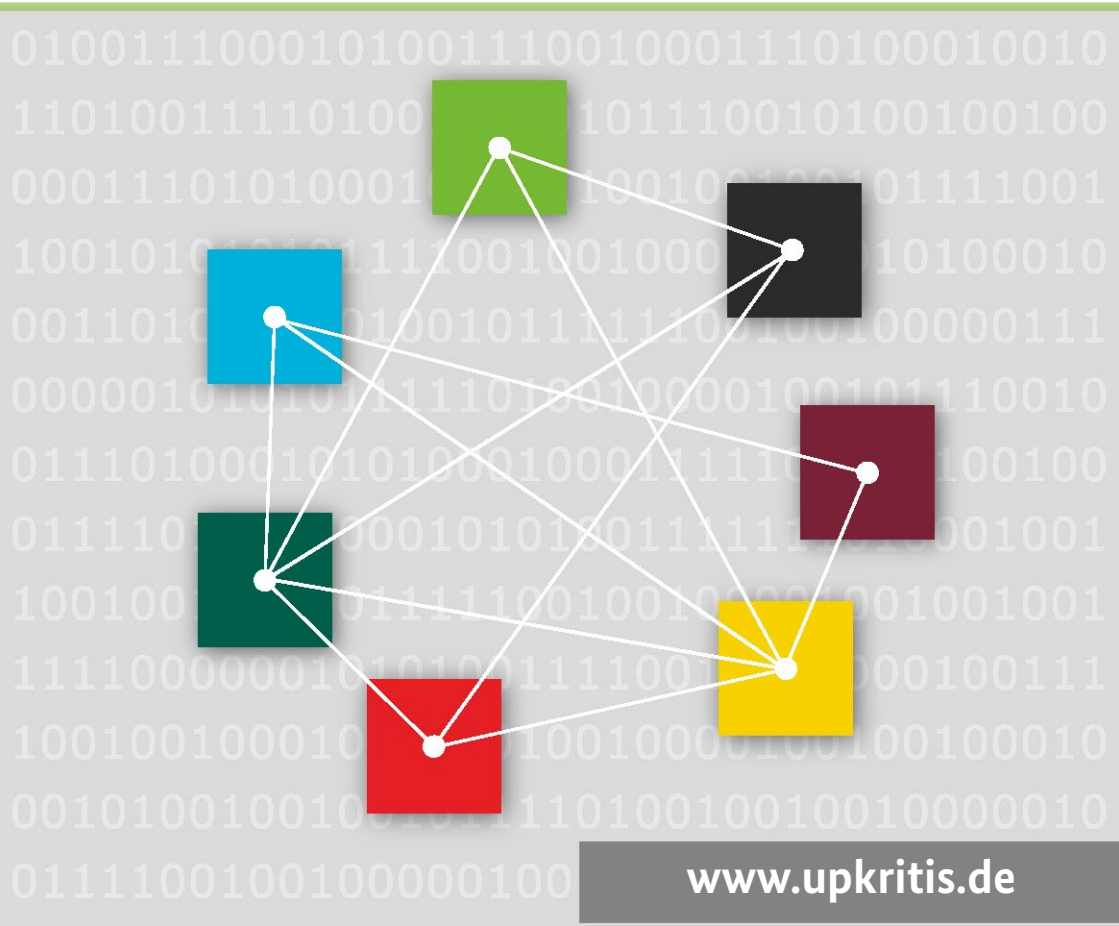
UP KRITIS

UP KRITIS

Public-Private Partnership for
Critical Infrastructure Protection

- Basis and Goals -



www.upkritis.de

Contents

1 Introduction and motivation

1 Introduction and motivation

Germany is one of the leading industrial and technology-oriented nations. Germany's importance as a business location and ensuring the country's competitiveness in a globalised world as preconditions for prosperity and progress significantly depend on the availability of high-performing and well-functioning infrastructure. A serious disruption or even an interruption of the services rendered via these infrastructures can have negative consequences for our society; in some cases, a failure can even result in severe impairments in social co-existence. If only small failures are tolerable or failures are not tolerable at all, this constitutes a service which is absolutely essential and thus vital for society; these services are rendered by so-called critical infrastructure (CI). The National Strategy for Critical Infrastructure Protection (CIP Strategy) pursued by the Federal Government defines critical infrastructure as follows:

Critical infrastructures are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.

In Germany, organisations and facilities in the fields of energy supply, information technology and telecommunication, transport and traffic, health, water, food, the financial- and insurance sector, state and administration as well as media and culture are counted among critical infrastructure (see Fig. 1).

Irrespective of whether organised as private or public institutions, the operators of critical infrastructure provide the services which are vital and absolutely necessary to supply the population at a high level of quality and stability. The exceptional resistance of these vital services to various threats is proof of the CI operators' sense of responsibility and constitutes a crucial basis for the functioning of society.

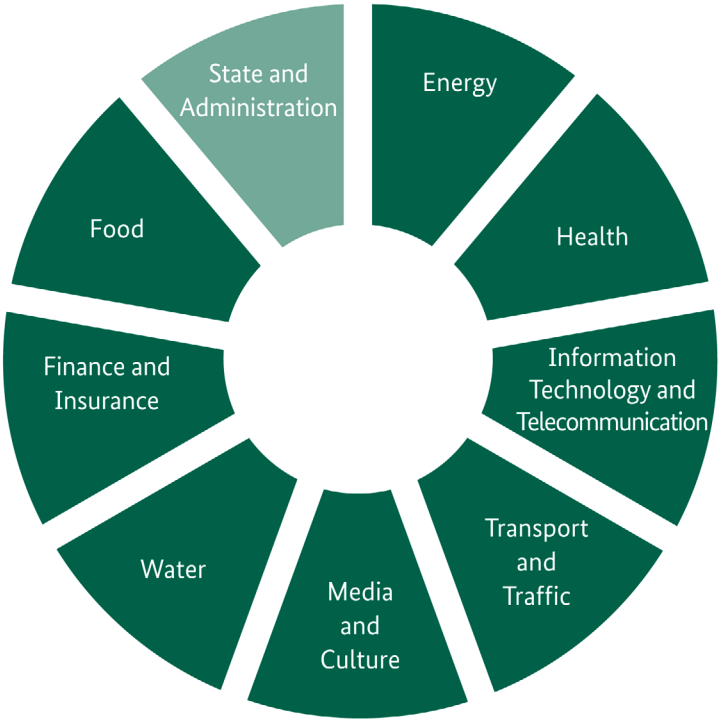


Fig. 1: The sectors of critical infrastructure in Germany

The protection of critical infrastructure in order to maintain the supply of the population is a continuous process which has to be regularly adapted in the light of a constantly changing environment. This has already been recognised by the public and the private sector for years and has been taken up as an important national task.

