

CRYPTOMAGAZINE



For the customers of Crypto AG, Switzerland

2 • 2009



ARMED FORCES

Dear Reader

Keeping correctly and sufficiently informed is a crucial factor in the success of any undertaking, be it a business or an army. Secret military data also requires maximum protection to cope with modern information behaviour, including networking and the resulting dependencies on information technology. The nature of the threat has reached new dimensions. It used to be we could communicate one-on-one with the antagonists. Today, digitalisation has rendered these adversaries anonymous and the means of communication available globally have made them unpredictable. The classic patterns of communication and security in the military therefore fall short of adequately meeting these threats.

A comprehensive approach should be taken to information security. After all, the task is not just to repel cyber attacks but also to deal with physical onslaughts and psychological factors. Sensitising the armed forces to all aspects of security must be a top priority and cover everything from security concepts, cryptological principles, and elements of communication to network and data security and the security of operating systems and application software.

I wish you interesting and absorbing reading.



Giuliano Otth

President and Chief
Executive Officer

3	Transformation of the armed forces Focus on asymmetry and increased latency	FOCUS
5	Network Centric Warfare NCW – a catchword with a complex background	FOCUS
8	The Swiss Armed Forces The complexity of transmitting military information	INTERVIEW
10	MultiCom Encryption Unit HC-2650 Communication: an important part of our modern world	TECHNOLOGY
12	RCU-2650 Remote Control Unit/RCS-2650 Remote Control Software HC-2650: the latest additions	TECHNOLOGY
13	Ethernet Encryption for Next Generation Networks Ethernet Multipoint Encryption	TECHNOLOGY
15	Series on Crypto Services (IV) ICT security can be learned	SERVICES
18	Portrait: land forces	SERIES
19	Milestones in the history of the company part 2: the 1960s Fresh impetus for progress – the trend towards digital electronics	SERIES
22	Using mobile devices securely	SECURITY AWARENESS

IMPRINT

Published three times a year **Print run** 6000 (German, English, French, Spanish, Russian, Arabic) **Publisher** Crypto AG, P.O. Box 460, 6301 Zug (Switzerland), www.crypto.ch **Editor-in-chief** Gabriela Hofmann, Crypto AG, Tel. +41 41 749 77 81, Fax +41 41 741 22 72, E-mail gabriela.hofmann@crypto.ch **Design/Typesetting** illugraphic, Sonhalde 3, 6332 Hagendorn (Switzerland), www.illugraphic.ch **Translation** Apostroph AG, Töpferstrasse 5, P.O. Box, 6000 Luzern 6 (Switzerland), www.apostroph.ch **Printing** Ennetsee AG, Bösch 35, 6331 Hünenberg (Switzerland) **Reproduction** Free of charge with the consent of the editorial office, courtesy copies requested. All rights reserved Crypto AG **Illustrations** Corbis: p. 3, 17, 24 · Crypto AG: p. 2, 8, 9, 12, 14, 19, 20 · Getty Images: p. 5 · Imagepoint: p. 11, 15, 16, 22 · Swiss Armed Forces: cover, p. 6, 7, 18 · Shutterstock: p. 4, 16, 17, 21

TRANSFORMATION OF THE ARMED FORCES

FOCUS ON ASYMMETRY AND INCREASED LATENCY

Defence organisations rely increasingly on highly complex communication structures to cope with what some experts are calling the “new wars” and with changes in the operating environment such as the digitalisation of the battlefield. Their modern military command and control systems (C4ISTAR¹) link sensitive points with each other in real time and support secure, mobile access to vital strategic and tactical information.

By Dr. Silvan Frik, Head of Marketing Services



The term “new wars” first came into parlance around the time of the Balkan wars in the 1990s. German political scientist Ralph Rotte cites two new aspects that distinguish these phenomena:

- Asymmetric warfare: Primarily civil conflicts, violations of international humanitarian law, and the emergence of war economies that give the phenomena a dynamic of their own.
- Use of modern information technologies.

Several countries have since set about adapting to this new situation and reforming their security architecture in evolutionary processes. Until now, security architecture has been considered a static entity, but this viewpoint is inadequate for addressing the new threats. German Professor of Political Theory Herfried Münkler explains that in responding to asymmetry, states have military and police tasks to

perform as well as intelligence and social therapeutic tasks. He believes cooperation with other like-minded states is the only solution, and a mandatory one. The threatened states display a reduced ability to apply force to assert their political will, Münkler notes and says this fact must be taken into account in this context.

With respect to ICT advances, defence ministries and armed forces are, for varying reasons, making increasing use of work techniques and methods already employed in other administrative agencies and private enterprises. This change has made the transmission of information much easier, also between organisations.

What most studies fail to do, however, is to draw an inference from these two observable trends, which can also be applied jointly – by all players involved!

New level of warfare

Modern technologies are now used by all parties in a conflict, not least because they can be acquired so inexpensively today. For instance, public opinion can be “twisted” using the Internet (information warfare). Cyber warfare is another approach. Its goal is to inflict as much socio-economic damage on the opponent as possible by impairing its ICT infrastructure. It is interesting to note that this type of warfare is increasingly directed at civilian targets. Military operators are usually aware of the needs for greater security and respond accordingly. Asymmetry is taking on a new dimension as a result.

The “new wars” must also be ascribed a further dimension, namely, their function as a “new precursor to war”. Latent threats are becoming more direct; the potential for defence readiness must be structured in a more concentrated

and networked way. The general awareness of our being constantly at risk from this new precursor to war is absent however, or insufficiently keen.

Examples appear daily in the papers and involve substantial damage. For instance, it was recently reported that cyber hackers breached the development programmes for the new F-35 fighter at arms manufacturer Lockheed Martin in the United States. The unnoticed loss of several terabytes of data over the years is as amazing as it is alarming. According to a current survey conducted by the Swiss daily Tages-Anzeiger, McAfee, the computer security specialist, has counted at least 120 countries that are engaged in Internet espionage. Twenty-five countries are already developing actual cyber war programmes, with China taking the lead. And the even more horrific figures for business espionage are not even included. Business espionage often works hand in hand with the government intelligence services. In 2008, a small country like Switzerland barred entry to a remarkable 21 diplomats for engaging in illegal espionage (as opposed to eight just the year before). One can only guess how high the undetected or unreported cases might be.

Networking has consequences and poses new risks

The undisputed advantages of increased networking obviously have a counterpart, namely major risks:

- Infrastructure availability: This problem is now being addressed with more redundancies, ring networks, civilian-military emergency plans and other measures.
- Targeted attacks from without: Physical protection has to be provided for particularly critical nodes, e.g. central Internet servers or network servers in general. The civilian infrastructure/provider must become involved here too (asymmetry!). In a



broader sense, these efforts also include defence against cyber attacks, which to date is not yet as resolute as it should be.

In keeping with the premises of the new threat, many armed forces are undergoing transformation to render new technologies militarily usable and to adjust their organisational structures to the new challenges. Along with the professionalism of deployed personnel, the effectiveness of command and control depends largely on the quality of the available information (in the correct form) and its unhindered flow (to the right entities). The goal is to achieve modern, flexible and highly mobile armed forces capable of using their information superiority to act more quickly, more precisely and more in line with requirements – and to do so in an interoperable manner. Consequently, the new multidimensional ICT combines all aspects of modern warfare, from comprehensive intelligence to the mission of the individual soldier in the field. The arms race in this sector is already outpacing the one for weapons technology.

A two-edged sword?

The first signs of fatigue have already appeared as regards implementation. The integration of legacy systems has proved to require more resources than expected. And the desired standardisation often faces opposition from legacy infrastructures. It also remains to be seen whether an information overload and excessive decentralisation of command and control might not pose a certain risk to the functional-

ity of an army. A point on which everyone agrees is that sophisticated information networks are vulnerable to attack and that the attacker always shares the same capabilities and utilises them. It is no accident that China lists IT preventive strikes as a tool of proactive defence in its new military doctrine. ■

Sources:

Several articles from: Allgemeine Schweizerische Militärzeitschrift (ASMZ), Neue Zürcher Zeitung, www.c4istar.ch

¹ Command, Control, Computer, Communication, Intelligence, Surveillance, Target Acquisition, Reconnaissance.

NCW – A CATCHWORD WITH A COMPLEX BACKGROUND

In our age of global networking, the art of war is increasingly based on the potential for controlling and accelerating global networking. This observation may appear trivial at first glance. Yet in actual practice, NCW cannot be reduced to technological aspects, as the “transformation” of the armed forces, a term often used in this context, might suggest. This process covers the far-reaching implementation and intelligent handling of technologies as well as paradigm changes in societal structures and mechanisms. One fact frequently ignored is that networking entails not just advantages but also (often insidious) new dimensions of risk.

