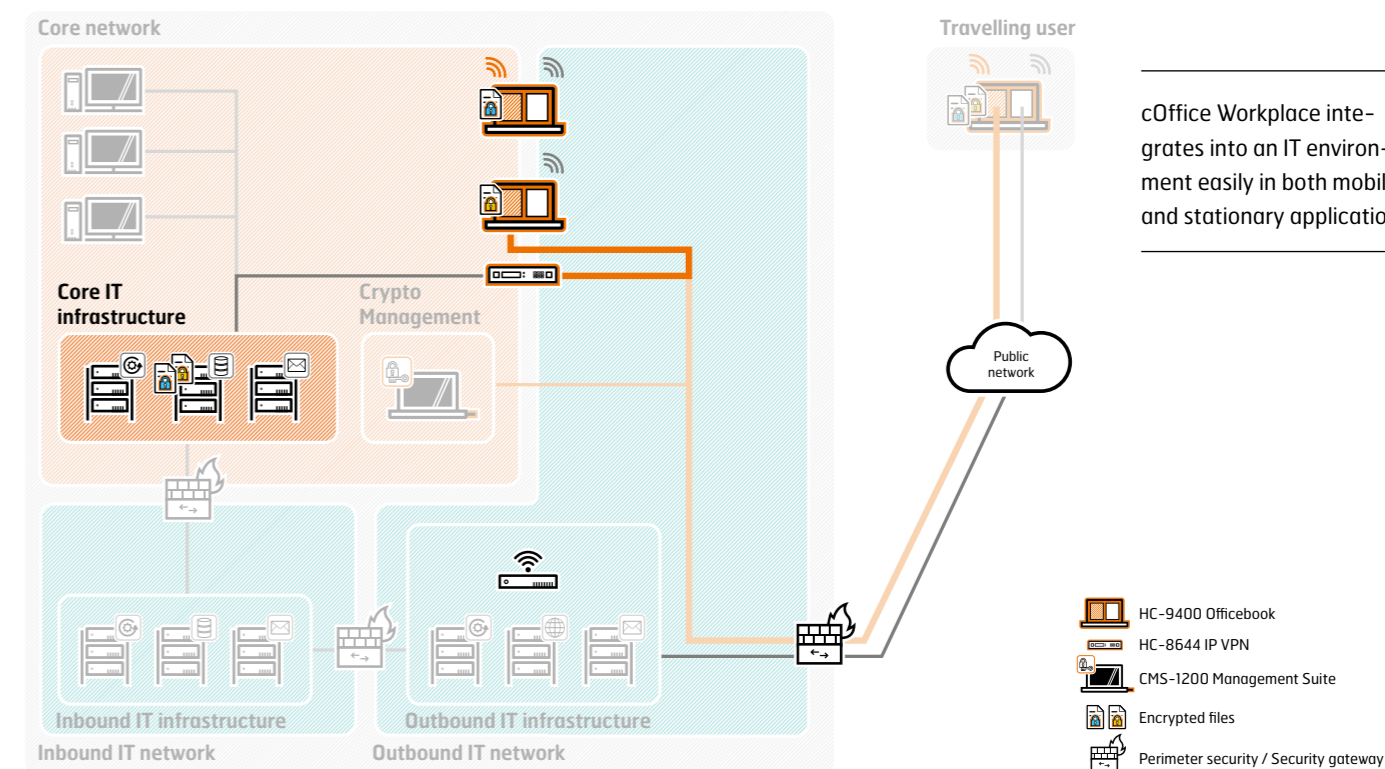
shown that all employees are potential targets, whether on their stationary or mobile workstations. In principle, therefore, every member of staff represents a potential gateway to an organisation's IT infrastructure. Nowadays, attackers specifically set their sights on workstations and deploy tailor-made malware with the aim of accessing, stealing or modifying sensitive data. This data could be infrastructure plans, secret service information, strategy concepts, commands or confidential protocols. It is therefore important, even for organisations with highly professional defence systems, to intensify the focus of their IT Security Architecture on employees' devices and their integration into the centralised IT infrastructure.



cOffice Workplace in a mobile application



cOffice Workplace in a stationary application



cOffice Workplace integrates into an IT environment easily in both mobile and stationary applications.

