Federal Office
of Civil Protection and
Disaster Assistance

“LÜKEX 11”
IT-Security in Germany
Evaluation Report

Civil Protection

Legal Information

"LÜKEX 11" – IT-Security in Germany
Evaluation Report
(Public version)

Project Group LÜKEX Bund

Provinzialstraße 93, 53127 Bonn

Telephone: +49-(0)22899-550-0
Telefax: +49-(0)22899-550-1620

Email: poststelle@bbk.bund.de
UR: www.bbk.bund.de

Graphic design:
Anna Müller, www.designflavour.de, Hennef

Printed by:
BBK

Picture credits:
Cover title picture: Federal Ministry of the Interior/Federal Office of Civil Protection and Disaster Assistance
Cover title picture: Collage: Logo „LÜKEX 11", BBK, BSI, Crisis Management Group BMI

Circulation February 2019

Cross-Länder Crisis Management Exercise

“LÜKEX 11” – IT-Security in Germany

Evaluation Report

(Public version)

Project Group LÜKEX Bund

“LÜKEX 11” – IT-Security in Germany
Evaluation Report
(Public version)

Contents

LÜKEX, Cross-Länder Crisis Management Exercise

Strategic staff exercise in the area of national crisis management for crisis and administrative staff respectively at Federation and Land level which has regularly taken place since 2004.

Note: LÜKEX is a cross-Länder and cross-departmental exercise at political-administrative level in the area of national crisis management. The target groups are political decision-makers from the Federation and the Länder and also providers of Critical Infrastructures.

A. General Remarks

"Cyberspace includes all information infrastructures accessible via the Internet beyond all territorial boundaries. In Germany all players of social and economic life use the possibilities provided by cyberspace. As part of an increasingly interconnected world, the state, critical infrastructures, businesses and citizens in Germany depend on the reliable functioning of information and communication technology and the Internet.

Malfunctioning IT products and components, the break-down of information infrastructures or serious cyber attacks may have a considerable negative impact on the performance of technology, businesses and the administration and hence on Germany's social lifelines. The availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace have become vital questions of the 21st century."

Federal Ministry of the Interior: "Cyber Security Strategy for Germany" (2011)

A.1. Legal basis

The legal basis for the planning, preparation, execution and evaluation of the 5th strategic crisis management exercise "LÜKEX 11", as part of the exercise series LÜKEX[1], is §14 of the Civil Protection and Disaster Management law (German Zivilschutz- und Katastrophenhilfegesetz (ZSKG).[2]

Cross-departmental and cross-Länder crisis management exercises

The law about the civil protection and disaster management of the Federation (Zivilschutz- und Katastrophenhilfegesetz ZSKG), at last amended by article 2, number 1 of the law of 29 July 2009 (BGBl., p. 2350), placed the training and exercise initiatives of the Federation on a modern footing. In particular, the successful cross-Länder crisis management exercise series LÜKEX is now legally sanctioned. To this end, the law stipulates:

§ 14 Training and further training

The training and further training measures of the Federal Office of Civil Protection and Disaster Assistance, according to § 4, section 1, sentence 2, no. 2, letter a, help the Länder to prepare their decision-makers, managers and other specialists for the management of disasters and accidents and include, above all, the planning, implementation and evaluation of cross-departmental and cross-Länder crisis management exercises. The training and further training measures of the Federation are based on the training of the Länder in the area of disaster management. They complement these.

A.2. Exercise topic

The topic of the exercise was IT-security in Germany. The topic reflects the increasing importance of information technology to public safety. Due to a multitude of actual IT-incidents and current threat analyses, the vulnerability of IT-infrastructures has increasingly become the centre of attention.

[1] Länder Übergreifende Krisenmanagement-Übung/EXercise (Cross-Länder Crisis Management Exercise)

[2] Law about the civil protection and disaster management of the Federation/Zivilschutz- und Katastrophenhilfegesetz – ZSKG of 2nd April 2009 (BGBl. I p. 693)

A.3. Exercise key points

3.1. Exercise target

The core target of the exercise was the training and testing of the concerted actions of the crisis and administrative staffs of the Federation and the Länder at the political-administrative (strategic) decision level by including private operators of Critical Infrastructures. Another aim was to assess, for the first time, the efficiency of strategies on the protection of national information infrastructures[3] in a joint exercise of the Federation, the Länder and enterprises of Critical Infrastructures.