By Rudolf Stirnimann, Customer Segment Manager

Network Centric Warfare, abbreviated NCW, is the latest stage of development for military concepts and strategies, whose purpose has always been to optimise means in order to achieve an established goal. The basic idea behind NCW is to attain the total electronic networking of the units within the armed forces, all their sensors and actors. All units should be able to draw their information for operations from a current data pool and feed any information they obtain into this pool. Computerised command and control systems triage the data, edit it and automatically produce bases for decision-making

in real time. They also facilitate the preparation and synchronous execution of concurrently running operations, which is akin to multiplying their potential effect.

Asymmetry, networking and responsibility

Just taken alone, NCW would be a rather revolutionary advance. But “network” can no longer be interpreted as referring merely to the military radio network, etc. Warfare nowadays is increasingly asymmetric. Images arise of pirates attacking sailors, freedom fighters battling Red Cross auxiliaries or “pacifists” clashing with police troops at G8 summits. The current trend is definitely toward network access for all governmental and, in some cases, semi-governmental organisations entrusted with operating and protecting services that are central or vital to society. This task poses technical as well as political problems.

On the technical side, the integration of civilian networks and especially networks of public providers is not a serious problem. After all, military organisations often implicitly treated these networks as part of their own ICT infrastructure in the past. This view naturally necessitated appropriate plans for ICT security.

A complicating factor has been that cost pressures have compelled some armies to dispense with the requirement that everything they procure be militarily functional and comply with MIL standards. Militarily functional devices are more rugged and more costly to design and are therefore considerably more expensive than commercial products. At the same time, conditions are often better in protected military spaces than in civilian environments. Commercial over-the-shelf (COTS) products are suitable in these cases because networking with parts of civilian society (interface harmonisation) is much easier and even facilitates a country’s ability to enter into coalitions with other countries.

Taken to its logical conclusion, however, this approach also means that the different work scenarios want to see their hierarchical security needs satisfied despite end-to-end networking. With modern encryption technology, this responsibility can be met.

Rapidly increasing cost-benefit ratio

A look back in history shows that revolutionary ideas often have many fathers. In the case of NCW, one father was and continues to be the political demand for cheaper services, a demand also directed at defence organisations. For the

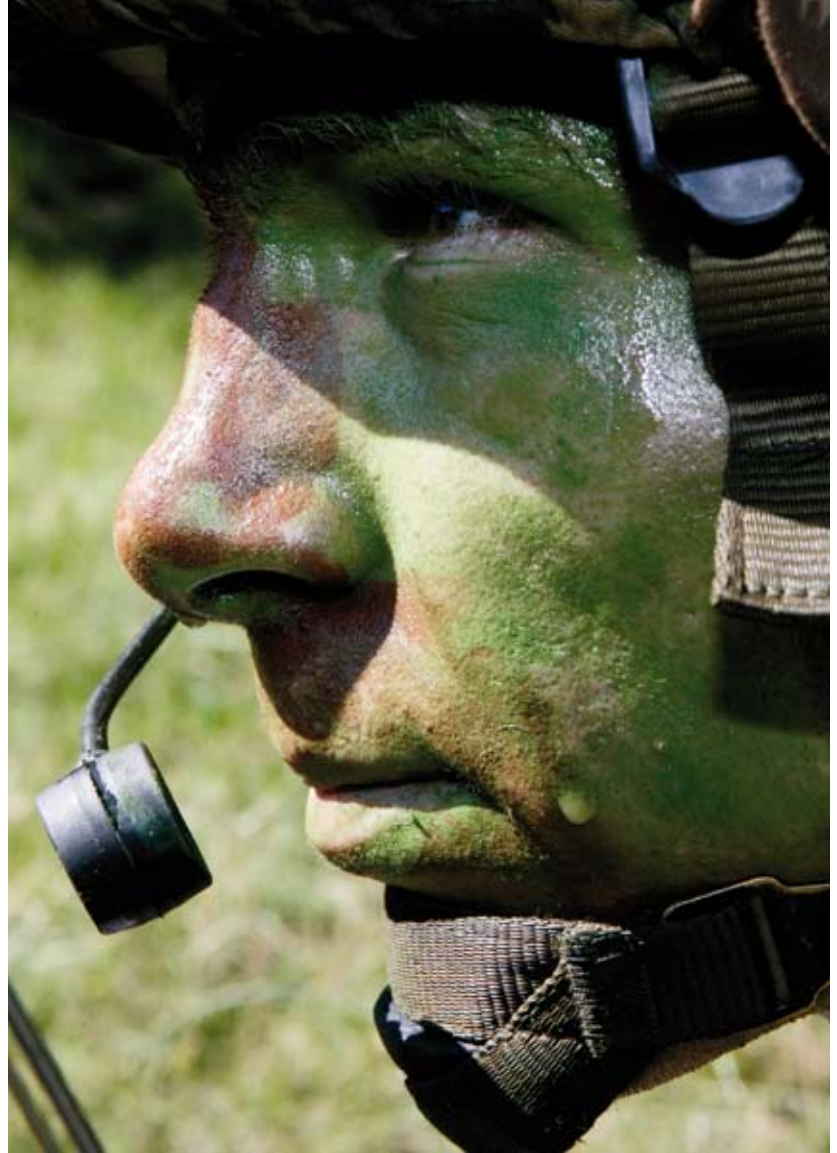


armed forces, this means fulfilling their current responsibilities with less personnel and material than before. The practical solution may be to have a modern, end-to-end system that processes and assesses the data with a large number of distributed sensors, including satellites. With this database, small and flexible units can reach the hot spots more quickly and take effective action. Larger areas can also be monitored with relatively little effort using this approach.

Systems such as these can be put in place using highly effective networks that have been reduced to a handful of basic protocols, and the investments involved are actually less in relative terms. Renowned experts estimate that one euro invested in NCW has the same effect as ten euros invested in heavy combat equipment.

Asymmetry and decentralisation

One main trait of the asymmetric threat is the shift of (potential) threats or conflicts to peripheral areas, not just geographically but also in terms of the size of organisations, groups of actors and infrastructures. This means more information and more decision-making power are also pushed to the edge of the organisation than was the case before, so the edges have become more agile. The main headquarters now merely stipulates the goal; the ways and means are effectively decided on site. This means, for instance, that provisions must be made at the front to ensure that the units along the different sections of the front have access to each other's information. They can then form a more accurate picture of the overall situation and use this knowledge to decide on the next steps to take to achieve the goal set for them. This principle known as "power to the edge" does not contradict the control circuit for command and control. Instead, subordinate control circuits are introduced into the system to improve the accuracy of



command and control for the system as a whole. In terms of communication equipment, power to the edge naturally means there is a greater exchange of data at the edge, which lightens the load of networks elsewhere. This fact must be taken into account when the infrastructure is planned.

This approach is what ensures an effects-based operation (EBO). The armed forces do not carry out their mission in a vacuum or on a relief map or in a sandbox. They do so in a polygon whose legs link mission, national and multinational interests, demands from the local civilian population and environmental concerns.

Coping with latent threat

Asymmetric conflicts can begin at a very low level, completely inconspicuously. Who would have dreamt before 9/11, for example, that flight schools and their training

programmes should be analysed and maybe even kept under surveillance? Or who would have imagined until recently that US Defense Department computers are in fact vulnerable to outside attacks involving cyber war methods?

Contemplation of what all could add up to a latent asymmetric threat profile and what measures would be appropriate to avert that threat must start at a much earlier stage. To put it more realistically, asymmetric war is raging all the time. The only question is the degree of latency involved. The corresponding risk profiles can only be drawn up if the specifics of the country or culture involved are taken into account. The quality of the profile will determine the success of any operations that may later prove necessary.

In this sense, an expanded EBO approach is highly significant. In

the effects-based approach to operations (EBAO), an attempt is made to foresee all possible consequences of (semi-)military action for every possible military action or threatening action (knowledge base development). This information is saved in a knowledge database. Once a goal is defined, EBAO is applied to help filter out the actions necessary for goal attainment, actions that harm the fewest interests or that incur the least collateral damage (effects-based planning). To keep the opponent's air force on the ground, for instance, you can destroy the aircraft or the airfield. If you do the former, you strike a blow only at the opponent's attack forces; if you do the latter, you render the airfield unusable for later humanitarian and other civilian flights. The actual operation (effects-based execution) is followed by an assessment (effects-based assessment), which in turn is saved in the knowledge database.