Based on Crypto SmartProtect technology, cOffice Workplace allows you to work in a convenient and highly secure way at all times.

Success depends on boundless, highly secure communication

Until now, IT security administrators have all too often faced the dilemma of having to strike a balance between protecting valuable data appropriately and providing the greatest possible ease of use for users. This dilemma is all the more acute because many organisations' employees depend on being able to communicate in a highly secure manner regardless of time and location, and require constant, unrestricted access to internal and / or public information. After all, boundless communication is now a matter of course and, sometimes, a key factor in an organisation's success. If practicability is impeded by elaborate security measures, there is a considerable risk that even security-conscious employees will disregard security requirements in the heat of the moment. This is summed up by the following maxim: if an application does not work as desired, people will find a way around it, substantially increasing the potential risk. For this reason, Information Security should not be an obstacle to ease of use; rather, it should operate in the background without the user noticing.

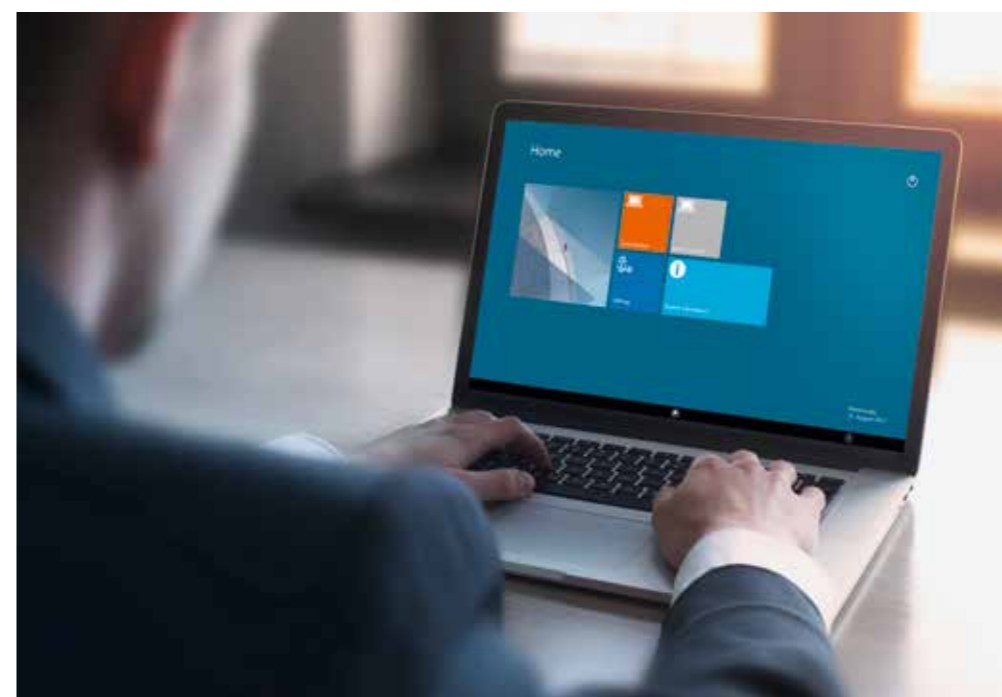
cOffice Workplace – information is extensively protected at all times

cOffice Workplace is a system for accessing and handling sensitive information securely within a civilian or military organisation. It allows users to access publicly available information on the Internet easily and without putting the organisation's internal information and IT infrastructure at risk. At the heart of this system is the HC-9400 Officebook, which is based on Crypto SmartProtect technology. Users can make this Officebook their stationary workstation or take it with them to use outside the organisation. The HC-9400 Officebook provides users with access to two completely separated user environments. One user environment can be used to handle sensitive internal information. Via a secure link to the HC-8644 IP VPN, this environment can be connected to the headquarters' IT infrastructure, providing users with online access to the organisation's centralised information and applications. With the second user environment, users can connect to public networks and therefore also access publicly available information. The cOffice Workplace system also includes management infrastructure in the form of the CMS-1200 Management Suite and the HC-8644 Management Gateway. These two system components can be used to configure and administer the HC-8644 IP VPN and users' HC-9400 Officebooks.