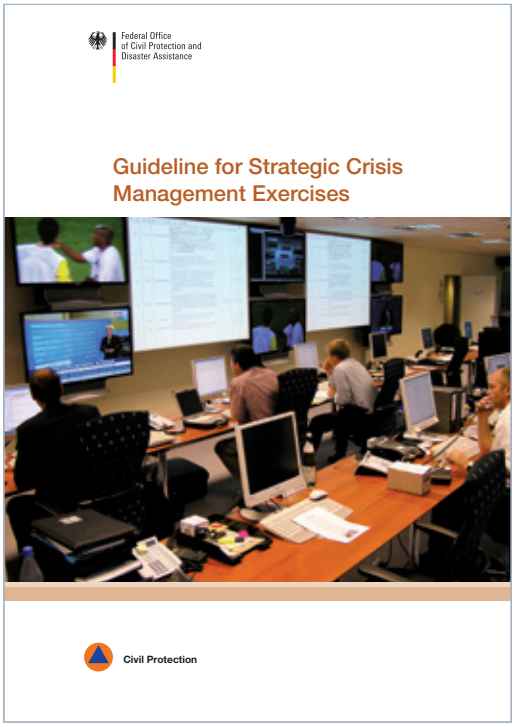
The exercise "LÜKEX 11", which was based on a national crisis in the wake of Cyber-attacks, pursued the following goals:

- To make the public aware of the overall topic
- To contribute to the networking of all relevant players
- ITo further develop IT crisis management and general strategic crisis management as a whole in a coherent way and
- If possible, to raise the status quo of national and social preparations to a higher level, with regard to new threats

3.2. Exercise concept

The exercise "LÜKEX 11" was based on the *Leitfaden für strategische Krisenmanagement-Übungen*[4] *(Guideline for Strategic Crisis Management Exercises).* It states that the entire exercise cycle, which lasts, as a rule, two years, comprises the following phases:

- Planning
- Preparation
- Execution
- Evaluation

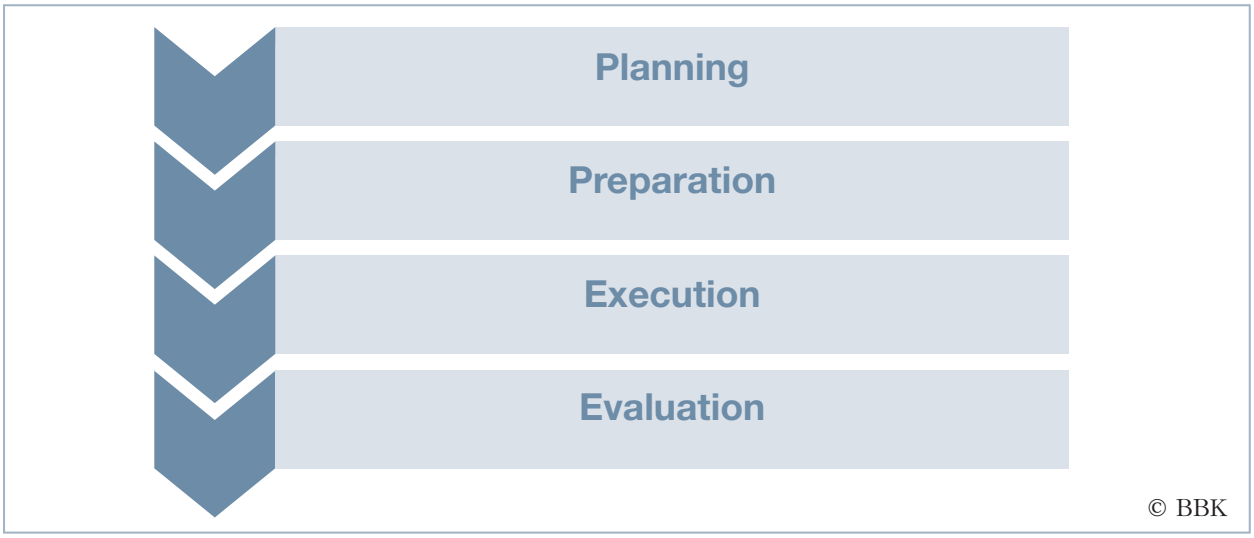


© BBK

Picture 1: The "Guideline for Strategic Crisis Management Exercises" presents principles of Strategic Exercises.