Via which channels should this data be communicated in times of (ostensible) peace and in which data memories should it be stored? Unfortunately, people continue to be quite nonchalant about this question, even today. But it is a non-issue, really. Highly confidential plain-text data circulating in networks used by the public may as well be printed in the morning paper...

Convergence, global networking and global risks

It is obvious that networking itself brings "everything" together and opens up positive and negative prospects. The question is this: How does a country or a community wish to handle a situation when aspects of security are at stake? Having a trend under control means knowing everything about it or at least as much as you can. This is the only way to prevent cyber war and information warfare from becoming haunting and perturbing presences in modern society. It could be desirable to teach logical and physical security



as subjects in school. There are so many others with a much less lasting effect. At the very least, society might then develop a basic awareness of the measurable effects of global electronic networking.

NCW is just as subject to and profits just as much from current trends as civilian ICT as a whole, trends like increasing integration, standardisation at all levels, convergence of technologies and expanded networking, greater flexibility and decentralisation. An NCW network of this kind must be protected from outside attack regardless of the technology used. It cannot be left up to users to decide which information to encrypt and which not to. All information in the network must be encrypted. "Always on" is the iron-clad rule. The information must be protected from access and manipulation at all times. Each sensor, each effector out there on the edges must have encryption and decryption capabilities. The same holds true for operational control systems and command and control information systems in which information is processed, condensed and further processed.

From this standpoint, the implementation of information security solutions is a job for experts. Expertise on the protocol and network technologies employed is just one side of the coin. The other side entails understanding the users'

own individual operating scenarios. Security in the NCW environment is by no means a ready-made product. There is generally too much at stake for that. ■

THE COMPLEXITY OF TRANSMITTING MILITARY INFORMATION

Fending off cyber attacks on our data networks has become part of everyday life. In our personal lives, we have to see to infrastructure protection ourselves. The government and armed forces, however, are expected to maintain maximum security against the dangers of the modern world.

Gabriela Hofmann, Corporate Editor, interviewing Divisionär Andreas Bölsterli (a rank equivalent to major general), Chief of the Armed Forces Planning Staff



Divisionär Bölsterli, how important do you think secure information transmission is in the Swiss Armed Forces in this digital information age?

The way we treat information security, security in the transmission of sensitive information, is crucial. Digital data, such as an e-mail, for example, is like a postcard. You throw it in a letter-box and hope it makes it to the recipient. It goes through many hands on the way there. If someone has the right expertise, he can read the message, alter it or even destroy it. Another danger is non-secure data lines. Outsiders can take over these lines and flood the servers with mass e-mailings in an attempt to paralyse the attacked systems or to make them crash. This scenario materialised two years ago in Estonia. A cyber attack was launched from Russia in the form of mass inquiries sent to the government, causing the ICT infrastructure of this Baltic country to collapse.

Are attacks of this kind conceivable in Switzerland?

I think we are much too casual, fatalistic and negligent in the way we deal with sensitive data. The risk and relevance of data espionage and data theft are not fully appreciated; in fact, they are often underestimated. It seems to me that the government and federal officials responsible for data security in particular show too little awareness of the importance of this issue. And they persist in doing so even though the recently published mid-year report of the Reporting and Analysis Centre for Information Assurance (MELANI) recognised these real threats as such and made repeated mention of them. Or consider Ghost-Net, a network operating out of China. A lot of persuasion is still needed in this area. It is vital that the individuals responsible for these matters in parliament approve the necessary funding so it can be used to protect extremely sensitive data. The cyber attacks already mentioned are real and by no means horror stories spread by a handful of IT freaks.

Is crisis management failing in this area?

Crisis management is not failing but it should be optimised. Precisely because we know about the risks that can arise from the networks. In Switzerland today people are all taking an “every man for himself” approach to fighting digital threats. Instead of federal government, cantons, municipalities and private businesses each struggling on their

own, it would be better to have everyone working together to find joint solutions. That would generate more financial incentive, too. A number of companies can no longer afford the security measures so urgently required.

What do you think the Swiss Armed Forces can do to provide protection from cyber attacks?

The Swiss Armed Forces must stand up to this threat. With information security, as elsewhere, you face the dilemma of always trying to keep up with the latest advances. You install new firewalls, adapt them, implement new encryption methods and the attacker tries to overcome them, to find new ways to circumvent them and the whole spiel starts all over again from the beginning. This digital competition is extremely demanding and costly.

In concrete terms, the Swiss Armed Forces protect themselves by having classified information circulate only within closed networks. Of course, these security features still have to allow an exchange of messages with parties outside the infrastructure. Contacts inevitably occur with other networks that may not have appropriate protection. We have to strike a balance between handling our own system as restrictively as possible to ensure its protection and guaranteeing freedom of communication to an appropriate extent. The decisive question is this: How important is the information for the person receiving it? Does the information fall into the category



“nice to know” or “need to know”? This question must be answered prior to sending the message.

Funding must also be available for recruiting and training specialised personnel. Tough demands are placed on these specialists. As an employer, the Armed Forces must be able to offer competitive salaries in line with the labour market. The Armed Forces do have one advantage, namely their very own IT Departments within the command support units. The benefit is that, under the Swiss militia system, specialists can be assigned to the formations who deal with the same issues daily in their everyday jobs. The Armed Forces can profit from this knowledge.

Do the Armed Forces treat strategic and tactical information differently in terms of security?

Nowadays, it is difficult to divide information so neatly into these two categories. The old image of officers standing around in a tent making only strategic decisions for a battle while letting the soldiers on the front do the real “work” is outmoded. Today, if a soldier at a control point issues a command, his doing so could very well also have strategic ramifications if he behaves or reacts incorrectly.

The goal of modern command and control information systems is to make certain types of information available simultaneously to all hierarchical levels. This permeability is desirable so that all levels of the organisation can be involved. However, it does presume that the

next higher level also knows in each case what was decided at the lower levels. This permeability in communications is highly complex and renders communication extremely vulnerable. Breakpoints occur at the interfaces, providing a target for attacks.

How do those responsible for communication security in the Armed Forces deal with the use of private mobile phones, laptops, etc.?

Anyone who disseminates classified data is liable for prosecution. According to routine orders, soldiers are prohibited from making recordings and posting them (e.g. on YouTube). Use of mobile phones cannot be banned totally, though; that would be counterproductive. Clear limits have been set, however, for the use of private hardware and software. All data implemented in the closed network is monitored by special interfaces before being released and approved as information.

Divisionär Bölsterli, thank you very much for this interview! ■

Personal details

Divisionär Andreas A. Bölsterli (1953), married, 3 sons

Career

- Law studies
- 1982 Entry into the instructors corps
- Subsequently trainer in schools and in courses for the infantry
- From 1995 trainer at Commanders and Staff College, Lucerne
- 1998–1999 Continuing education at Fort Leavenworth, USA
- 1999–2000 Military reform project “Armed Forces XXI”, Bern
- 2001 Commander for supplementary Courses 1 and 2 at the Swiss Military College at the ETHZ (MILAK), Zurich; (ETHZ = Federal Institute of Technology in Zurich)
- From 2002 Brigadier General, Chief of Staff Field Army Corps 2.
- From 2004–2008 Operations/ Planning in the Swiss Armed Forces Joint Staff, Deputy to Chief of the Armed Forces Joint Staff
- Since 1.6.2008, Chief of the Armed Forces Planning Staff as Divisionär, Bern

Military

Commander of an infantry battalion and an infantry regiment, also General Staff Officer assigned to various positions.

COMMUNICATION: AN IMPORTANT PART OF OUR MODERN WORLD

Communication is an absolute necessity in our everyday lives. We use communication in a variety of forms: writing, spoken speech, diagrams, even images. Each form has its own advantages. Communication today depends heavily on the world of radio communication, which enables information to be transmitted over long distances. This technology, in turn, relies on transmission methods that are very easy to eaves drop.

By Tim Harms, Product Manager

Dependency on telecommunications, particularly radio transmission, is also an issue for land-based (military) armed forces. Communication is a vital channel in the chain of command. An interruption or interception of communications can have grave consequences for resources, costs, and timetable, and not least, for the success of the operation. It is vital that communication in a military scenario be conducted independently of the vulnerable communication infrastructure in the civilian world. Land-based and other armed forces need an independent infrastructure that is mobile and combat-ready. For short distances, this function can be performed by dedicated military fibre optic networks, microwave links and VHF/UHF radio systems for line-of-sight communication. Over longer distances, HF radio is the only infrastructure-independent technology that allows point-to-point and broadcast communication.