HC-9400 Officebook – efficient working in a familiar user environment

The HC-9400 Officebook reliably protects against cyberattacks and allows employees to work securely and conveniently in a familiar user environment. The HC-9400 Officebook is made up of two Compartments with completely isolated user environments. The first Compartment consists of a user environment with the Windows 10 operating system and Microsoft Office applications for handling internal information. The second Compartment consists of a user environment with the Windows 10 operating system and a web browser for accessing public information. The two Compartments can be operated simultaneously, allowing employees to work with information on different, completely separated networks in a convenient

and highly secure way. The consistent separation of user environments ensures total Information Security at all times. A single click is all it takes to switch between the user environments. All of the protective mechanisms operate unnoticed in the background without compromising the working process.



The HC-9400 Officebook allows you to work securely even while out and about and offers extensive protection against cyberattacks.

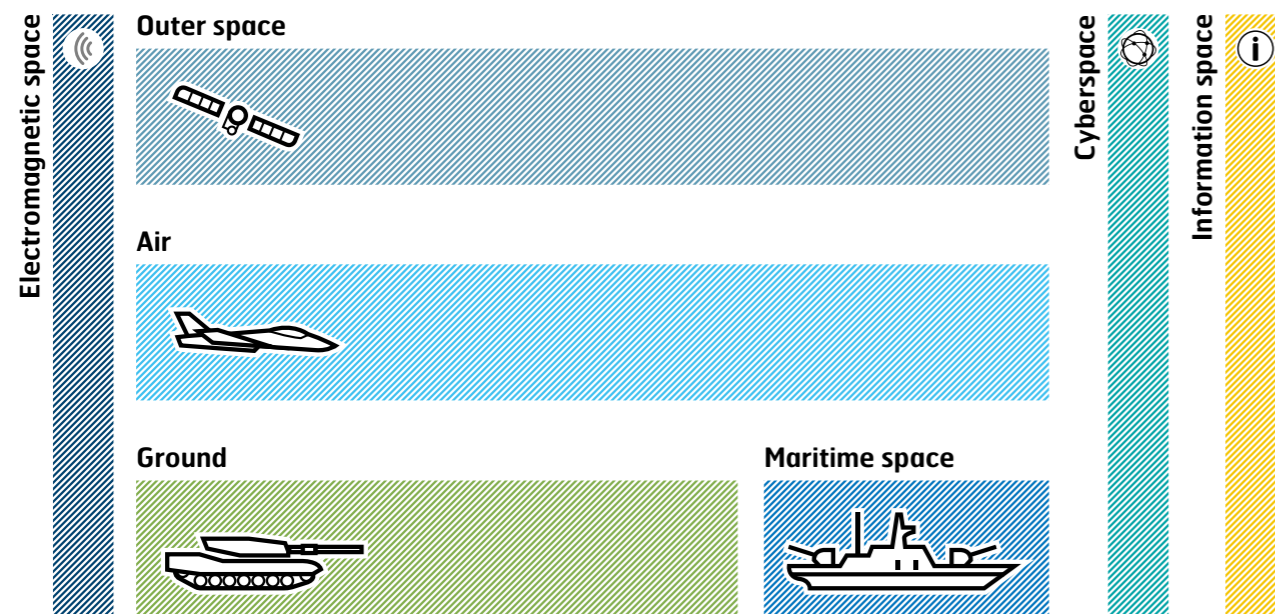
Digital warfare: the beginning of an era

A nation's security can be put at severe risk at the click of a mouse. Armed forces operating on land, at sea and in the air offer little protection against threats of this kind. Rather, there is a need for online armed forces that know how to do battle using codes instead of tanks. For these cyber armies, the top priority is to increase cyber security in order to protect defined security zones.

The armed forces are in a state of flux: for years, the process of transforming the armed forces of the industrial era into those of the information era has been in full swing around the globe. The key driver of this radical transformation is digitisation, which is continuously expanding the room for manoeuvre, redefining security standards, changing modes of operation and boosting efficiency in all areas of the armed forces.

However, the growing trend towards networking IT systems also creates new risks. The military information infrastructure itself becomes a main target of attack. The top priority is therefore to protect the military information network, and especially its integrity, stability and speed, because the greater the degree of digital networking, the more vulnerable the information infrastructures become. In this context, protective mechanisms such as encryption, authentication and segmentation have become an essential aspect of modern armed forces.