Strategically and on the operative level, the Federal Government follows a holistic approach to critical infrastructure protection, in the framework of which the German CIP Implementation Plan ("Umsetzungsplan KRITIS") was prepared in 2005 and 2006 in cooperation with operators of critical infrastructure. With the publication of the implementation plan in 2007, this public-private cooperation, which is now called "UP KRITIS", was institutionalised. The joint goal is to improve the protection of critical infrastructure across sectors.

Since 2007, in particular the IT threat situation has severely intensified. The Federal Government has responded to this by refining strategies and concepts on critical infrastructure protection and adjusting them to current conditions. In 2009, the Federal Ministry of the Interior (BMI) published the "National Strategy for Critical Infrastructure Protection", in which reference is also made to the particular risks and threats for information infrastructure. In 2011, the "Cyber Security Strategy for Germany" was published with "Critical Information Infrastructure Protection" as the core issue. Since then, many other activities such as the foundation of the National Cyber Security Council and the National Cyber Defence Centre have made a substantial contribution to CI protection.

The protection against IT-related risks, especially against cyber attacks, is one of the main components of an all-hazard approach; it is integrated into an operative risk and crisis management. Since vital services are rendered by means of critical (production) processes, protection must primarily focus on these processes.

In almost all critical processes, information technology has become a central and indispensable component. At the same time, it has been undergoing a remarkably dynamic development for the past few years, resulting in a constantly changing threat situation. For these reasons, the protection of information infrastructure is of particular importance to UP KRITIS.

UP KRITIS, however, also deals with topics which go beyond the IT area in order to maintain and strengthen the availability and robustness of critical infrastructure. In order to ensure a comprehensive protection of critical infrastructure, physical protection and IT security must be jointly developed and implemented.

The cross-sectoral cooperation between industry and the state within UP KRITIS has become a success. The organisations involved cooperate on the basis of mutual trust. They exchange ideas and experience(s) and are learning from each other with respect to the protection of critical infrastructure. Together, all parties are thus finding better solutions. Within the framework of the UP KRITIS, concepts are developed, contacts established, exercises held and a joint approach for (IT) crisis management developed and launched.

In order to be able to continue cooperation constructively in the future, the goals and structure of the UP KRITIS were adjusted in 2013 to address new tasks and challenges. The results of these adjustments are set down in this document. Updating the CIP Implementation Plan has, at the same time, established the basis for cooperatively developing sector-specific security requirements, further increasing the resilience of German critical infrastructure and actively supporting relevant proposed legislation. On this basis, the organisations involved in UP KRITIS will also cooperate in the years coming in order to ensure optimal provision of vital services even in times of omnipresent IT.

2 Achievements

2 Achievements

Since the CIP Implementation Plan was adopted in 2007, many companies and the Federal Government are working jointly within UP KRITIS in order to sustainably protect critical infrastructure and especially the underlying information infrastructure. With the idea of bringing the expertise and know-how of the public and private sector together, with respect to the protection of critical information infrastructure, **cross-company and cross-sector communication** in particular was promoted, which has established itself in all areas of UP KRITIS.

The "feeling of togetherness" resulting from this has significantly reinforced the trusting co-operation between the parties involved. Many contacts, also between sectors, were established. In addition, it was possible to develop mutual understanding for the partners' opinions, views and positions. Despite the different tasks at hand, this development has promoted co-operation and has helped considerably to achieve the goals set.

We have been able to build a **network of trust** between the members of UP KRITIS and develop it into a functional instrument for fast and reliable communication even in crisis situations. Thus, the Federal Republic of Germany is equipped with an instrument allowing to quickly take action in a crisis and to understand crisis management and mitigation as a joint task of the public and the private sector.

A particular task of the UP KRITIS was to **prepare and implement joint recommendations**. In the working groups established, the two basic concepts *"Early Detection and Mitigation of IT Crises"* as well as *"IT Emergency and Crisis Exercises in Critical Infrastructures"* were prepared.

The concepts were published within and implemented by UP KRITIS members:

» On the basis of the **exercise roadmap** from the "IT Emergency and Crisis Exercises in Critical Infrastructures" concept, exercises were carried out repeatedly. Both simple exercises to test communication and complex exercises such as participation in the LÜKEX series of exercises or dedicated dry runs (for preparation of the exercises) have resulted in optimisation of joint crisis communication structures and processes. By means of the exercises "Bundessonderlage IT 2009" (in English: "German Federal Special IT Situation 2009") and "Eltville 13", UP KRITIS members were able to intensively exercise IT crisis scenarios in particular and to identify improvement potential during the course of the exercise as well as to develop solutions in order to deal with disruptions to critical processes.

» By means of the intensive preparation and the integration of members of the UP KRITIS into the exercise "LÜKEX 2011" concerning "IT-Sicherheit in Deutschland" (in English: "IT Security in Germany"), it was possible not least to further strengthen the abilities of the parties to quickly and successfully manage and mitigate IT crises in practice. The experiences gained are constantly incorporated into the safeguards of the involved companies for IT security and BCM. The participation in the EU exercise "Cyber Europe 2012", too, was a great success and has shown that cross-border cooperation is possible and useful in a crisis. The basis for **operative cooperation** is the "Early Detection and Mitigation of IT Crises" concept paper which was implemented, amongst other things, by setting up several "Single Point of Contacts" (SPOCs) and establishing emergency contacts. Representatives of the public and the private sector have jointly defined processes to respond to crises, which have already proven their worth when managing different incidents. The Situation Centre of the BSI has sent situation information, reports and analyses to the companies and the companies have reported, sometimes via the SPOC, incidents and irregularities.