[3] National plan concerning the protection of information infrastructures (NPSI); implementation plans of Federation and KRITIS (UP Bund and UP KRITIS respectively), Federal Ministry of the Interior, 2007, as well as Cyber-security strategy for Germany; Federal Ministry of the Interior, February 2011

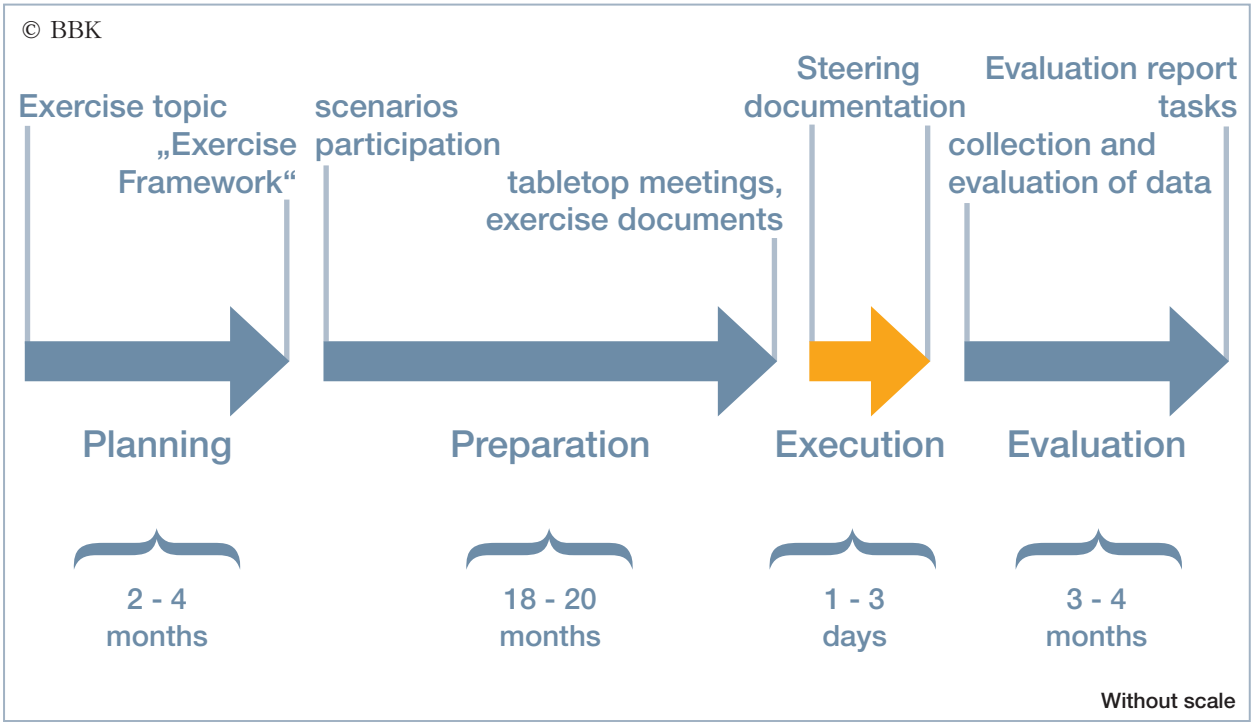
[4] Federal Office of Civil Protection and Disaster Assistance (2011) Guideline for strategic Crisis Management Exercises, Bonn



Picture 2 shows the cycle of strategic exercises with its 4 phases

The "core" of the exercise is the exercise preparation phase. Here, by means of interdisciplinary expert talks, the exercise scenario is gradually and discursively developed and structured as realistically as possible by relying on the expertise of the exercise participants. Thus, in the course of 18 months, the exercise scenario of "LÜKEX 11" was thoroughly prepared by profiting from numerous seminars, "thematic workshops" on selected specific topics and special workshops relating to the scenario. The preparatory phase gave the exercise participants the opportunity to assess their crisis management structures and procedures and to remove weak points before the execution of the exercise.

The highlight of the exercise was the exercise execution phase on 30th November and 1st December 2011. Mainly high-ranking representatives of Federal and Land crisis and administration staffs as well as numerous authorities, relief organisations and enterprises took part in coping with the fictitious national crisis.



Picture 3: The exercise cycle of „LÜKEX 11" comprised from the beginning of the planning phase to the end of the evaluation phase nearly 24 months

3.3. Exercise scenario

The scenario of the "LÜKEX 11" exercise was based on the assumption that target-oriented attacks on IT took advantage of weak points in the IT-systems and the network of the government.
For the design of the scenario, a group of perpetrators, who operated together in the shadow ("hacktivists"), and shared multifunctional malware ("SPY-tool") were introduced to set the necessary overall context and to create a plausible picture of the manifold IT-disruptions and different repercussions.