Operational domains of the armed forces



From a military perspective, there are various so-called operational domains. Cyberspace runs vertically alongside the classical operational domains, meaning that cyberattacks can take place not only on the ground but also in the maritime domain, in the air and in outer space. The selection of possible targets therefore increases ad infinitum.

Source: HWZ University of Applied Science in Business Administration Zurich, Center for Digital Business

The fourth generation of warfare

The rapid development of modern technologies is also changing how armed forces can be deployed. Digitisation within the armed forces has now ushered in the fourth generation of warfare. In the first generation, the focus was on Napoleonic line and column tactics. The principal innovation of the second generation was that the infantry occupied and secured areas that had first been conquered using artillery. The third generation introduced the tactics of blitzkrieg, and the fourth generation of warfare is being waged in cyberspace. This fifth dimension runs vertically alongside the four "classical" operational domains: land, sea, air and outer space (see diagram). In other words, cyberattacks can take place on the ground, in or on water, in the air, and in outer space. Since the operational domains are interconnected, the number of potential targets increases ad infinitum.

Cyberspace essentially consists of the following areas: software, hardware, data, networks and people, as well as electricity as an energy source. A cyberattack is independent of time and location and is almost always anonymous in origin. This means that an attack often has no immediate consequences. The attacker can only be traced and identified in very few cases and following an elaborate process of reverse engineering.

Digitisation within the armed forces has now ushered in the fourth generation of warfare.

The damage caused by a cyberattack is rarely immediate; often, the attack can continue undetected in the background for a long period of time and is only discovered due to additional actions on the part of the attacker. The scale of the resulting damage is hard to estimate, though it is often more extensive than a direct confrontation. Digital warfare also includes activities such as industrial espionage, the disruption or destruction of critical infrastructure, financial warfare (manipulation of agency ratings for countries or banks), and the use of beam weapons to disable electronic applications such as mobile phones, for example. The transformation of the armed forces is intended to expand the military's capabilities to influence a generic system for its own objectives. At its heart, this represents an expansion of military actions into the civilian realm. Warfare of this kind pursues one main goal: it seeks to wear a society down. Conventional military action can provide no protection against such tactics.

Building up a cyber army

The preparations for digital warfare are in full swing: across the world, often huge sums of money are being invested into building up and expanding an IT army. The cyber command centres operate as units in their own right alongside the army, navy and air force. Their principal role includes guarding against attacks perpetrated using information technologies. In just the first few months of this year, a number of governments have reported huge cyberattacks against their armed forces. These included attempts at espionage and data theft, as well as attacks on their military's digital infrastructure with a view to manipulating or destroying it. The armed forces' reliance on digital technology puts them at a huge risk of cyberattacks. Entire combat units, aircraft or warships could be put out of action if the communication connections and information systems were sabotaged. This led one European defence ministry to declare that as soon as an attack jeopardises the armed forces' functional and operational capabilities, it would also be permissible to defend oneself using offensive tactics.

The seriousness of this risk was brought home by a cyberattack on mobile phones in 2016. A case came to light in which mobile phones of artillery soldiers were infected with a virus. This virus transmitted the coordinates of their locations to the attackers, whereupon the locations were bombarded and soldiers were killed. There is no shortage of examples of how effective digital attacks can be, but they don't necessarily involve a high level of programming skill: the targeted dissemination of false reports is another effective tactic for the purposes of manipulation.

Protection against hacking techniques

Among other impacts, hacking techniques jeopardise the security of communications. For an organisation, it is immensely important to consistently minimise the prevailing risks of unauthorised access to sensitive information. One efficient option is the "hard encryption" of all information that leaves a protected area, in conjunction with further measures under the ambit of Security Policy. In this instance, hard encryption means that the encryption takes place exclusively in separate, tamper-proof hardware, which also meets the relevant military standards if necessary.

Hardware-based encryption and a user-specific proprietary algorithm, i.e. an algorithm that is unknown to third parties, are used to counteract cyberattacks – cyberattacks such as infiltrating and spying on networks using masquerading tactics, the manipulation and interception of classified data, or the smuggling in of malware. This approach ensures the confidentiality, authenticity and integrity of sensitive information.