In line with efforts to **optimise crisis management**, two several-day training courses were performed at AKNZ (Academy for Crisis Management, Emergency Planning and Civil Protection of the Federal Office of Civil Protection and Disaster Assistance (BBK)) in order to strengthen and deepen the understanding of cooperation between the public and the private sector in specific crisis situations. Due to the increased involvement of the BBK in UP KRITIS, it has also been possible to enhance the links of **IT security and BCM** in critical infrastructure in the interest of comprehensive CI protection. A **study on potential crisis scenarios** has contributed to the organisations involved being able to develop a joint view of possible IT crises and corresponding courses of action.

For the **identification of critical processes and their IT dependencies**, a study was conducted by UP KRITIS. In this study, critical processes were identified for selected sectors and an overview of their complex dependencies was provided. It was completed in 2012 and, since then, has been a basis and a starting point for further examination and measures. This study constitutes the basis for an overview of the vital services in Germany (including dependencies on each other), supporting the planning of adequate measures against interruptions in supplies in the interest of the community.

In order to ensure **better national and international cooperation**, the partners were regularly informed about relevant European activities regarding the protection of critical infrastructure. The effects on Germany were discussed and some of our own positions were conveyed to the EU committees by BSI. This gave UP KRITIS members an opportunity to influence decisions made at the European level at an early stage, furthering the interests of UP KRITIS in particular and Germany in general.

Successful work in terms of content was based on several organisational frameworks:

» With the principles of cooperation within the framework of UP KRITIS and the signing of an agreement on the "Traffic Light Protocol" (TLP) by all members of the UP KRITIS, a **reliable basis for cooperation within UP KRITIS, maintaining required confidentiality, was established**.

» In order to support the plenum and the working groups, a **technical platform for the exchange of information and documents as well as for discussion** was additionally set up, allowing the members of the UP KRITIS to access documents, minutes, reports and other results from the joint work.

» The **office**, located at BSI, supported the comprehensive work performed in the work-ing groups and sub-working groups and has taken over administrative activities.

Today, the protection of critical infrastructure as well as the "cyber security" topic are still in the focus of politics and industry. Not least due to the many years of work of UP KRITIS, the awareness for the necessity to particularly protect critical infrastructure in Germany has grown in all areas of our society. Since the importance of IT continues to increase in the operation of critical infrastructure, UP KRITIS will continuously face new challenges. In order to master these challenges and to successfully continue with established structures, the goals and measures were revised through this update in 2013 addressing current needs.

3 Vision

3 Vision

Since its official start in 2007, the UP KRITIS partnership has made an essential contribution to the reliable provision of vital services for the population in Germany. Here, the focus lies on an effective interaction between IT security and business continuity management (BCM). The mission statement of UP KRITIS is cooperation of the operators of critical infrastructure with governmental bodies in order to strengthen the expertise of the Germany industry and the Federal Government, both having joint responsibility, especially for IT security in the processes of critical infrastructure.

Various measures should help to ensure that all operators of critical infrastructure maintain a high level of security in general and in IT-systems used in the companies in particular and to adequately develop them further. The long-term cooperation on the detection and mitigation of IT crises should be promoted together with the Federal Government both within and across sectors. In this regard, the cooperation within UP KRITIS follows this vision:

In joint responsibility of the public and the private sector, UP KRITIS makes an essential contribution to the protection of critical infrastructure with the aim of ensuring the provision of the population with essential, sometimes vitally important goods and services (vital services) as well as of avoiding significant disruption to public safety and security or other dramatic consequences.

Due to the importance of information technology for critical processes, the focus of activities lies on the IT used in critical processes.

In the past few years, it has been shown that a separate examination of physical security and IT security is not sufficient to achieve the joint goal of critical infrastructure protection. The cooperation of all relevant actors is indispensable for the success of measures and projects regarding the security of critical processes: this means the cooperation between areas specialised in IT and IT security and the experts in physical protection, business continuity management (BCM) and crisis management.

The examination of critical processes by UP KRITIS should put emphasis on the preventive aspect, i.e. preventing critical infrastructure from failing, improve the response to "nevertheless" failures and be designed with a view to sustainability in order to ensure the availability of critical infrastructure. For this purpose, the operators of critical infrastructure accept their responsibility in UP KRITIS and work independently on the implementation of the goals specified. The state supports the activities of the private sector within UP KRITIS and compares their results to governmental requirements for CI protection.

Aware that individual actors from the public or the private sector alone cannot operate with as much resilience as a well-networked group, UP KRITIS should be strengthened further and extended.

4 Goals

4 Goals

The UP KRITIS pursues the central goal of increasing the resilience of critical infrastructure, and, in this respect, especially the resilience of critical information infrastructure, and of stabilising this resilience on a high level adequate to the significance of specific critical infrastructures.

Resilient critical infrastructure is resistant to disruptions of any kind, adapts itself to new conditions and responds flexibly to changes in order to be able to guarantee the security of supply of the population as unrestricted as possible.

In order to achieve this overall goal, the parties involved defined sub-goals in different areas, which are described in the following sections.

In the appendix, various measures are described, which are to be implemented in the next few years. Here, work is being carried out both at a strategic-conceptual and at an operative-technical level. The strategic-conceptual measures are developed in the committees of UP KRITIS, the operative-technical measures are implemented by the organisations involved and/or via the communication structures established between UP KRITIS participants.

4.1 Joint analyses, recommendations and specifications

It is a strategic task of companies to ensure the robustness of IT systems underlying their processes. UP KRITIS exchanges views about standards, norms, and good practices and prepares and implements analyses, recommendations and specifications on the improvement of IT security of critical infrastructure. If necessary, any research activities in this respect are also accompanied and supported.