The following selected sectors of Critical Infrastructures (KRITIS)[5] were particularly affected:

- State and administration
- Information technology and telecommunication
- Transport and traffic
- Finance and insurance.

Critical Infrastructures (KRITIS)

Critical infrastructures are organisations and institutions of special importance for the country and its people where failure or functional impairment would lead to severe supply bottlenecks, significant disturbance of public order or other dramatic consequences.

Note: cf. Federal Ministry of the Interior, "National Strategy on the Protection of Critical Infrastructures" (KRITIS-strategy) of 17 June 2009.

Source: BBK, publication series "Praxis im Bevölkerungsschutz", volume 8, "Ausgewählte zentrale Begriffe des Bevölkerungsschutzes", Bonn, 10/2011

Exercise participation

The following parties participated in the exercise:

- 10 Federal departments (of which five with their own share of the scenario),
- 20 Federal authorities as well as
- the National Cyber Defence Centre (in German abbreviated as Cyber-AZ) which was established in spring 2011,
- Five Länder which were deeply involved (so-called intensively exercising Länder): Hamburg (HH), Lower-Saxony (NI), Hesse (HE), Saxony (SN) and Thuringia (TH) and
- seven Länder which participated to a less degree (so-called exercising Länder): Brandenburg (BB), Berlin (BE), Baden-Württemberg (BW), Bavaria (BY), Mecklenburg-West Pomerania (MV), Rhineland-Palatinate (RP), Saxony-Anhalt (ST),
- 45 enterprises of Critical Infrastructures and associations,
- the European Central Bank (in German abbreviated as EZB) and
- EUROCONTROL.

[5] Federal Ministry of the Interior (2009) National Strategy for the Protection of Critical Infrastructures (KRITIS-Strategy), enclosure 2 (www.bmi.bund.de)

In the exercise execution phase, altogether about 3,000 people were involved, either as exercising participants in the crisis staffs or as steering groups in the exercise steering organisation.

As in previous exercises, the *Schutzkommission beim Bundesministerium des Inneren* (SK – Protection Commission of the Federal Ministry of the Interior)[6] accompanied the exercise cycle "LÜKEX 11" by contributing its special scientific knowledge.

3.5. Real media work and visitors' programme

Even before the exercise had actually started, the real media interest in the "LÜKEX 11" exercise was considerable. With regard to this interest, the Federation and the Länder had coordinated guidelines on real media work (including a FAQ catalogue) for the exercise execution phase.

On the exercise days, the Federal Office of Civil Protection and Disaster Assistance (BBK) organised, together with the Federal Agency for Security in Information Technology (BSI) and the Federal Office for the Protection of the Constitution (BfV), a comprehensive visitors' programme, which, among other things, included an "Additional Forum" for visitors of the exercise from home and abroad.

Picture 4: The accompanying programme for high ranking visitors from home and abroad, which was for the first time offered at "LÜKEX 11", was highly appreciated.

[6] www.schutzkommission.de

A.4. Exercise evaluation

With regard to the contents, the exercise evaluation was aligned to the previously defined exercise objectives. In the course of the exercise preparation, aims and methods were coordinated between the exercise participants and summarised in a conceptual framework.

The concept was based on a qualitative comprehensive approach ("combination of methods"). During the follow-up to the exercise "LÜK-EX 11", a multitude of individual findings, observations and conclusions from questionnaires, reports, events and talks were put together.

B. Conclusions with regard to contents

B.1. Preliminary remark

The task of the crisis and administration staffs at Federal and Land level was the coordination of the actions of the Government and the cross-national and inter-divisional administration.

The IT reporting structures under construction and the cooperation between the structures of general crisis management and IT crisis management structures under construction, which, to a large extent, had not yet been tested, were a particular challenge of the exercise "LÜKEX 11". This was particularly true for the close cooperation with the IT service providers and the inclusion of IT-dependent Critical Infrastructure providers in the decision finding process. Due to the increasing penetration of all areas of life with information and communication technology, availability, confidentiality and integrity of information and communication technology are vitally important for Critical Infrastructure providers. Another aim of the "LÜKEX" exercise was to determine the impact of massive IT-failures in the four previously exemplified sectors of Critical Infrastructures and to try out appropriate comprehensive defence strategies.

B.2. Comprehensive conclusions

2.1. National crisis management

Altogether, the exercise was, once again, proof of the generally good and trusting cooperation between the Federation, the Länder and Critical Infrastructure enterprises. Nevertheless, the continuous networking between public administration and private Critical Infrastructure providers at all levels was regarded as urgent and therefore further actions were called for.