E-government: towards a digital state

Digital transformation has also become a reality for state institutions. So-called e-government not only simplifies the exchange of information between public authorities and their stakeholder groups, it also presents a diverse set of challenges.

The civil servants who stamp official documents behind armoured glass still exist. In many countries, however, a virtual colleague has taken their place. Nowadays, the exchange of information between citizens and public authorities increasingly takes place online: 24 hours a day and 7 days a week. Moreover, internal and inter-authority processes are often handled exclusively using digital information and communication infrastructures.

The advantages of this are clear: improved efficiency, easier operation, lower error rates and greater transparency. In this respect, e-government looks set to play an increasingly significant role in the age of digital transformation. It represents nothing less than a complete redesign of the administration against the backdrop of new technical capabilities. For the transformation to a digital state to be successful, it will require a combined overall strategy, updated legal frameworks where necessary, and interoperable IT infrastructures.

Interfaces pose a challenge for IT administrators

This interoperability presents challenges for many countries, especially those with a federal structure, as the different public authorities at various levels of government currently provide their services through their own individual portals. The data from these portals is handled in different processes, which may not be interoperable, and stored at a multitude of different data centres, which are operated by multiple IT service providers. In many cases, suitable interfaces do not yet exist.

Digital transformation presents government IT administrators with the challenge of providing corresponding interfaces. At the same time, attempts to deliver nationwide networking give rise to a whole host of new security risks. Not only does the rapidly increasing complexity of IT make the network more prone to faults, but the vulnerability to cyberattacks also increases. This, in turn, exacerbates the threat to data integrity and confidentiality. Data classified as "confidential" or higher requires additional protective measures during access, transmission and processing. Information Security is therefore

also a key issue in e-government. In order to minimise the potential risk to IT applications and systems, the field of IT security must develop appropriate security concepts, regulate the assignment of access authorisations, and implement inter-authority security standards.

The possibility of accessing data anywhere and at any time also involves risks for e-government.

Of course, security consists of many different elements that must all match up in order to prevent the chain from breaking at its weakest point. When it comes to choosing which technology and systems to use, public authorities typically enjoy less room for manoeuvre than companies in the private sector. Depending on the country and public authority in question, there are legal frameworks that govern data protection and Information Security with varying degrees of strictness. For many administrations, this results in an attitude that is best described as "wait-and-see". At the Secretariat of eGovernment Switzerland, for example, the approach is to continually observe the development of different technologies and to check which of them is successful on the market. Crypto AG offers tailor-made solutions in the field of e-government; read more about this topic on page 20.

Technical progress has also changed the way the armed forces operate.

There is very little that can be done against the attackers themselves. Identifying them is extremely difficult or even impossible in many instances and requires the malware they used to be unravelled and reverse engineered. The covert and non-kinetic nature of the operations means it is virtually impossible to identify the persons responsible. Even if there is evidence that a state is behind an attack, it remains unclear how to respond without putting trade relations at risk or disclosing further sensitive information.

Rules for cyber warfare

In the long term, international standards could be established to regulate or forbid cyber warfare against sovereign states. International sets of rules for conducting cyber operations have already been devised, such as the proposal for an international Information Security treaty (2009) and the "International Code of Conduct for Information Security", which was submitted to the United Nations (UN) Security Council in 2011. However, the proposals aimed at adopting international agreements on cyber warfare were rejected. This goes to show that the world is in the midst of an arms race in terms of encryption techniques. Keeping pace is the order of the day. The risks are likely to continue getting worse as the degree of digital networking is set to increase massively in the future.

SUCCESS STORY

Information Security concept for secure e-government

Governmental organisations and authorities are using new information and communication technologies to improve efficiency and transparency in the performance of their duties. Since e-government projects involve processing large volumes of sensitive information, security is of paramount importance in their planning and implementation.

Public authorities are not immune from technical change and are left with no choice but to adapt their processes and infrastructure. They therefore increasingly provide their services online. The challenge here is to guarantee the security of the documents being sent or being made available for download, either within the ministries or to the general public via online portals. It should also be noted that various transactions between citizens and public authorities require collaboration between multiple ministries.