Due to the central significance and the omnipresence of IT components, their resilience should be enhanced particularly in the critical business processes and their tolerance for disruptions strengthened. If required, UP KRITIS intends to expand existing analyses by processes and their IT dependencies which were previously not included in the examination.

Furthermore, the parties involved in UP KRITIS aim to jointly analyse and evaluate the longterm threat and risk situation in order to identify existing risks to the security of supply and those to be expected at an early stage.

4.2 Joint action with regard to third parties

The goal of UP KRITIS is to induce third parties to contribute to the protection of critical infrastructure and thus to the security of supply through their actions. These third parties can be European organisations, manufacturers of products or service providers, for instance.

Based on this motivation, joint interests and positions should be identified and coordinated within UP KRITIS; they serve as a basis for a joint and effective appearance with regard to third parties.

4.3 Joint assessment of the situation

The members of UP KRITIS pursue the goal of exchanging views and ideas on incidents, jointly analysing and evaluating the current threat and risk situations and thus having a uniform assessment of the IT security situation of critical infrastructure available at any time.

4.4 Coordinated crisis response and management

All organisations involved in UP KRITIS have the goal of establishing crisis management structures and/or optimising and operating established structures.

In order to be optimally prepared for potential crises, UP KRITIS aims to interconnect these crisis management structures across sectors as well as to further extend joint crisis communication structures and processes in particular. If necessary, additional sector SPOCs will be established for this purpose.

By means of operative-technical cooperation in UP KRITIS, crises which occur should also be managed and mitigated jointly and quickly.

4.5 Emergency and crisis exercises

UP KRITIS sets itself the goal of jointly planning and performing various emergency and crisis exercises as well as participating in national and international exercises of third parties or evaluating their results. In these exercises, it is particularly tested if the communication structures agreed upon can be established and maintained and if the joint crisis management structures and processes are efficient and effective.

4.6 Extension of sectoral coverage

UP KRITIS aims to adequately integrate all CI sectors into a cooperative framework. This is the only way to provide for comprehensive security of supply in Germany.

4.7 Trusting cooperation

The organisations involved in UP KRITIS cooperate in a stringent and goal-orientated manner on the basis of mutual trust. This trusting cooperation should also be continued and expanded further in the future. UP KRITIS thus pursues the goal of the parties involved learning from each other with respect to the protection of critical infrastructure and, together, finding better solutions. For this purpose, an exchange of experience and a targeted transfer of know-how takes place in UP KRITIS.

5 Organisational structure

5 Organisational structure

Since the beginning of collaboration of members within UP KRITIS, the participating companies, associations and governmental authorities have gathered in working groups at regular intervals in order to reach the goals agreed upon. Simultaneously, for special topics, sub-working groups were set up by the working groups. This principle of operation has proven its worth. However, it does not allow for any further expansion of the group of participants, as otherwise the number of participants in the working groups would be too large.

UP KRITIS, however, pursues the goal of reaching as many organisations as possible from all CI sectors. By means of updating the CIP Implementation Plan, a new organisational structure was introduced; this structure allows the straightforward integration of new organisations into UP KRITIS whilst ensuring an effective working atmosphere in a modified committee structure.

5.1 Integration of an organisation into UP KRITIS

An organisation is first integrated into UP KRITIS as a participant. If an organisation wishes to collaborate more actively, it can, based on this, also become a partner in UP KRITIS.

5.1.1 Participant of UP KRITIS

All organisations with their headquarters in Germany operating critical infrastructure in Germany, national professional and sectoral associations from the CI sectors as well as the responsible government authorities can apply to become a participant of UP KRITIS. The participants appoint representatives for their organisation, who are granted access to the products of the UP KRITIS as well as to the information offered by the Alliance for Cyber Security including confidential information contained therein. In particular, all participants of UP KRITIS are provided with the situation information and warnings on IT security made available by the BSI.

In order to strengthen the joint assessment of the IT situation, all participants should inform the BSI about serious and severe IT security incidents.

5.1.2 UP KRITIS Partners / members of a working group

The participants of UP KRITIS can apply for the integration of their representatives into sectoral working groups (BAKs) and thematic working groups (TAKs) in order to actively participate in intra-sectoral or topic-specific activities within UP KRITIS. In order to secure and stabilise an exchange of views and experience with the federal state level, representatives of the federal states (Länder) can also be invited by the working groups.

If representatives of a participant (i.e. of a participating organisation) are integrated into a working group of UP KRITIS as a member, these organisations thus become partners of UP KRITIS.

All members of the working groups actively and independently work on the goals and projects of UP KRITIS. Each working group of UP KRITIS constitutes an information network of its own, in which information can be exchanged on a confidential basis.

5.2 Forms of cooperation within the UP KRITIS

Within UP KRITIS, a distinction is made between two forms of cooperation:

» the operative-technical cooperation between all participants of UP KRITIS and

» the strategic-conceptual collaboration in the established committees.

5.2.1 Structures for the operative-technical cooperation in the UP KRITIS

At the operative-technical level, the proven structures of UP KRITIS are continued: Sectors can establish SPOCs which take over the exchange of information with the companies of their respective sector. Companies from sectors without SPOCs can exchange information directly with the BSI. No changes are made to the previous communication structure and procedure as shown in Fig. 2.

All participants of the UP KRITIS contribute to the operative-technical cooperation.

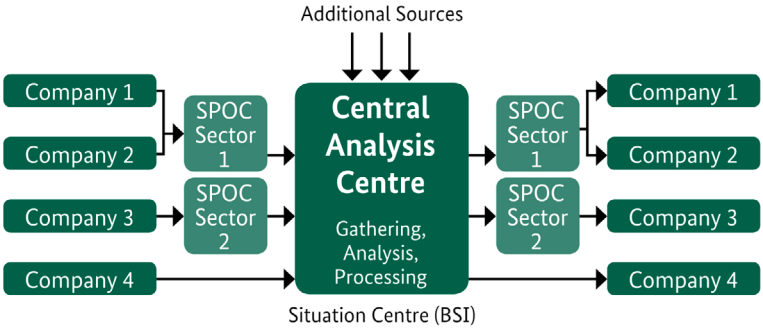


Fig. 2: Communication structure of the operative-technical cooperation in the UP KRITIS

5.2.2 Committees for strategic-conceptual collaboration within UP KRITIS

The core components of the new organisational structure are working groups for the exchange of expertise between specialists, the cross-sectoral plenum and a council established at a high level (see Fig. 3). A planning staff and the office support these committees.