These transmissions can be easily tapped, however. For this reason whenever highly sensitive informa-

tion is involved, protective measures must be taken. In the civilian world, the use of communication encryption is ever more widespread – https, VPN and other security methods have long been part of our everyday Internet use and provide vital protection from tapping and the misuse of information. Message encryption has long been standard practice in politics and in military settings.

The new HC-2650 Encryption unit

The goal of Crypto AG is to achieve the highest level of information security and the best quality of communication in all its forms. Customers can communicate securely and with ease thanks to the seamless integration of security and transmission quality in products from Crypto AG. One of the best known products from Crypto AG for this purpose is the MultiCom Radio Encryption HC-2650 unit. It enables the ultra-secure transmission of voice and data over HF, VHF and UHF connections and now IP-based networks.

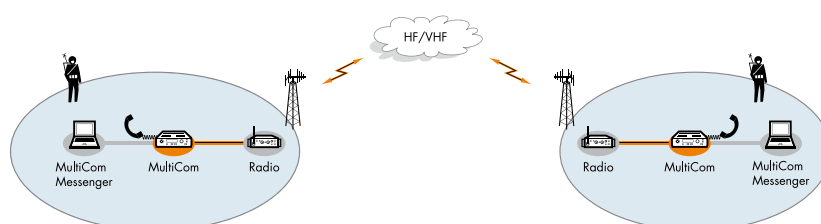
MultiCom Messenger

One of the latest additions to the MultiCom product palette is the MultiCom Messenger. Teamed up with the MultiCom HC-2650 Encryption unit, the MultiCom Messenger allows secure e-mail services over radio channels and complements the voice and other services of this product. The end user thus has a choice of communication options for the most varied types of communication. This communication is secure and completely independent from standard networks.

The MultiCom Messenger platform is based on the STANAG 5066 standard. This STANAG standard offers standardised, flexible user access points for different applications over the same communication channel. If they are connected to the HC-2650, the transmitted information is protected by ultra-secure solutions from Crypto AG.

Wide variety of possible combinations

MultiCom Messenger allows users to exchange e-mails, diagrams and photos securely. Users can opt for



MultiCom Messenger in a point-to-point scenario and a broadcast scenario with individual radio nodes



the internal modem of the HC-2650 or continue to use an external modem if they already have one. Messages can be transmitted either in ARQ (Automatic Repeat Request) confirmation mode in point-to-point communication, or in Non-ARQ/FEC (Forward Error Correction) mode for broadcast, or in radio silence mode.

The voice service of HC-2650 is naturally also still available as a parallel feature. In other words, a single encryption unit can be employed for messaging and voice communication.

MultiCom Messenger Gateway

The system options are not just confined merely to point-to-point and broadcast radio connections. MultiCom Messenger has further components that enhance the networking capabilities compared to other proprietary transmission systems. With the MultiCom Messenger Gateway, the MultiCom Messenger System can be integrated directly into most commonly used server environments, allowing direct access to remote stations via e-mail from any location within the network. This feature saves time and reduces the risk of human error in the transmission of messages.

IP VPN encryption

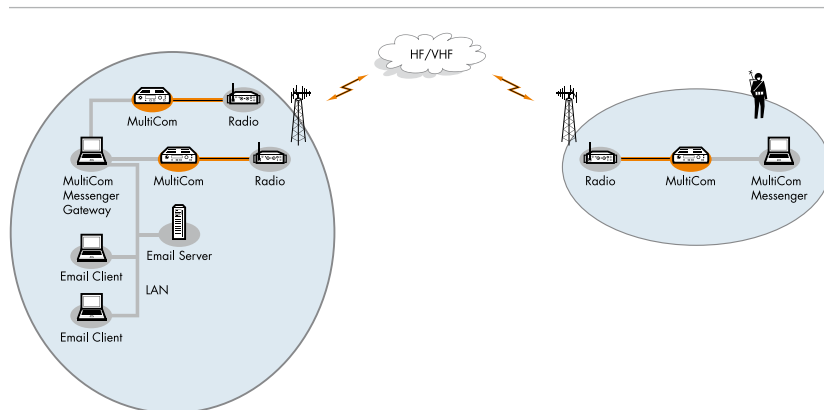
In addition, the MultiCom HC-2650 can also be employed as an encryption unit for IP VPN networks to establish secure WAN connections in the MultiCom Messenger

network. Using the HC-2650 for IP VPN encryption also saves time and money in logistics and personnel training.

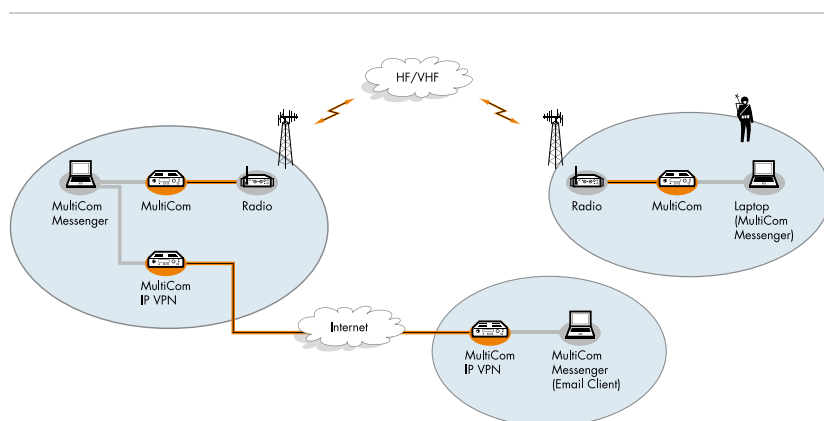
System components and services

Crypto AG also has an extensive range of system components for system construction that are ideal for creating these types of messaging systems. Ruggedised laptops, servers, Ethernet switches, RS232 switches and other standardised

components can be combined with each other to assemble flexible standardised systems for meeting specific requirements. On request, Crypto AG can also configure and integrate the MultiCom Messenger components in a legacy system or deliver a completely new turnkey network. ■



MultiCom Messenger Gateway



Use of the HC-2650 with IP VPN application to provide security for a MultiCom Messenger network

HC-2650: THE LATEST ADDITIONS

The MultiCom Radio Encryption HC-2650 unit from Crypto AG is unbeatable in ensuring secure mobile communication. The universal platform provides convincing security for all voice and/or data communication transmitted over radio no matter where it is used, in a regular or armoured vehicle, in a helicopter, aeroplane or ship.

By Tim Harms, Product Manager, and Martin Maron, Senior Product Manager

Flexibility, reliability and future expandability were the challenges set for the design of this unit. But the design engineers did not stop there. To meet the demands for operation both in tight spaces and in a large operational centre, yet another function was incorporated: remote control. This flexible remote control option opens up new possibilities for the technical and operational remote control of the MultiCom Radio Encryption unit.

When space is at a premium

A space problem always exists in mobile operations. Units must



Remote control features of the MultiCom HC-2650

satisfy myriad requirements when used in mobile military environments. They have to withstand vibrations, power failures, and extreme light and temperature conditions. Ease and simplicity of operation are paramount in these circumstances.

The latest product in the HC-2650 remote control family is ideal for use in tight spaces. With the Remote Control Unit RCU-2650 from Crypto AG, users can operate an HC-2650 encryption unit from a

remote position. The focus is on control and status functions necessary for operations. The RCU-2650 is extremely small, allowing it to be integrated into almost any environment with no reduction in operational functionality.

The RCU-2650 is available in different models and for a variety of applications, e.g. for regular and armoured vehicles, for helicopters and aeroplanes and, in a 1U 19" format, even for rack or panel installation involving multiple units. The various models are based on a common module (remote control module), but have different front and mounting panels.

Designed for special environments

At headquarters, in command posts or on larger vessels, MultiCom HC-2650 units are often found in a centralised arrangement in a machine room along with other communication equipment such as modems and radios. Beside the RCU-2650 there are two other methods for remotely controlling these separate MultiCom encryption units. The first involves use of remote control software (RCS-2650) from Crypto AG. With this software installed on the workstation PCs, all encryption units installed at this location can be controlled completely and be supervised seamlessly.