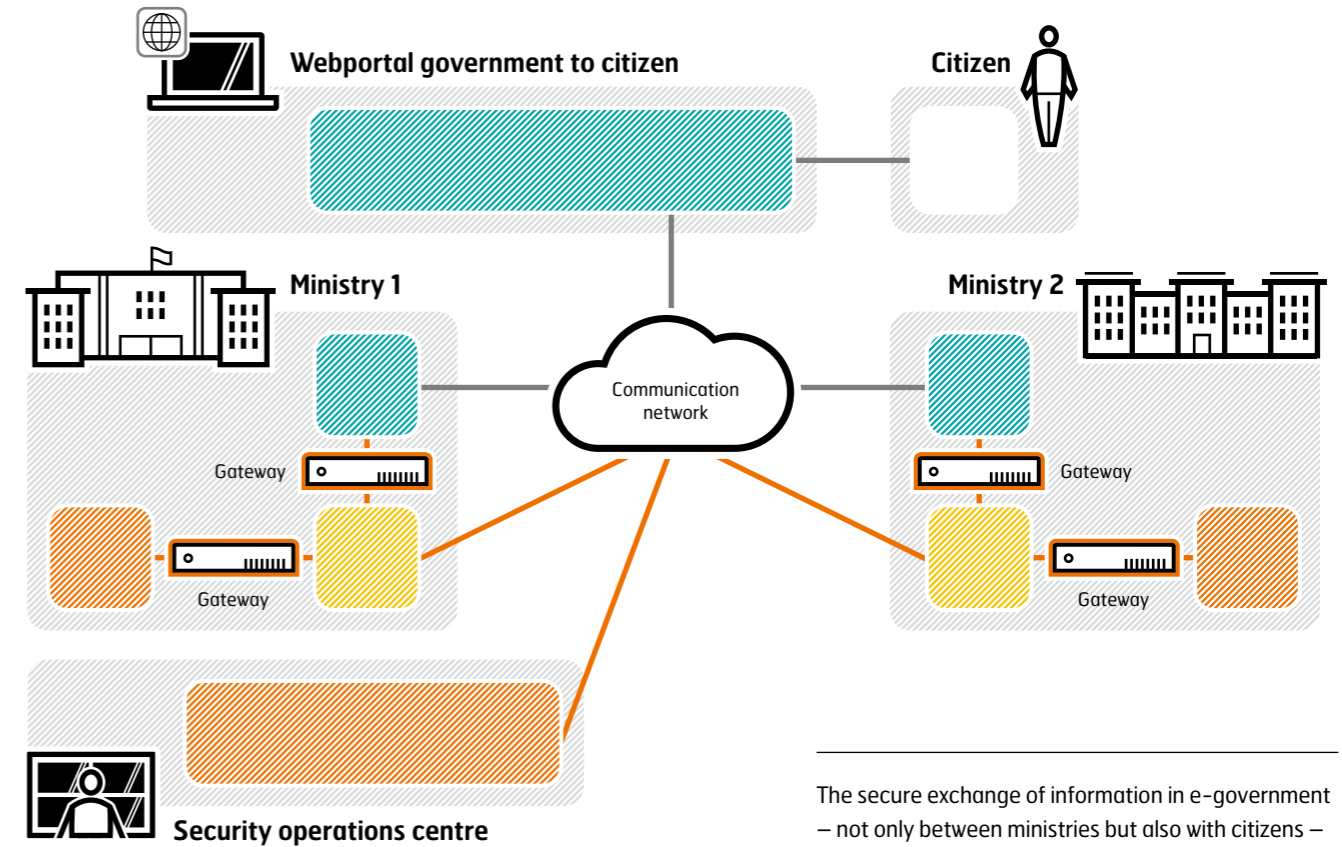
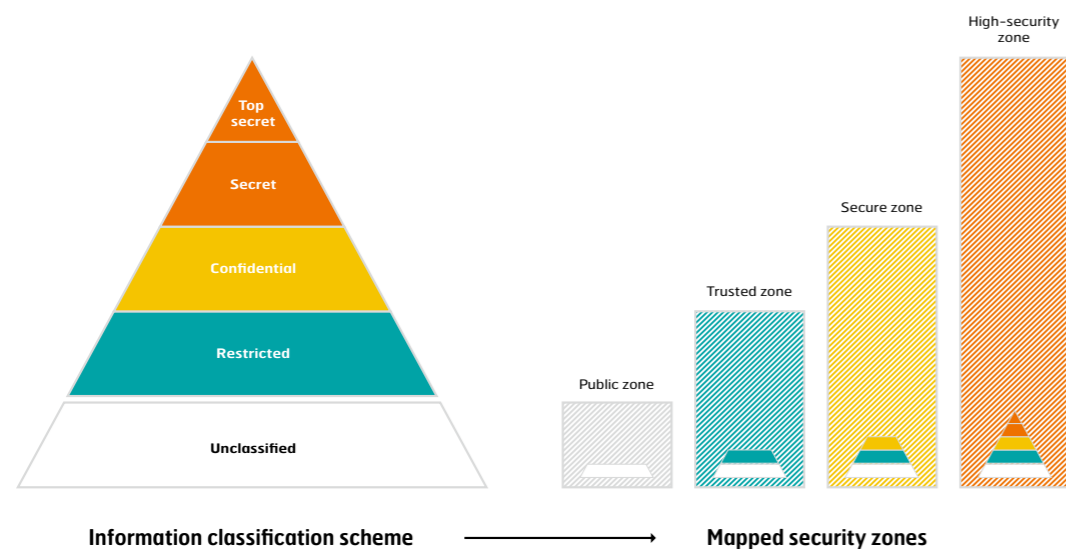
Accordingly, the definition of different security zones, including their perimeters and transitions, plays an important role in the secure exchange of information. Thanks to these security zones, it is possible to provide appropriate protection for documents with varying degrees of classification – from "restricted" to "top secret", for example. Information is processed and stored in different security zones depending on its classification. The different security zones can be "trusted", "secure" or "high-security" zones, with each zone also allowing the processing of more deeply classified information.