The inclusion of „expert advisors" of Critical Infrastructure enterprises in the crisis staffs at different levels has made sense.

However, the follow-up phase revealed that the exercise aim of cross-national cooperation was not everywhere fully reached.

The exercise showed the vital importance of individual essential information and communication technology structures, processes and professional procedures. In terms of strategic preventative failure measures and basic social care for the society as a whole, it was necessary to assess whether current preventative failure measures are sufficient to allow quick and efficient reactions. If necessary, an action plan for a potentially long-term failure of regulatory structures has to be developed.

As the coordination processes of the Länder among each other are concerned, there is still some room for improvement. The mutual exchange about measures taken could have been more intensive.

Furthermore, the following conclusions were drawn:

- Unless this task has already been done, the Federation, the Länder und Critical Infrastructure enterprises should identify information and communication technology structures, processes and professional procedures which are vital for basic social care and public order.

- In future, the Länder should have a more lively exchange about their views on taken measures to be able to include findings in their own actions, if necessary..

- Unless this has already been implemented, all crisis staffs should include technical IT-authorities, IT-service providers or IT-expert providers – temporarily also Critical Infrastructure enterprises – in the work of the crisis staff. If possible, their representatives should include the management level (e. g. CIO to give advice on politics).

2.2. Crisis management at Federal level

Without exception, the crisis management structures which exist in the Federal sector – both in the area of general crisis management and IT crisis management – have stood the test. According to the underlying conception, the crisis staff of the Federal Ministry of the Interior is called on, when serious IT-security incidents or a national IT-crisis, in particular in the sector of Critical Infrastructures, exist.

Picture 5: The crisis control by the crisis staff at Federal level (in the picture) was anticipatory and professional.

The anticipatory and professional crisis management by the crisis staff at Federal level was aimed at. Almost throughout the exercise, the Security State Secretary of the Federal Ministry of the Interior was in charge of the crisis staff; his representative was the head of the department "crisis management and civil protection". The portfolio authorities of the Federal Ministry of the Interior (BSI, BVA, BBK, THW, BKA, BfV and BPOL) were represented by the respective office heads.

As the Federal Ministry of the Interior is responsible for the use and security of information technology within the Federal administration, the representative of Information Technology of the Federal Government (BfIT) and the IT-director were included in the structure of the crisis staff work. The cooperation of the Federal authorities can be referred to as good and trusting.

To assess the situation, IT-aspects were appropriately considered. When they referred to IT-failures and break-downs, the discussions between the staff members often focussed on technical aspects. More importance should be attached to thoughts about the possible impact on the population and the administration.

The IT-crisis management should be institutionalised across departments and integrated into general crisis management.

As the information and communication structures and the professional procedures are concerned, which are vital for basic social care and the guarantee of public order, the IT-infrastructure should be redundant and self-sufficient (meaning independent of public nets).

2.3. Crisis management at Länder level

The vast majority of the intensively exercising Länder (Hamburg, Lower-Saxony, Hesse, Saxony, and Thuringia) evaluated the exercise cycle „LÜKEX 11" as successful and, especially against the background of the current IT-security threat, as necessary and goal oriented.

For most of the Länder it can be said that it was the first time that a cooperation of responsible managers in general crisis management with IT-security experts from the respective Land and private Critical Infrastructure providers took place in the context of an exercise. This kind of networking was regarded as extremely useful and helpful and regarded as a considerable additional value of the exercise.

During the preparation of the exercise, interface problems between general crisis management and IT-crisis management became obvious, the latter belonging partly to the sector outside the interior departments or to private operators. Therefore, the preparation phase was used to sort out these problems and to establish appropriate structures to be tested during the exercise. The exercise showed that structures and processes concerning the IT-crisis reaction in the Länder (e. g. information exchange and "VerwaltungsCERT-Verbund[7]": "AdministrationCERT-Association") by simultaneously strengthening the role of the national IT-crisis reaction centre of the Federal Agency for Security in Information Technology (BSI) must undergo an ongoing improvement process. To achieve this, interdisciplinary professional expertise concerning Cyber security should be appropriately included.

During the exercise, a competent and politically sensitive management of the crisis staffs could be noticed throughout the Länder. As a rule, the responsible Secretary of State/State Council was present for an adequate amount of time.

[7] CERT= Computer Emergency Response Team, VerwaltungsCERT-Verbund" = Federation-Länder cooperation at operative CERT-level, currently discussed in the IT-planning council.