The partners of UP KRITIS bear the responsibility for the strategic-conceptual collaboration.

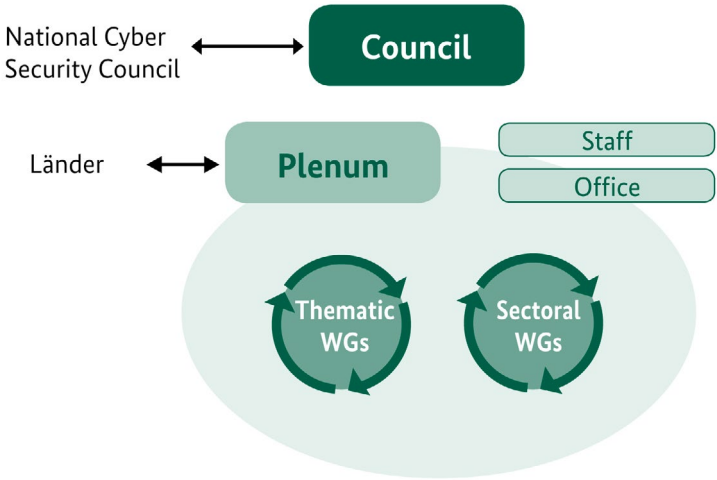


Fig. 3: New organisational structure of the UP KRITIS

Sectoral working groups

In each CI sector, there should be a suitable sectoral working group (German: "Branchenarbeitskreis", BAK) for IT/cyber security[1]. In addition, it can also deal with related topics such as BCM, crisis management and emergency/contingency planning. Within the sector as well as with the responsible government authorities, the BAK serves networking, the trusted exchange of information, and the development of joint positions and documents (e.g. frameworks for the sector) in particular. If there are already working groups on IT/cyber security in sectors outside the UP KRITIS, they are invited to collaborate with UP KRITIS and/or directly participate within UP KRITIS. If there is no BAK for IT/cyber security in a sector, such a BAK should be established by UP KRITIS participants from the sector.

Thematic working groups

Thematic working groups (German: "Themenarbeitskreis", TAK) serve as forums for the cross-sectoral, trusted exchange of information and the development of joint positions and documents. TAKs are set up on cross-sector topics (e.g. industrial control systems, exercises, SPOC exchange of experiences, BCM, crisis management).

Plenum

The plenum is the cooperation committee of UP KRITIS, which acts across sectors and covers a wide range of topics. It serves the exchange of information, sets UP KRITIS's strategic key activities, decides on the establishment or dissolution of TAKs as well as on the integration of BAKs, combines the results of the working groups, allows the exchange of views, ideas and experiences between them and plans the further course of joint action.

The plenum consists of representatives of the CI operators, their professional and sectoral associations as well as representatives from the public sector. Members of the plenum are

1 If necessary, sectoral working groups can also cover several sectors.

the speakers of the working groups in particular as well as the members of the planning staff and the office. For the connection to UP Bund (Implementation Plan for the Federal Administration) and to the federal states, they should each appoint a contact person to participate in the plenum as a permanent guest. Additional guests (e.g. from research) can attend the plenary meetings if specific events require this.

Planning Staff

In the periods between the plenary meetings, the planning staff coordinates the continuation of work and prepares strategic goals and measures. The members of the planning staff are composed of three representatives of the private sector selected by the plenum and one representative each of the BMI, BSI and BBK.

Office

The office is the service provider for organisational matters of UP KRITIS. It is operated by the BSI and supports the council, planning staff and plenum in particular.

Council

The council strengthens the partnership and cooperation within UP KRITIS and provides impetus for strategic goals and projects of UP KRITIS. In addition to this, the council members will speak for UP KRITIS in personnel, organisational and financial matters in their respective companies, within the sectors and among political and business representatives in order to ensure that it can perform its task of safeguarding the interests of critical infrastructure protection using adequate resources and with the necessary support of management from the public and the private sector. For this purpose, the council will also delegate a member to attend meetings of the National Cyber Security Council.

The council consists of high-ranking decision-makers of the CI operators and of the public sector.

6 Summary and outlook

6 Summary and outlook

Critical infrastructure (KRITIS) is vital for our society. It is of central importance for the functioning of the state, economy and society in Germany. As its failure or an impairment could entail a sustained shortage of supply, significant disruptions of public safety and security, or other dramatic consequences, maintaining the supply of the population with vital services is an important national task.

The operators of critical infrastructure are aware of this responsibility. With high priority, they are therefore pursuing the goal of delivering disruption-free vital services.

The Federal Government has recognised the need to jointly assume this responsibility and therefore adopted the "National Plan for Information Infrastructure Protection" (NPSI) in 2005, out of which the CIP Implementation Plan (UP KRITIS) emerged in 2005 and 2006. Since then, the public and the private sector have been jointly working in close partnership to continuously improve the (IT) protection of critical infrastructure. Within the framework of UP KRITIS, contacts are established, concepts compiled and implemented, exercises held and a joint approach for (IT) crisis management was developed and established. Among the parties involved, a network of trust has been formed, in which experience and (confidential) information can be exchanged and know-how transferred. Thus, all parties involved are learning from each other and are finding better solutions.

At the operational level, a close cooperation developed, in which the crisis management structures were established across sectors, which are also well integrated into the sectors via several SPOCs. Joint exercises pointed out the need for optimisation, but also demonstrated the effectiveness of the structures and processes already established, which have also proven successful in real situations.