The definition of different security zones, including perimeters and transitions, plays an important role in the secure exchange of information.

More than just an online portal

When an online portal offers electronic self-service, it is essential that the applicant be reliably authenticated. Unlike at the counter in a government office, where this is done using a photo ID card, the online portal has to depend on a reliable electronic identity. The only way to ensure this is to adopt an integrated e-government Information Security concept.

However, e-government is more than just an online portal. Suitable devices and networks are also needed in order to make



The secure exchange of information in e-government – not only between ministries but also with citizens – is ensured thanks to the subdivision of information into different levels of classification.

use of e-services. This suitability is ensured through a powerful and customer-specific network solution, as well as through end-to-end encryption to protect communication connections between ministries. On top of this, the zone transitions and perimeters are protected by high-security gateways.

The entire infrastructure is monitored by a centralised Security Operations Centre (SOC), which can not only carry out

systematic analyses of threats but also assists with the identification of attackers, the escalation of security incidents, and much more. With tailor-made user and authorisation management, the information being processed can only be viewed and edited by authenticated users. Furthermore, constant availability and fail-safeness are ensured at all times thanks to communication channels implemented on a redundant basis.

Appropriate protection of information at every level of classification

Total security

Crypto AG's unique Security Architecture offers the best possible protection for sensitive information against malicious interception – and this information can only be viewed and edited by authenticated users thanks to customer-specific user and authorisation management.

Perfect integration

The security layer can be integrated perfectly and economically into the existing infrastructure – including the SOC.

High availability

Communication channels implemented on a redundant basis ensure constant availability and fail-safeness.

Independent operation

The entire high-performance network can be operated autonomously by the system administrators thanks to comprehensive knowledge transfer.



encompasses the whole part of the World Wide Web that is not indexed by normal search machines and is estimated to be around 500 times larger than the Visible Web, which is also known as the Surface Web. The Darknet itself is just a small, encrypted section of the Deep Web. Experts currently estimate that there are about three million TOR users. For the sake of comparison, the "normal" Internet was used by an estimated 3.4 billion people in 2016.

"Just because the attempts originate from the Darknet doesn't necessarily mean they are more dangerous or more cunning," explains Bernhard Tellenbach, Professor of Information Security at ETH Zurich.

How dark actually is the Darknet?