Pictures 6 and 7: In the course of the exercise it became obvious that all Länder managed the crisis staff in a competent and politically sensitive way – the pictures show the crisis staff Thuringia during the exercise execution.

Again, permanent crisis management structures (e.g. permanent staff positions in all departments) have proved their value. As this aspect is concerned, cabinet decisions on the development and adaptation of crisis management structures are beneficial. In some Länder, binding regulations on the establishment of crisis staffs, based on the IMK-decision[8] about the structure of administrative staffs, were implemented in an exemplary way. In some cases, binding regulations concerning the integration of IT-crisis management into general crisis management were put into practice. Thanks to its experience with operations in the areas of police and disaster management and its logistic preconditions, (situation centres, well-rehearsed channels, technology etc.); the inner department is principally able to see to the coordination by profiting from systematic professional advice and the involvement of experts. Under such conditions, this is even possible in crisis situations which include other thematic key aspects. To a large extent, in all Länder, IT-crisis management could be successfully integrated into general crisis management structures during the execution of the exercise. In several authorities, emergency planning measures were initiated and modified respectively.

[8] Standardised national *Hinweise zur Bildung von Stäben der administrativ-organisatorischen Komponente (administration staffs-VwS),* Beschluss der Ständigen Konferenz der Innenminister und -senatoren (IMK) of 21/11/2003

Furthermore, regional providers of Critical Infrastructure – e. g. banks, savings banks, carriers – were successfully involved in the decision-making process. The degree of their involvement varied. During the exercise preparation, networks were developed which, together with the existing networks, allowed the close coordination and cooperation between the respective crisis staffs of the Land and the crisis staffs in the sector of Critical Infrastructure. Against the background of potential real situations, this fact should have a positive effect. The involvement of the exercising Länder Brandenburg, Berlin, Baden-Württemberg, Bavaria, Mecklenburg-West Pomerania, Rhineland-Palatinate and Saxony-Anhalt in the exercise varied. Partly, the crisis staffs were convened at Land level and the impact of the IT-incidents on their own structures were reflected in the intensively exercising Länder.

The joint management structure of the Länder Berlin and Brandenburg was a novelty. Thus, they could achieve synergy effects.

Without exception, it was possible to sensibilise the responsible managers for the dependency of the administration on IT, an aspect which is particularly important when business processes are critical.

In the course of the exercise, the following conclusions were drawn:

- the factors institutionalisation of IT crisis management with developing structures,
- the integration of IT crisis management into general crisis management and
- the "transfer efficiency" of the players (e. g. the ability to present professional problem situations in a comprehensible way)

are an essential basis of successful crisis management during an IT related crisis.

Further essential conclusions:

- Staff structures for strategic crisis management are to be defined on a binding basis and be approved by cabinet resolution. As a matter of principle, the resources and experiences of the respective inner department are to be used, even when another department is in charge of the technical leadership.
- The structure of the normally available IT emergency management of the respective IT service providers is to be adapted and more closely linked to the political-administrative decision-level.
- The cross-departmental cooperation of crisis management in the event of IT crises, involving Critical Infrastructure sectors, is to be further optimised. It should be broadened in the context of exercises and implemented in practice.
- Proven structures and processes concerning the IT crisis reaction (e.g. information exchange and "AdministrationCERT-association") are to be successively put into practice across Germany. To this end, the capacities of the national IT crisis reaction centre are to be used and the role of the Federal Office for Information Security be strengthened.

2.4. Civil-military cooperation (ZMZ)

The exercise was suitable for exercising the organisation and procedures of Civil-Military Cooperation (in German abbreviated as: ZMZ) at strategic level. The four military subdistrict commands (German abbreviation: WBK) and the Armed Forces Support Command (German abbreviation: SKUKdo) took part in the exercise. The counselling of the crisis and administration staffs by the Land commands was based on established procedures and provided by contact persons. To this end, the possibilities and limits of administrative cooperation, provided by the Armed Forces, were taken into account. The tried and tested cooperation of the Federation and the Länder in the area of Civil-Military Cooperation (ZMZ) should be continued and be regularly tested and practised as part of strategic crisis management exercises, based on new threat scenarios – in spite of the fact that the Armed Forces are undergoing a structural transformation.