The second remote control option is known as CLI (Command Line Interface) and consists of a set of commands with which the HC-2650 can be controlled. A customer or



RCU-2650-01 in use in a helicopter

system integrator can use it to control the encryption unit and other communication components such as modems, radios etc. with an own, homogeneous and dedicated user interface. ■

ETHERNET ENCRYPTION FOR NEXT GENERATION NETWORKS

ETHERNET MULTIPOINT ENCRYPTION

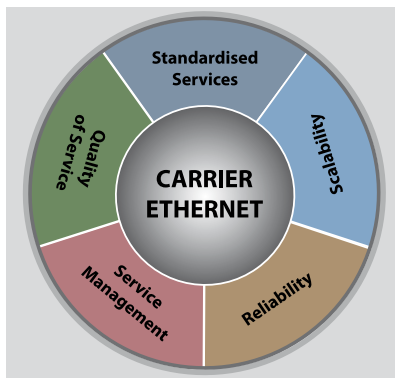
In recent years Ethernet has developed rapidly to become the main network communication technology (in conjunction with IP) for organisations (public authorities, armed forces) and companies of every size. Ever increasing location networking alters the communication in organisations and companies, and demands faster and more secure processing of the increasing digital business processes.

By Willy Landolt, Product Manager

This structural change requires support from appropriate information and communication technologies in order to ensure cost advantages and guarantee investment security. Ethernet is the intelligent choice when it comes to networking locations and computing centres efficiently.

Standardised networks

Carrier Ethernet networks are standardised by the Metro Ethernet Forum (MEF, www.metroethernet-forum.org). This describes the attributes such as Standardised Services, Scalability, Reliability, Service Management and Quality of Service which define the Ethernet service specifications.



Carrier Ethernet attributes (source: MEF)

Standardised Services

The Standardised Services area defines the transparent Private Line and Private LAN services. The Service Access Point between client and service provider or end user and network operator is formed by the User Network Interface (UNI) which defines all the service features in the Service Level Agreement (SLA).

Two or more locations are connected with each other using Ethernet Virtual Connections (EVC) which are either point-to-point or multipoint-to-multipoint connections.

The EPL (Ethernet Private Line) and EVPL (Ethernet Virtual Private Line) are based on the point-to-point EVC, and the EPLAN (Ethernet Private LAN) and EVPLAN (Ethernet Virtual Private LAN) on the multipoint-to-multipoint EVC. In contrast to the port-based EPL and EPLAN types of service, the EVPL and EVPLAN services provide service-multiplexed interfaces. The EPL service therefore corresponds to the traditional LeasedLine whilst the EVPL service corresponds to an ATM or FrameRelay service.

Scalability

Scalability refers to the gradation of bandwidths in steps of the required size. Starting with 1 Mbit/s these can be increased in as small steps as desired up to 10 Gbit/s or more.

Reliability

Reliability (operational safety) means the ability to recognise events in the network and to restore network functionality without any effect on the end client.

Service Management

This primarily concerns OAM (Operation, Administration and Maintenance) carrier class functionality as well as the necessity of maintaining the various services and of providing a diagnosis quickly in the case of faults.

Quality of Service

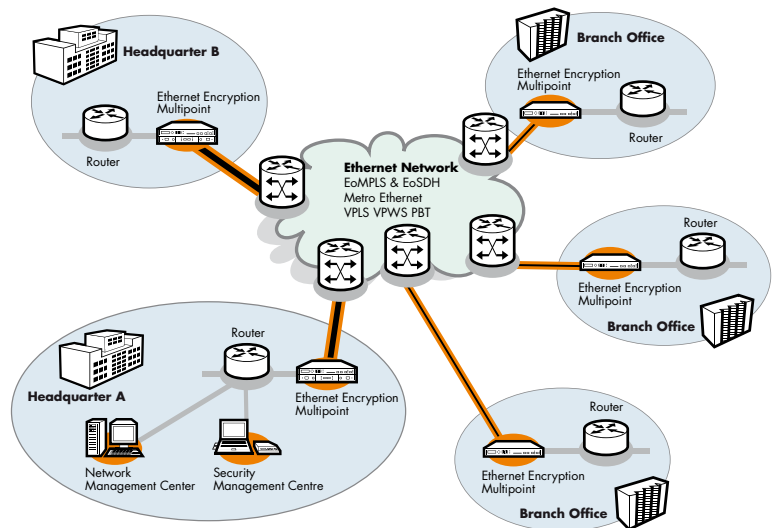
Quality of Service mechanisms are usually used to fulfil the various SLAs which define the end-to-end Quality of Service.

Ethernet encryption at the UNI

The Ethernet encryption units HC-8550 and HC-8552 are suitable for protecting communication in Carrier Ethernet or Metro Ethernet networks. These universal and flexible encryption platforms provide a broad application in the most varied network topologies. The HC-8550 100 Mbit/s platform and HC-8552 1 Gbit/s platform are designed as 19" rack versions and have high availability due to redundant power supplies and fans. The units are highly suitable for use with Ethernet over MPLS (EoMPLS), Provider Backbone Transport (PBT), Ethernet over SDH (EoSDH) or Metro Ethernet networks. Ethernet encryption units have a modular design so that the appropriate configuration can always be used, from entry scenarios with low bandwidths, few peer locations and no class of service up to multi-application networks with high bandwidths, many peer locations and traffic prioritisation.

If configuration changes are due in the network, the units can have the latest software version implemented in the field using a local or remote update or can be equipped with additional features using a remote or local upgrade. The combination of basic hardware and software and the appropriate auxiliary modules provides the client with a configuration tailored exactly to his needs.

Ethernet encryption units have been tested and installed in various MEF network scenarios (EPL, EVPL, EPLAN and EVPLAN) many times over. The HC-8550 and HC-8552 encryption units have been successfully integrated into different networks (incl. EoMPLS, EoSDH) in current projects. This involved importing the different communication topologies, such as FullMesh or Hub&Spoke, into the encryption units in accordance with the specifications. In relation to performance, maximum throughput is achieved before and after encryption due to the constant frame length (no frame overhead).



Carrier Ethernet Network

For traffic prioritisation, Ethernet priority bits (802.1p) or VLAN tags (802.1q) are used. Double tagged (Q-in-Q) frames are also supported. Ethernet encryption often forms the security for the basic transport network at the service access point. Depending on the requirements, additional encryption can be installed on this encrypted network at a higher level (IP, application).

The Crypto Security Management Centre SMC-1100 is used for security management. Network management can be handled using the Crypto RAD-1100 Remote Access Device and commercial SNMP management systems.

Future-oriented

Ethernet has retained its status as the preferred transport system for progressive services such as IP, telephony, video streaming, medical imaging and data storage. The factors responsible for this are high availability, granular bandwidths, reduced investment, low operating costs and a seamless interoperability with existing broadband technologies. This gives the client a simple and step-by-step migration from legacy networks (FrameRelay, ATM, LeasedLine) to modern Ethernet networks. Furthermore, Ethernet is a mature and sophisticated technology for which organisations and companies already have skilled personnel. ■



HC-8550



HC-8552

SERIES ON CRYPTO SERVICES (IV)

ICT SECURITY CAN BE LEARNED

A chain is only as strong as its weakest link – or, applied to ICT security: the best information security or encryption solution is only as good as the people who install, configure, use and maintain it. This is why Crypto AG has been running its own Academy for the training and professional development of specialists in all relevant areas for decades.

By Rudolf Robbi, Head of Education Services

It is well known that the often-quoted “human factor” is of key importance especially for information security. But in order for a security solutions provider to actually be able to deliver the essential know-how themselves – in the required quality and technical breadth – they require a suitable infrastructure, including professional teachers. This is why Crypto AG has been running its own Academy with full-time instructors, five modern classrooms and a spacious cafeteria for decades. The Academy has developed into a true showcase for Crypto AG because clients gain far more insight into the company philosophy during courses than is possible from the outside.

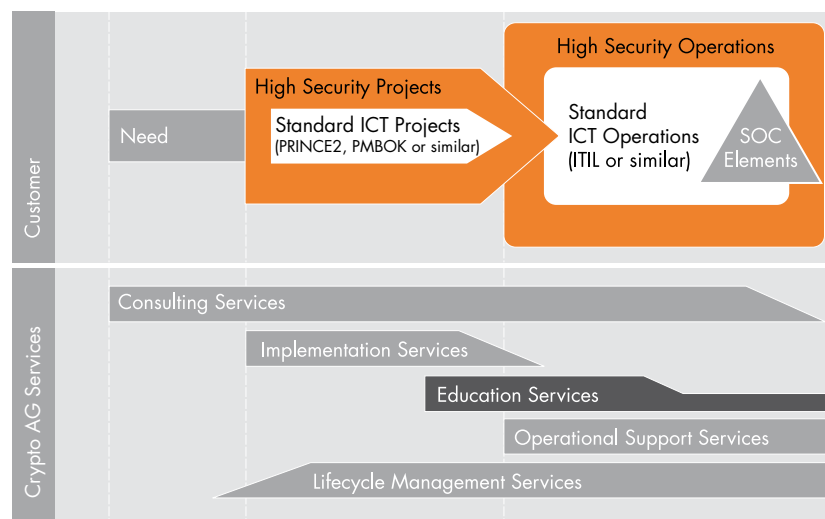
Tailor-made courses

Anyone wishing to keep pace with technical progress needs to make consistent investments in training. Secure communication protected by encryption can only be guaranteed if all the devices involved are configured and used correctly. This goal can be achieved by means of professional training. The training material is agreed and designed individually for the needs of each client. When planning the course, any gaps in knowledge are remedied and prior knowledge taken into account. The course length can vary accordingly. The aim is to train the client to be able to pass on his acquired knowledge to other users as an instructor in his own organisation (train the trainer principle).