The cross-sectoral cooperation is an important added-value of the UP KRITIS and should also be maintained and extended in the future. In order to reach a larger number of participants in the future, but to still remain able to carry out its work, a new organisational structure with a two-level participation model was created, allowing integration of all operators of critical infrastructure in Germany as participants into UP KRITIS. The participants are provided with situation information and warnings on IT-security by the BSI and can exchange their views and experience as needed on specific incidents within the framework of the operative cooperation. In addition to this, their representatives can collaborate in sectoral and thematic working groups dealing with intra-sectoral and/or cross-sectoral topics.

In the past six years, the cyber threat situation has severely intensified. Incidents such as Stuxnet, Duqu and others show that critical infrastructure has increasingly become the focus of attention for attackers. At the same time, the number of attacks performed by large organisations or states is also increasing. The private and the public sector must adequately respond to this professionalisation of attackers. With the Cyber Security Strategy for Germany, the Federal Government in 2011 has initiated several safeguards and UP KRITIS is also adjusting itself to these new prevailing conditions by means of this update.

The joint work within UP KRITIS has clearly shown that only taking IT/cyber security into consideration does not lead to the desired results: IT and physical security must be jointly developed and implemented. In addition to the central topic of IT/cyber security, UP KRITIS therefore also deals with other security issues such as physical CI protection and business continuity management (BCM).

Over the coming years, UP KRITIS has set itself new goals: In addition to the extension of the trusted cooperation and the extension of sectoral coverage by increasing the number of participants, the goals include the implementation of exercises, the joint assessment of the situation, the preparation of joint analyses, recommendations and specifications, coordinated crisis response and management as well as joint action with regard to third parties. For this purpose, the visibility of UP KRITIS at the national and European political level is also to be enhanced. As UP KRITIS now has a seat in the National Cyber Security Council, its political significance is strengthened.

UP KRITIS has become a successful public-private partnership and demonstrated how a cross-sectoral cooperation based on mutual trust between the state and the industry can work on a voluntary basis.

Due to the updated goals and tasks, its new organisational structure and the revised principles of cooperation, UP KRITIS is well set up to also increase the resilience of German critical infrastructure in the future and/or to stabilise it at a high level adequate to the significance of specific critical infrastructures and to meet the (cyber) challenges effectively in the years ahead.

7 Index of abbreviations

7 Index of abbreviations

AKNZ	Akademie für Krisenmanagement, Notfallplanung und Zivilschutz des BBK (in English: Academy for Crisis Management, Emergency Planning and Civil Protection of the Federal Office of Civil Protection and Disaster Assistance)
BAK	Branchenarbeitskreis (in English: sectoral working group)
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (in English: Federal Office of Civil Protection and Disaster Assistance)
BCM	Business Continuity Management (in German: Aufrechterhaltung der Geschäftsprozesse)
BMI	Bundesministerium des Innern (in English: Federal Ministry of the Interior)
BSI	Bundesamt für Sicherheit in der Informationstechnik (in English: Federal Office for Information Security)
CERT	Computer Emergency Response Team
CI	Critical Infrastructure(s)
CIP	Critical Infrastructure Protection
IT	Information Technology
IKT	Informations- und Kommunikationstechnik (in English: information and communications technology)

KRITIS	Kritische Infrastrukturen (in English: critical infrastructure)
LÜKEX	Länderübergreifende Krisenmanagement Exercise (in English: national crisis management exercise across the federal states)
NPSI	Nationaler Plan zum Schutz der Informations-infrastrukturen (in English: National Plan for Information Infrastructure Protection)
SPOC	Single Point of Contact
TAK	Themenarbeitskreis (in English: thematic working group)
TLP	Traffic Light Protocol
UP KRITIS	Designation (name) for the cooperation between the industry and the state described in this document

8 Literature

8 Literature

» Federal Ministry of the Interior (publisher):
National Strategy for Critical Infrastructure Protection.
Berlin, 2009

» Federal Ministry of the Interior (publisher):
Cyber Security Strategy for Germany.
Berlin, 2011

» Federal Ministry of the Interior (publisher):
CIP Implementation Plan of the National Plan for Information Infrastructure Protection.
Berlin, 2007

» Federal Ministry of the Interior (publisher):
Early Detection and Mitigation of IT Crises.
Berlin, 2008

» Federal Ministry of the Interior (publisher):
IT Emergency and Crisis Exercises in Critical Infrastructures.
Berlin, 2008

» Federal Ministry of the Interior (publisher):
Protecting Critical Infrastructures – Risk and Crisis Management. A guide for companies and government authorities.
Berlin, 2008

» Federal Ministry of the Interior (publisher):
Protection of Critical Infrastructures – Baseline Protection Concept.
Berlin, 2005

Publications are available at www.upkritis.de under “Publikationen”.

9 Glossary

9 Glossary

All-hazard approach	Taking all (known) hazards into consideration equally, for example when performing a risk analysis, and not only individual areas such as terrorism or sabotage.
Operators of critical infrastructure (CI operators)	Operators of critical infrastructure are (private-sector or public-sector) organisations from critical infrastructure sectors, that operate facilities required for the functioning of the vital services.
Cyber security	(Global) cyber security is the desired condition of the IT security situation, in which the risks of the global cyberspace have been reduced to an acceptable minimum. Cyber security in Germany is thus the desired condition of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is developed through the sum of suitable and adequate safeguards.
Information technology (IT)	Information technology (IT) encompasses all technical resources which serve for processing or communicating information. Information processing includes acquisition, recording, use, storage, communication, program-controlled processing, internal display, output and deletion of information.

IT dependency	A process depends on IT if the successful implementation of the process depends on the proper functioning of IT.
Information infrastructure	Information infrastructure is the entirety of IT components of an infrastructure.
Infrastructure	Infrastructure refers to all public and private facilities which are considered to be necessary for adequate public services and economic development. In most cases, infrastructure is divided into technical infrastructure (e.g. transport and communications facilities, energy and water supply or waste water disposal) and social infrastructure (e.g. schools, hospitals, shopping or cultural facilities).
Interdependency	Interdependency is the complete or partial mutual dependency of several goods or services.
IT security	IT security is the condition in which availability, integrity and confidentiality of information and information technology are ensured by appropriate safeguards.
IT crisis	There is an IT crisis within the context of the UP KRITIS if a failure or an impairment of organisations and facilities of major importance for society with sustained shortage of supplies, significant disruptions to public, safety and security or other dramatic consequences directly or indirectly occurs and/or is to be expected for IT-related reasons.