2.5. Information management, situation assessment and decision-making

The exercise showed that informational cooperation structures within IT security must be further optimised. To achieve this, conclusions, gained during the exercise, should be taken into consideration. Above all, the regular information exchange between the Federation, the Länder and Critical Infrastructure sectors should be institutionalised and authorised by the responsible committees. Generally, both the cooperation between the Federal Agency for Security in Information Technology (IT situation centre) and the Critical Infrastructure Implementation Plan (UP KRITIS) as well as the reporting channel via the structure of Single Points of Contact (SPOC) have stood the test. The active IT crisis management and the networking with regional Critical Infrastructure providers via Single-Point-of-Contacts (SPOC's) is necessary.

How a formalised information exchange between the SPOC's of Critical Infrastructure sectors and the Federal level (Federal Office for Civil Protection and Disaster Assistance (BBK)/German Joint Information and Situation Centre (GMLZ) and the Federal Agency for Security in Information Technology (BSI)/IT-situation centre) could take place has to be assessed.

As the situation assessment and decision making process by the crisis staffs is concerned, the prognostic component seemed to be lacking in many cases.

The "KRITIS Implementation Plan"

An important component of the implementation of the targets of the National Plan for the Protection of Information Structures is the protection of information technology concerning so-called Critical Infrastructures.

Important infrastructures, for example in the sectors of finance, energy and supply, increasingly depend on IT and are becoming increasingly networked. In Germany, about four fifths of so-called Critical Infrastructures are under the responsibility of the private industrial sector.

Therefore, the Federal Ministry of the Interior developed the "KRITIS Implementation Plan" – together with about 30 big German infrastructure enterprises and their interests groups which all rely on IT systems to a large extent. The participating organisations voluntarily undertake to maintain a minimum level of IT security. Therefore, the KRITIS Implementation Plan is a model of how national offices can efficiently cooperate with the economy in the future…

Source: Federal Ministry of the Interior, www.bmi.bund.de

Nevertheless, to a large extent it was possible to get "ahead of the situation" towards the end of the exercise.

Again, the telephone conferences between the Federation and the Länder turned out to be the right means to trigger quick coordination and decisions between the Federation and the Länder.

Additionally, the following aspects need to be explored:

- The possibility whether the crisis staffs will be able to use their own prognosis cells and appropriate simulation software
- The Federation, the Länder, municipalities and Critical Infrastructure providers should carry out inter-divisional exercises concerning IKT-emergency planning.

2.6. Special conclusions concerning IT crisis management

"LÜKEX 11" was the first exercise in which the implementation of the IT council's decision on "IT-crisis management during IT-crises with an impact on Federal administration"[9] was exercised. The decision is an essential element for the cooperation of the Federal departments in cross-social crisis management.

Furthermore, the IT cooperation structures (reporting channels, reporting procedures), which, during the exercise preparation phase, had been agreed upon with the Länder, could be tested for the first time. The cooperation with the Federal Agency for Security in Information Technology (BSI) received a positive feedback by the Länder. In terms of sustainability, the Länder should further develop and expand their competences in IT crisis management and exchange their ideas about essential IT-incidents with the BSI in the follow-up phase to the exercise. This should be done via defined contact points. The establishment and intensification of the "VerwaltungsCERT-Verbund" („AdministrationCERT-Association") should be followed up as part of the committee work of the Federation and the Länder.

The exercise yielded a multitude of insights into the further optimisation of the processes within the national IT-Crisis Reaction Centre (in German abbreviated as IT-KRZ) of the Federal Agency for Security in Information Technology (BSI) and into the cooperation within inter-divisional IT-crisis management, including the Federal Office for Civil Protection and Disaster Assistance (German Joint Information and Situation Centre/GMLZ). The prepared structures and processes concerning the IT-crisis reaction of the Federal administration within the Federal Agency for Security in Information Technology have principally stood the test.

In its role as a centre of competence and coordination authority in the area of IT-security, the Federal Agency for Security in Information Technology could provide important incentives and contributions to the solution of problems. The BSI has regularly provided public agencies with an updated IT situation report as well as warning and alarm messages containing new findings concerning the threats on which the situation is based.

Unless this has already been done, clearly defined information and reporting procedures and IT security structures (e.g. Landes-CERTs) should be established for the Länder IT sector, which guarantees the cross-national information exchange as well as the information exchange with the Federation. This could be done, e.g., by a "VerwaltungsCERT-Verbund" („AdministrationCERT-Association"). To achieve this, the responsible committees of the Federation and the Länder have to be involved.