All course leaders speak several languages, are trained in education and teaching methods, and have at

least five years’ experience in adult education. Due to travelling all over the world and active contact with our clients, we are familiar with

course together for reasons of sovereignty. Groups made up of people from different countries can only be instructed together when the project



Education within a project for high-security operations

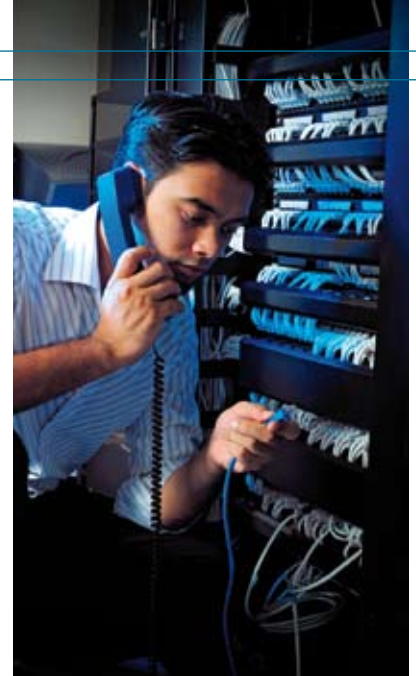
their different cultural backgrounds. The company’s customer restaurant offers meals which take account of religious requirements. We also supply appropriately furnished rooms for religious practices. We attach great importance to personal contact with our clients, including outside the training sessions. This includes excursions to see the attractive Swiss countryside. Competent and experienced course leaders are usually in charge of the same group for the entire course. “Swissness” is therefore interpreted as a quality concept for company performance overall and not just as “Swiss made”.

Our training courses can also be run on site for the client. As we operate in the high-security area, only participants from the same organisation can take part in the same

requires this and the participating countries have given their consent. Each training course concludes with the presentation of diplomas and a small personal gift.

From network technology to security management

Encryption technology is always an integral component of information and communication technology. Information security must therefore be incorporated directly in the project schedule when developing ICT infrastructures. Due to the mutual dependency of encryption (cryptography) and networks, it makes sense to offer clients appropriately structured basic ICT training as well as specialist training on units. Training courses for specific functions can be arranged individually depending on the client’s existing knowledge base or lack of



it. The following short overview of the range is naturally not exhaustive.

Encryption technology for network specialists

IP VPN networks have been set up in many places in recent years, a trend which is continuing. Copper wires are increasingly being replaced by fibre optic transmission lines which are able to transmit data with increasingly large bit rates. This evolution is influencing the educational infrastructure. Along with the latest generation of encryption units, we are constantly developing new training modules in order to give the client as much practical knowledge as possible.

Each participant in the small groups practises typical configurations with their own unit set. The characteristics and special features network of the new units can be explored under guidance. Participants are introduced to more demanding tasks step-by-step. At the end of the training course, participants must be able to carry out configuration and maintenance tasks independently with the goal of being able to correct "engineered" faults as quickly as possible.

High-security projects for system integrators

In more complex projects our encryption units are dealt with by system integrators commis-

sioned by the client. The interaction and correct implementation of the equipment requires specialist knowledge not possessed by all the parties involved. We are the specialists when it comes to encryption and can pass on our knowledge to the integrator. Our clients therefore benefit directly and indirectly from the extensive experience which we have gained in the course of various projects. By focussing consistently on practical applications and providing efficient training for specialists at a high level, unnecessarily long (and therefore expensive) courses plus loss of working time and high travel costs can be avoided.

Design and operation of secure radio systems

The centres of conflict in recent times show that wireless speech and data communication via radio is gaining in importance again. With the HC-2650 MultiCom System, Crypto AG has developed a military platform that satisfies every requirement. Speech, data and IP communication can now be encrypted with one and the same unit. However, the complexity of the unit's multifunctionality demands a sound training, whilst customised adaptations which require many years' experience need to be dealt with during implementation (e.g. on ships and in helicopters).

What applies to installation is also true of operation. The system of

antennas, amplifiers, radios, intercom systems and encryption units requires fine-tuning which can only be optimised using a series of painstaking tests.

Technology know-how for telephone security

Technological change is also making itself felt for telephone networks operators. In the course of the privatisation of public networks, there is an unmistakable trend towards speech and data compression. Even old transmission lines are now used to transmit data as well as speech. At network gateways, i.e. where old and new meet, undesirable effects can crop up which have particularly disastrous consequences for encrypted data traffic. For this reason, encrypted fax and telephone traffic suffers more frequent faults, leaving badly trained operators completely at a loss. Experience shows that all organisations are affected by network deregulation. Those who subscribe to the services of a state monopoly are powerless to avoid the general trend. When it comes to cross-border telephone traffic and communication via satellite, if not before, problems can become apparent. Telephone specialists can benefit from a refresher course. Sensitive areas in telecommunications are looked at in more detail using hands-on training units. The client is familiarised with the latest upgrades, and



methods of protection against unpleasant surprises are demonstrated.

ACC for cryptography and security specialists

Anyone who is familiar with the philosophy of customised algorithms understands the numerous mechanisms which make our encryption units so secure. The ACC (Acceptance Cipher Check) enables the functions of relevance for encryption to be checked. This training course is aimed at those responsible for quality and evaluation of new encryption units. ACCs are only carried out in Switzerland and only for people who possess the relevant authorisation. Before the actual ACC training, the client receives a short course on the relevant unit. The first part of the course explains how to get data from the unit. In the second part, the cryptologist from Crypto AG explains the method of operation of the customised algorithm and hands over the necessary means of verification.

Individual special courses for VIPs and security managers

We offer special training courses for VIPs and security managers to familiarise them with the application scenarios of our units. Security managers are responsible for the implementation of an organisation's security policy in the ICT field and therefore need detailed know-

ledge of the processes used in the system and how they are controlled. More generally, managers should have a picture of the job profile that an employee has to fulfil. An important basic principle is that a training course requires a minimum of basic technical knowledge in order to be completed successfully. This is provided based on the individual requirements. Specialist terminology is acquired by working together on simple scenarios which comprise alternating theoretical and practical sequences.

Visitor services from A to Z

The clients who take our training courses have very often had a long flight and experienced a time shift and change of climate. It is not always easy to get your bearings in a new cultural environment. We therefore attach great importance to a high standard of accommodation which is available in good hotels close to Crypto AG. Transport is provided by our own chauffeur-driven vehicles.

Clients who prefer to live in an apartment or to cook for themselves can use Crypto AG's spacious five-room apartment in the town of Zug. We cater for the well-being of our clients from collecting them at the airport at the beginning of the course to delivering them there at the end. ■



PORTRAIT: LAND FORCES

When you talk about land forces, this immediately evokes the picture of fully laden infantry or convoys of tanks. This picture is correct in as much as the infantry and tank forces are in general the largest units. But without the assistance of other corps such as artillery, anti-aircraft, engineers, communications, rescue and medical corps as well as logistics services – and without their incorporation in the strategic and tactical communication networks – national sovereignty goals would be impossible to achieve.

By Rudolf Stirnimann, Customer Segment Manager



In most countries, the army's remit is defined along similar lines by the political leaders. The central task is the safeguarding and defence of the realm, followed by subsidiary operations for safeguarding livelihood, i.e. supporting civil institutions during natural disasters, major national and international incidents, and peace-keeping (e.g. support for UN peace-keeping missions). To carry out all these tasks requires the deployment of land forces. After reconnaissance by the air force, the army enters and secures the territory. Protected by the air force, the army fights forward on the ground and secures supply lines.

The number of communication methods has multiplied for the land forces just as it has in economic sectors and civil government agencies. This enables efficient and secure transmission of information at the highest level.