Everyone has heard of it at some point – but when it comes to the details, things are a little more hazy. We are talking about the Darknet. It sounds like something disreputable or even illegal, but is the Darknet really only the evil twin of the normal, familiar Internet – with Google, Facebook, Amazon, etc. – that we all know so well, and is it something we should be protecting ourselves against? Or does its secrecy hold the key to something bigger – and perhaps even something useful?

From the perspective of computer science, and hence from a purely factual standpoint, the Darknet is a network whose participants establish connections between one another manually. On the normal Internet, this is done automatically and on an arbitrary basis. The Darknet therefore offers a greater degree of security, as potential attackers cannot readily access the PC or the user's data – and, ideally, are not even aware that the network exists.

A virtual tunnel to an unknown destination

But how do you actually get into the dark side of the Internet? Sites on the Darknet do not end in common domain suffixes such as ".com" but rather in ".onion". This extension represents the so-called TOR network, which is a type of virtual tunnel. TOR stands for "The Onion Router", which neatly paraphrases how data traffic is handled on the network: queries are encrypted and redirected to constantly changing routers via various servers and nodes, none of which is aware of the actual destination. In other words, an onion or multilayer principle.

The aim here is to obscure the origin and identity of the communication partners and to ensure maximum anonymity.

Any computer connected to the TOR network can host a web page without disclosing its location (and therefore its identity) to the rest of the world. The server's genuine IP address is invisible to other users, and even the user does not reveal their location. Moreover, the intermediate nodes through which the data is relayed to conceal its origin receive no information about the respective end points or about the contents of the data being exchanged.

The risks are the same

However, the TOR network does not protect the user from the dangers that are also present on the normal Internet, such as computer viruses. For example, if an infected PDF document or a Java file is downloaded, it is entirely possible for this to be used to reveal the user's location or true identity. Likewise, it is also possible to hack a Darknet server. The most recent

example was in early 2017, when a hacker from the Anonymous collective shut down the pages of the well-known operator Freedom Hosting II, which was hosting prominent websites on the Darknet and offering webspace for any given purpose. The attack took an estimated 10 to 20 percent of the entire Darknet offline. Moreover, around 74 gigabytes of stolen data and 2.3 gigabytes of user data were made public and the users of the illegal sites were unmasked online.

Companies, public authorities and even private individuals can protect themselves against attacks from the Darknet in the same way as they do against those from the normal Internet – in other words, with firewalls, encryption, etc. "Just because the attempts originate from the Darknet doesn't necessarily mean they are more dangerous or more cunning," explains Bernhard Tellenbach, Professor of Information Security at ETH Zurich. The difference, he says, is that it is harder to identify the attackers, although the Darknet is just one of various ways to conceal the source of an attack. There is no special danger from the Darknet, Tellenbach adds, although there is an indirect threat "because the Darknet is sometimes used to trade in tools and information used for attacks".

The scale of the Darknet is significantly smaller than articles about it often suggest as the Darknet is often confused with the Deep Web, especially in size comparisons. The Deep Web

What to do about the Invisible Internet

For now, it is hard to say what the future has in store for the Darknet. On the one hand, politicians are increasingly calling for a crackdown on the Invisible Internet because of the high levels of criminal use. On the other hand, the Darknet is also promoted as a way for journalists, whistle-blowers and dissidents to distribute their information safely.

One thing is clear: public authorities are attempting to assert control over the illegal activities on the Darknet – which make up around 50% of its content according to the latest estimates. The usual approach is to establish specialist units with an explicit focus on this subject. Even so, investigators have still not fully established how, for example, the details of around half a billion users were stolen from the Internet company Yahoo in 2014 in what was probably one of the biggest data thefts in history. At the time it was said that the attackers were from outside the Yahoo network, and the suspicion was that the attacker had state backing. It is still unclear whether the attack originated from the Darknet or not.



Crypto AG
P.O. Box 460
6301 Zug
Switzerland
T +41 41 749 77 22
F +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Crypto cSeminars

cSeminar Information Security Specialists

16 to 20 April 2018
10 to 14 September 2018

cSeminar Contemporary Cryptography

23 to 27 April 2018
17 to 21 September 2018

The seminars are held at the Crypto Academy
in Steinhausen / Zug, Switzerland.

Contact and further information

www.crypto.ch/seminars