Critical infrastructure (CI)	Critical infrastructures are organisational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortage, significant disruptions of public, safety and security or other dramatic consequences. In Germany, the following sectors are assigned to critical infrastructure: » Transport and traffic (air transport, maritime transport, inland waterway transport, rail transport, road transport, logistics) » Energy (electricity, oil, gas) » Information technology and telecommunication (telecommunication, information technology) » Finance and insurance sector (banks/financial institutes, insurance companies, financial service providers, stock exchanges) » Government and public administration (government and public administration, parliament, judicial bodies, emergency and rescue services including civil protection) » Food (food industry, food trade) » Water (public water supply, public sewage disposal) » Health (medical services, pharmaceuticals and vaccines, laboratories) » Media and culture (broadcasting (television and radio), print and electronic media, cultural property, structures of symbolic meaning)

Vital services	Vital services are important, sometimes essential goods and services for the population. An impairment of these vital services would cause significant shortage of supply, disruptions to public, safety and security or other comparable dramatic consequences.
Critical process	Critical (business) processes are specialised tasks which are of great importance for the creation of value in the organisation. The classification into uncritical, less critical, critical and highly critical business processes can be made, for example, based on known damage scenarios as set out in the protection requirements definition according to IT-Grundschutz.
Resilience	Resilience is a system's ability to deal with changes. Resilience means resistance to disruptions of any kind, adaptability to new conditions, and a flexible response to changes with the aim of maintaining the system, for example a company or a process.
UP KRITIS	UP KRITIS is the initiative for cooperation between CI operators, associations, and the state in order to protect critical infrastructure in Germany with a focus on IT security.

CIP Implementation Plan *(in German: Umsetzungsplan KRITIS)*	Resulting from the National Plan for Information Infrastructure Protection (NPSI) published by the BMI in 2005, the CIP Implementation Plan was written in the following years, describing UP KRITIS, the initiative for cooperation between the public and the private sector in order to protect critical infrastructure. The implementation plan was published in 2007 and is replaced by the publication of this document.
Single Point of Contact (SPOC)	A Single Point of Contact is a well-established function in a sector, which, for the companies within this sector, is the central communication platform and reporting point from and to the companies.

10 Appendix: Concretisation of the goals by means of measures

10 Appendix: Concretisation of the goals by means of measures

In order to realise the goals described, the following measures should be implemented in the organisations involved, in the operative-technical cooperation of the participants as well as in the committees of UP KRITIS.

10.1 Joint analyses, recommendations and specifications

M1:		Based on the structure and tasks of the CI sectors, the identification and description of the vital services in the sectors as well as the critical processes required for this purpose should be continued by taking possible cross-sector interdependencies into consideration. The additional vital services and the critical processes required for this purpose as well as their IT dependencies should be identified under the responsibility of the sector working groups in accordance with the ICT study which has already been carried out in order to ensure comparability for follow-up measures.
	M1.1:	The results from the sectors are subsequently examined and assessed across sectors.
M2:		In order to be able to give suitable recommendations on the protection of critical processes, the medium- and long-term threat and risk situation must be analysed and assessed by means of an all-hazard approach.

M3:		UP KRITIS develops sector-specific security standards for the protection of those IT systems, components and processes which are crucial for the operability of critical infrastructure. Existing regulations, standards, frameworks and recommendations from individual sectors, particularly those with relevance to IT are included and are also used across sectors in view of their transferability.
	M3.1:	For this purpose, existing standards, good practices, and similar documents should first be compiled and compared with each other in the sectors.

Especially with regard to their relevance to IT, it should be evaluated at regular intervals if the identified critical processes and their dependencies have undergone changes and if the sets of rules to be applied have to be revised.

M4:		In order to be able to perform an efficient benchmarking of the sectors with respect to their resilience, the development of a suitable and generally accepted abstract model for both the intra-sector and cross-sector comparison is aimed at (e.g. a capability maturity model).
	M4.1:	Such a generally accepted model should be applied uniformly and consistently in all sectors and must therefore leave room for sector-specific requirements.
	M4.2:	Benchmarking results are exchanged and assessed across sectors.
	M4.3:	If the need for action results from this, it is addressed in the sectors.

The exchange of information on additional sector-specific procedures and results, e.g. in terms of risk management, is also an essential component in order to establish "good practice" procedures.

M5:		In addition to UP KRITIS' own analyses, external studies and analyses, e.g. on long-lasting and large-scale failures of IT core technologies, should be reviewed as to if and how the results can be used for UP KRITIS.

10.2 Joint action with regard to third parties

In addition to the work carried out by the members of UP KRITIS, the effective protection of critical infrastructure also requires adequate prevailing conditions regarding an increased security of supply and the provision of corresponding products and services by third parties outside UP KRITIS.

M6:		Based on this motivation, joint interests and positions should be identified and coordinated in UP KRITIS in order to ensure that they can serve as a basis for a joint and effective appearance with regard to third parties.
M7:		The matters of critical infrastructures and their special protection requirements must be sustainably represented to the bodies responsible. In as far as this is effective, UP KRITIS will therefore take a stand on current topics with relevance to CI (e.g. on the IT security perspective for technological developments or on corresponding initiatives of the EU, the Federal Government and the Federal States) at a national and international level and, if necessary, call for activities from third parties (e.g. in order to eliminate vulnerabilities in products).

UP KRITIS will, on its part, share its results and findings with third parties. In addition to partner organisations, these third parties can also be manufacturers or research facilities, for instance.

10.3 Joint assessment of the situation

The members of UP KRITIS should have a joint assessment of the IT security situation of critical infrastructure at their disposal at any time.