For international operations, communications which function well and are interception-proof between all the units involved need to be reliable even across borders. Securing these connections between the different participating organisations under all circumstances requires the parallel and redundant operation of a wide range of channels and technologies.

Strategic communication

On the one hand, this involves strategic networks for the area of logistics and administration. These are nationwide connections for the transmission of speech, images and data using fibre optic, wire, radio and directional radio connections. The transfer of this valuable strategic information requires interception security, integrity and authenticity (Comsec). It is therefore essential to transmit this information in encrypted form. Fail-safe transmission is ensured by networking with redundant and substitute paths.

Tactical operations

On the other hand, tactical networks are set up and operated temporarily for operations in the field. The emphasis here is on speech and data transmitted by mobile radio and directional radio connections. This information is highly sensitive and time-critical, so has to be made interception-proof by means of encryption. In addition, interference-proof transmission can be achieved using frequency hopping in the case of radio (transmission security – Transsec).

For operations in remote areas, operational command and headquarters are kept in constant contact with the top levels of army command by means of satellite connections and also short-wave radio (HF) if need be.

Support from Crypto AG

Information security in the operational scenarios mentioned is reliably guaranteed with, for example, the MultiCom Encryption HC-2650 from Crypto AG. This sturdy and mobile unit encrypts speech and data for transmission using HF, VHF, UHF and satellite, and can connect securely to the strategic core network using VPN with the IP VPN application mobile units. Our application-specific systems secure all applications (fax, telephone, e-mail, FTP, etc.) and protect communication connections between stationary and mobile units. Crypto AG not only develops encryption units but also supplies complete security solutions for integration in existing ICT. We support our clients with customised services in every project phase and during the entire lifetime of their security solution. ■

FRESH IMPETUS FOR PROGRESS – THE TREND TOWARDS DIGITAL ELECTRONICS

Even in the early 1960s, the trend towards electronics and digitalisation could be recognised in the development of encryption units. The changeover happened with the “integrated circuits” (IC) already available, which could be used to develop arithmetic circuits. Crypto AG switched directly from electromechanics to the discipline of microelectronics and was the first company in Europe to implement “IC” industrially. The era of tubes and transistors was bypassed, apart from a few applications for special devices.

By Gabriela Hafmann, Corporate Editor

The advantages of the new technology were obvious: the electronic units had improved operating characteristics, greater flexibility, more automated functions and in most cases they weighed less. In addition, electronics enabled the use of more complex cryptographic arithmetic procedures, primarily by making use of what was known as the shift register. The increased operating speed of the electronic units also enabled messages to be encrypted much more rapidly. At the same time, the greater degree of cryptographic variability provided a very high level of security.

Transition technology in the learning phase

The actual “transition unit” was the punched tape cipher machine RTE-5 (WUMA) which worked purely mechanically to begin with. Improvements were carried out in such a way that only a minimum of mechanical features remained and compatibility with the new, 100 baud (1 baud = 1 bit/s) fast telex machine could be achieved as far as possible.

Its successor, the electrically operated RTE-59, was developed specifically for use in communications organisations which were using mechanical punched tape decoders. It had no printing facility and was therefore always linked to a telex page printer which functioned as the output device. As an input

device, the RTE was also of limited use because it did not permit a direct

keyboard input but text had to be entered using punch tape.



RTE-5



T-450 TROL

The first fully electronic cipher machine

The first real milestone in this new era was the legendary fully electronic T-450 machine. It was also called the CRYPTROL (TROL for tape and rotorless online), so was a unit lacking any moving mechanical parts and was used for online operation along with telex and radio telex encryption.

Thanks to its great flexibility – the TROL could be operated with telex machines from almost every manufacturer – it was a huge success. Its main use was in military applications as well as diplomatic services and stationary and mobile networks. In the commercial realm, many postal administration centres connected this unit to their telex services. The T-450 was soon in use all over the world. It could be used in synchronous and asynchronous mode with a speed of 50, 75 and 100 baud, using radio links and wire and telex connections. A five-bit code (CCITT No. 2) with speeds up to a maximum of 100 baud was used, enabling the production of 15.3 characters per second.

The text information arriving from a telex in five-bit code was sent to the T-450 where it was converted into binary information (digitised). Encryption took place using key information from the key generator controlled by individual modules. This information was enabled by C-MOS technology¹. The T-450 receiving station (equipped with the same base and message key as the sending device) received and deciphered the message, then relayed it to a telex machine which printed it out.

The base key was formed from 25 letters, allowing 2.5×10^{35} combinations. The message key consisted of five letters, corresponding to 1.1×10^7 combinations which were generated using a teleprinter keyboard or by means of random selection of the letters by the internal key generator.



The customers had the option of programming the key information themselves in a key generator consisting of JK flip-flops². If necessary, the message received could be kept in encrypted form to be decoded offline later. Thanks to a “highly stable clock generator” the TROL remained synchronous in a short-wave network as well, even during long interruptions to reception due to fading or atmospheric disturbances. The synchronous operation guaranteed that sender and receiver always used the same key information, thus making use of “start/stop” synchronisation.

Text encryption in offline mode

The desire for short transmission times led to an increased demand for connection encryption. However, interest remained for purely

local cipher machines which could be used for special areas such as encryption of strategic messages with a very high security classification.

The line-independent semi-electronic H-460 cipher machine was developed specially for offline operation. This was able to encrypt 7.5 characters per second (5 characters plus 1 start bit plus 1.5 stop bits). The encryption principle was identical to that in the T-450 (TROL). The input keyboard with reed contacts⁵ developed in-house enabled entry of the necessary secret key and of clear or encrypted text. The base key here consisted of 26 letters, corresponding to 26^{25} or 10^{35} combinations, the message key of five letters which could produce 26^5 or 10^7 key combinations.

CCITT No. 2 Five-bit Alphabet

CCITT No.	32	5	28	31	27	20	1	9	14	15	19	18	8	4	12	26	21	3	13	6	7	10	16	23	2	25	11	22	24	30	17	29	
1		●					●				●		●		●	●	●		●		●	●	●	●	●	●	●	●	●	●	●	●	●
2			●					●			●		●		●	●	●		●		●	●	●	●	●	●	●	●	●	●	●	●	●
3	●			●					●		●		●		●	●	●		●		●	●	●	●	●	●	●	●	●	●	●	●	●
4					●				●		●		●		●	●	●		●		●	●	●	●	●	●	●	●	●	●	●	●	●
5						●			●		●		●		●	●	●		●		●	●	●	●	●	●	●	●	●	●	●	●	●
CCITT No. 2	E	≡	≡	≡	<	T	A	I	N	O	S	R	H	D	L	Z	U	C	M	F	G	J	P	W	B	Y	K	V	X	Q	↓		
	3					5	-	8	,	9	`	4	☒	☒)	+	7	:	:	☐	☐	☐	☐	0	2	?	6		=	/	↑	↑	

- Space (A)
- Mark (Z)
- Letter shift (LS)
- Figure shift (FS)
- Space (SP)
- Special symbols for national use
- Bell
- Carriage return (CR)
- Line feed (LF)
- Who are you (WRU)
- Not to be used

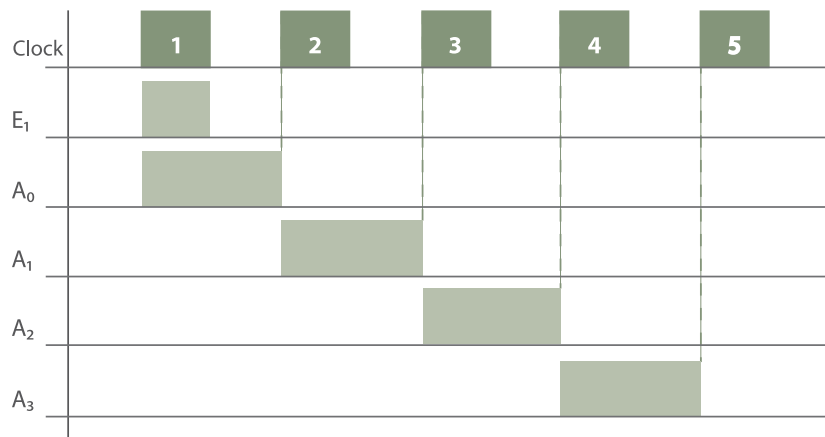


Even back in the age of the telex, information was transmitted between the parties in a digital manner. Coding was usually executed with punch tape on which five bits could be written width-wise. The status 1 and 0 were represented with a hole or no hole. All the characters required could be represented for each bit. The telex transmitted the bits using sounds in the audio range. For encrypted messages, the characters could be punched at the cipher machine output and then sent via the telex's punch tape reader (offline mode). Later, communication took place in online mode – i.e. directly using the five-bit code from the cipher machine on the sending telex.

As in the TROL, a group of five letters were printed as clear or encrypted text on two parallel strip printers (similar to the C-52 series, see *Crypto Magazine* 1/2009, page 12 ff). However, for punching the cleartext strips and the encrypted information, the machine required an additional external device (PEH-72), so that the messages could be punched onto punch tape and used for online operation with the telex machines.

Text encryption in online mode

With what was known as the online system, the cleartext for encoding was entered into the encryption unit using a keyboard or punch tape. The cipher machine was connected directly to the transmission line which was in turn connected with the receiver cipher machine and its printer via a wire circuit (telex network). Entering the cleartext, the encryption and transmission and, in the opposite direction, the deciphering and output of the printed text took place with almost no delay. If punch tape was used, several hundred characters could be entered per minute, depending on the set baud rate. In electronic communication links, these characters would usually be treated as a sequence of five elements (CCITT no. 2) where the elements were either 0 or 1. In this way the following five-step codes were used, for example: A = 11000, B = 10011 etc. This meant that an encryption system which was to encode around 400 characters per minute had to process 3000 bits per minute. This was quite feasible from an electro-mechanical point of view, but such a high speed was tricky, especially because the sending and receiving machines had to work completely synchronously. The typical solution for generating the key quickly and reliably in the key generator was to use what was known as the shift register (see impulse diagram), initially still constructed from very simple electronic components.



Impulse diagram

Shift registers are electrical circuits which pick up multi-digit binary signals controlled by a clock, store these and then emit them again. They operate using either serial or parallel inputs and outputs, and can be built using edge-triggered flip-flops. As a flip-flop can only store one bit, several flip-flops are connected into a shift register. If this is given an impulse at the input, this impulse propagates by one place (one flip-flop) with every clock. Source: www.elektronik-kompodium.de

Further developments

In the following years the introduction of the new digital technology was to make the development of speech and image encryption possible. From there on it was only a small step to complete systems, in other words, communication devices with integrated encryption. ■

¹ C-MOS: complementary metal oxide semiconductors are semiconductor components. C-MOS technology represents the most widely used logic family and is primarily used for integrated circuits. Source: de.wikipedia.org

² JK flip-flop: the flip-flop is a simple electronic circuit which can store one bit of data over a long period. It is a fundamental component of many electronic circuits (sequential circuits) from the quartz clock to the microprocessor. In addition, several thousand to billions of them are contained in computer chips (static memory components). Source: de.wikipedia.org

³ Reed contact: a reed contact consists of two metal tongues which are placed on top of one another in a glass housing. If the glass housing is approached with a magnet, the tongues are drawn together by the magnetic force and produce an electrical connection. Reed contacts enable contactless switching action, for example for counting and measuring applications. Source: www.bwir.de



USING MOBILE DEVICES SECURELY

Information security is not only a technical discipline but has a great deal to do with people because it depends on the conscious thinking and actions of the user. So what is a practical and safe way to deal with information and IT equipment? Crypto Magazine looks at the different topic areas, from the Internet to passwords, giving useful tips for everyday life. This fifth article in the series looks at the secure use of mobile devices.

*By Franco Cerminara, Head of Consulting and Education, InfoGuard AG**

Mobile devices are everyday objects. The extensive use of PDAs, notebooks, mobile phones and smartphones presents ever new challenges to the security of these means of communication. Every year, thousands of mobile devices with stored sensitive data are left lying in taxis alone.

Our mobile phone reminds us about appointments, the PDA guides us to a meeting using its navigation system and we use the smartphone to quickly log onto the Internet to read e-mails. The applications loaded on these devices are varied: text and multimedia news, contact data and calendar entries or confidential client information. The user often installs navigation systems, dictionaries and games. In addition, videos, photos and speech can be stored there. The devices enable access to the Internet or incorporate telephone or modem functions. A modern mobile device has access to a variety of different interfaces, such as GSM/GPRS, UMTS/HSDPA, WLAN and LAN connections, Bluetooth or USB.

Mobile devices with their multitude of hardware and software technologies should not only be protected from unauthorised access, but also integrated securely in company networks. It is unfortunately often the case that security is of secondary importance for most users, entailing extra effort, so opening the way for viruses, worms and other malware. Guaranteeing security is made harder by the fact that the devices are increasingly networked together and communicate with one another.



With the use of malware, not only can stored data be read and misused, but it nowadays requires little effort to bug a manipulated mobile device or record a location without the owner noticing anything!

In general, the same security measures apply to mobile devices as computer systems, in as much as these provide additional services beyond traditional telecommunication.

- Protect your mobile device with a good password (see CryptoMagazine 1/2009).
- Encrypt sensitive information.
- Do not use any unidentified memory cards in your devices.
- Only store a minimum of data on mobile devices and save this regularly, so that if the system crashes or breaks down not all the data is lost.
- Wireless connections such as Bluetooth, WLAN or infrared should only be activated when they are actually being used.
- Use an anti-virus scanner specifically

for mobile devices and carry out regular updates.

- Order the device from a trustworthy source so that you can be certain it has not been tampered with by the manufacturer or supplier.
- Always look after your mobile devices when out and about. ■

* InfoGuard AG, a company affiliated to Crypto AG and a member of the Crypto Group, specialises in comprehensive information security. Its fields of expertise include advice, training and awareness-raising as well as the development and implementation of technical security solutions.



Driving Information Security

For over 55 years we have developed, manufactured and implemented custom security solutions. Because we know that confidential information is of the highest value. You too can rely on the expertise and capabilities of Crypto AG – just like our customers in over 150 countries.

To Remain Sovereign

Crypto AG, P.O. Box 460, CH-6301 Zug, Switzerland, Tel. +41 41 749 77 22, Fax +41 41 741 22 72, get@crypto.ch, www.crypto.ch





PRESS REVIEW

Computer and human being – often a dangerous combination

People do not just acquire ailments when using computers, mice and keyboards – they increasingly have problems with the hardware which gets in their way. This is no longer surprising, as the number of computers and peripheral devices has grown enormously in recent years.

Scientists at the Center for Injury Research and Policy of the Nationwide Children's Hospital have recorded that, in the period between 1994 and 2006, the number of serious accidents connected to computers which required treatment in a casualty department has risen by 732 percent to over 78,000. At the last count that was 9,300 accidents per year. However, in the same period the number of computers has risen by "only" 309 percent. The place with the highest risk of injury appears to be at home. This is where 93 percent of the accidents recorded took place, according to the study which appeared in the American Journal of Preventive Medicine.

It actually appears that computers, monitors and other components literally get in the way as hardware: 36.9 percent of accidents involved people bumping into computers. The opposite also occurs, with 21.2 percent of accidents involving computers or computer components falling onto people. The most hazardous components are monitors, although since the introduction of the lighter LCD screens, the number of accidents of this kind has decreased markedly. For children under five and people over 60 years old, the hazard mainly arises from hardware and cables which can be tripped over. Injuries mainly affect the extremities, but for children under the age of 10, primarily the head.

The data which the study is based on was compiled by the US Consumer Product Safety Commission (CPSC). Their National Electronic Injury Surveillance System (NEISS) compiles data on injuries connected to products or hobbies from casualty departments all over the country.

Source: heise online, news from 9 June 2009

Crypto AG, Headquarters

Crypto AG
P.O. Box 460
CH-6301 Zug
Switzerland
Tel. +41 41 749 77 22
Fax +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Crypto AG, Regional Offices

Abidjan

Crypto AG
01 B.P. 5852
Abidjan 01
Ivory Coast
Tel. +225 22 41 17 71
Fax +225 22 41 17 73

Abu Dhabi

Crypto AG – Abu Dhabi
P.O. Box 41076
Abu Dhabi
United Arab Emirates
Tel. +971 2 64 22 228
Fax +971 2 64 22 118

Buenos Aires

Crypto AG
Maipu 1256 PB «A»
1006 Buenos Aires
Argentina
Tel. +54 11 4312 1812
Fax +54 11 4312 1812

Kuala Lumpur

Crypto AG
Regional Office Pacific Asia
Level 9B Wisma E&C
2, Lorong Dungun Kiri
Damansara Heights
50490 Kuala Lumpur
Malaysia
Tel. +60 3 2080 2150
Fax +60 3 2080 2140

Muscat

Crypto AG
Regional Office
P.O. Box 2911
Seeb PC 111
Sultanate of Oman
Tel. +968 2449 4966
Fax +968 2449 8929