M8:		For this purpose, they exchange their views on current incidents and jointly analyse and assess the respective threat and risk situation.
M9:		For the exchange of views and ideas on current incidents and situations, communication structures (for example via SPOCs) must be extended further and/or established.
	M9.1:	Via these structures, observations, assessments, threats as well as restrictions on the availability of the vital services should be reported by CI operators to BSI.
	M9.2:	Based on these, BSI prepares situational overviews and early warnings and makes them available to CI operators immediately.
	M9.3:	In addition to this, situational overviews by third parties should be analysed and, if necessary, their information should be used.
	M9.4:	For the joint analysis and assessment of the threat and risk situation, telephone conferences on the situational overview, to which BSI invites the people responsible for IT security working for CI operators, should take place at regular intervals or if there is a reason to do so.

	M9.5:	In order to organise an exchange of information for all parties involved in a way that is effective and reasonable, the topics, contents and formats of the exchange must be defined. These definitions are made within the framework of the thematic working group (TAK) "Operativer Informationsaustausch" (in English: Operative Exchange of Information), in which all parties involved formulate their expectations and compare them with each other.
M10:		In addition to the exchange of views on incidents and situations, the views and ideas on the approaches taken for updating the situations should be exchanged in all organisations. For this purpose, it is necessary for CERTs and situation centres of the CI operators to work together more closely in respective organisations and across organisations in order to also support the national situation control by exchanging CERT information.
M11:		A concept for threat analyses and forecasts should be prepared, which can then be used by the organisations involved. The experiences gained when applying this concept should be reported back to the thematic working group "Operativer Informationsaustausch" in order to be able to make the required adjustments.

10.4 Coordinated crisis response and management

M12:		The prevailing conditions for nationally coordinated crisis response are developed further within the framework of a thematic working group (TAK).
M13:		In accordance with scenario-based analyses, crisis response should be optimised.
M14:		Appropriate crisis management structures should be established, optimised and operated across the sectors, which must be able to perform their work immediately in a crisis. This also includes,
	M14.1:	further building up and extending crisis communication,
	M14.2:	defining crisis communication processes, channels and partners,
	M14.3:	ensuring 24/7 availability,
	M14.4:	introducing suitable technical systems (e.g. a crisis communication system including emergency communication) and
	M14.5:	establishing SPOCs in additional sectors if necessary.
M15:		It must be verified if an operative-technical cooperation between CI organisations can be established in a crisis.
	M15.1:	Instructions and procedures for cooperation in a crisis should be developed.
	M15.2:	Opportunities for mutual support (e.g. by means of aids provided by experts or technologies made available) should be created.
M16:		After a crisis has been overcome, the crisis communication including the technical systems used should be evaluated and, if necessary, potential improvements jointly implemented.

10.5 Emergency and crisis exercises

In these exercises it is tested whether the communication relationships agreed upon can be established and maintained and whether the joint crisis management structures and pro-cesses are efficient and effective.

M17:		Within the framework of UP KRITIS, different types of emergency and crisis exercises are jointly planned and carried out.
	M17.1:	Participation in national and international exercises carried out by third parties is required.
	M17.2:	The exercises must be subsequently evaluated; the results should be put into practice.
M18:		Exercise concepts and results of exercises carried out by third parties should be assessed with respect to their relevance to UP KRITIS.
M19:		Framework scenarios should be developed and exercise scenarios updated.
M20:		In order to perform exercises, the existing exercise concept is updated.
	M20.1:	For the different types of exercises, specific exercise plans are prepared; here, regular exercise routines are agreed upon. In addition, exercises can be carried out event driven.

10.6 Extension of sectoral coverage

As not all CI sectors are sufficiently involved in the committee work of UP KRITIS yet, current deficits with respect to sector coverage must be identified and eliminated promptly.

M21:		For this purpose, organisations in sectors that are currently not or insufficiently repre-sented should be addressed in a targeted manner and encouraged to participate in the cooperation.
M22:		In order to support this approach, a marketing concept for the partnership is developed within UP KRITIS.
M23:		In addition to existing working groups of UP KRITIS, additional sector working groups should be established in order to deepen and extend the sector-specific CIP cooperation.
	M23.1:	Existing sector working groups outside UP KRITIS should be encouraged and supported in address-ing topics related to IT security; a cooperation be-tween the sector working groups and UP KRITIS or an association is desired.
	M23.2:	By means of monitoring, it is ensured that UP KRITIS has an overview of the active sector working groups and of the progress made with respect to sector coverage at all times.

10.7 Trusting cooperation

M24:		In UP KRITIS, the operators of critical infra-structure and the representatives of government agencies exchange their views on current polit-ical, technological and sector-specific issues and developments as well as their effects on critical infrastructure. Related topics which should be dealt with in thematic working groups (TAKs) are decided upon by the plenum of UP KRITIS.

M25:		The members of UP KRITIS mutually provide each other with confidential information, especially about IT/cyber security incidents, about failures of vital services and about threats which might result in such failures.

For the exchange of information, the representatives of the organisations participating and the members have committed themselves to maintain confidentiality according to the Traffic Light Protocol (TLP). Further obligations of the members within the framework of the cooperation are regulated in the "Principles for the Cooperation" which were revised parallel to this update.

For the mutual exchange of views and ideas and in order to facilitate cooperation, a suit-able technical information platform can be used and expanded as needed for the committees of UP KRITIS.

When addressing and dealing with topics serving the protection of critical infrastructure, the members of UP KRITIS also include existing internal and external work results.

The members are aware of the fact that the experts' know-how must be continuously updat-ed given the constantly changing threat situation and the increasing importance of properly functioning IT for the processes of critical infrastructure.

M26:		For this purpose, training courses should be held and mutual work shadowing enabled in order to be able to learn from each other.

Impressum

Herausgeber
Geschäftsstelle des UP KRITIS

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik
Geschäftsstelle UP KRITIS
Godesberger Allee 185-189
53175 Bonn
E-Mail: upkritis@bsi.bund.de
Internet: www.upkritis.de
Telefon: +49 (0) 22899 9582 5089
Telefax: +49 (0) 22899 109582 5088

Stand
Februar 2014

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
63086 Frankfurt am Main
Internet: www.zarbock.de

Texte und Redaktion
UP KRITIS
Themenarbeitskreis Fortschreibung

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI; sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.