[9] Council decision on *IT-Krisenmanagement bei IT-Krisen mit Auswirkungen auf die Bundesverwaltung* of 31/03/2011

Picture 8: The IT Crisis Reaction Centre during "LÜKEX 11"

2.7. National Cyber Defence Centre

For the first time, the National Cyber Defence Centre (in German: Cyber-AZ), re-established as part of the National Cyber Security Strategy in April 2011, was included in an exercise. Within the scope of its tasks as an information hub, it contributed to the exchange of situation reports between the participating authorities and their enrichment with additional information thanks to joint evaluations. The following activities were recommended:

- The cooperation of the authorities at the National Cyber Defence Centre as information hub should be developed.
- The possibility of a joint strategic situation assessment at the National Cyber Defence Centre should be examined.
- In spite of the non-operative direction of the National Cyber Defence Centre, the testing of the communication competence in connection with the IT crisis reaction centre is recommended.

2.8. International participation

In spite of numerous international interdependencies of the participating Critical Infrastructure enterprises (e. g. in the sectors of banks, aviation and ICT), the exercise was largely restricted to the national level. This was done due to principle considerations and according to the character of the LÜKEX-exercise series.

The international, above all the European dimension, should also be considered during future strategic crisis management exercises.

B.3. Conclusions in the sector of Critical Infrastructures (KRITIS)

3.1. Critical Infrastructure sector “Information and communication technology” (IKT)

As the Critical Infrastructure sector of “Information and Communication Technology” (German: IKT) is concerned, the exercise has illustrated the pronounced heterogenity of the organisation structures of IT-service providers. IT-service providers with different legal status (authorities, public-law institutions and private enterprises) and telecommunication enterprises took part in the exercise.

As a rule, Information and Communication Technology aspects of the exercise scenario were perceived and treated with focus on the Länder.

It became clear that the close involvement of IT-service providers and telecommunication enterprises supports quick and professionally competent decisions.

3.2. Critical Infrastructure sector “Transport and traffic”

As the Critical Infrastructure sector of “Transport and traffic” is concerned, the exercise showed that, if IT-technology is compromised, this can have an impact and far-reaching consequences on air traffic processes, for example. The impact was clearly noticeable at all participating airports.

The breakdown of data-processed control systems in road traffic (tunnel monitoring, traffic light control systems), which was simulated during the exercise, revealed a national and inter-divisional impact which, in reality, would require a short term cross-national information exchange and appropriate emergency measures (e.g. care for affected people).

Pictures 9 and 10: IT-disruptions particularly affected the processes in air traffic. The picture shows the Frankfurt Airport.

.

3.3. Critical Infrastructure sector "Finance and insurance"

Thanks to the large participation of the banking sector (German Central Bank, European Central Bank, German Bank, Commerzbank, German Post Pension Service, Savings Bank Financing Group, insurance sector) and the multitude of diverse scenarios, which were exercised, procedures of cooperation could be tested in a reliable way. Thanks to an even better network, the principally successful information processes between the Federal Agency for Security in Information Technology and the SPOC's could be improved even further. It became clear that the situation reports of the German Joint Information and Situation Centre (GMLZ), which so far have only been made available to authorities, contain valuable information for the finance and insurance sector, as well.

Another conclusion: in crisis situations it can be useful if Critical Infrastructure enterprises have a kind of "emergency call directory" which allows the authorisation of the communication parties and thus the exchange of information of even confidential nature. Furthermore, the following is recommended:

Picture 11: The KRITIS sector "Finance and insurance" was involved in "LÜKEX 11" to a large extent – in the picture: the staff of the savings bank "Mittelthüringen" during the implementation of the exercise.

- Against the background of the rapid pace of information technology, the functionality of one's own organisation should be regularly checked. This could be done through exercises, e.g.
- In the event of disturbances and the breakdown of similar systems (e.g. in the sector of traffic), an immediate national information exchange should be ensured.
- The inclusion of, e.g., tax authorities and savings banks in the distribution list of the German Joint Information and Situation Centre should be taken into consideration, at least in the event of an emergency.

B.4. Conclusions in the sector of media and PR work

4.1. Preliminary remark

Risk and crisis communication can be described as a domain of strategic crisis management.[10] For a start, the exercising staffs were therefore expected to do justice to the significance of professional media work in crisis situations and to the requirements concerning a successful dialogue with the population (crisis communication) to cope with the crisis.

[10] Cf. the following publications, based on the practice: Brandenburgisches Institut für Gesellschaft und Sicherheit (ed.) (2011) Standpunkt zivile Sicherheit. Behördliche Risikokommunikation im Bevölkerungsschutz, Potsdam; Zukunftsforum Öffentliche Sicherheit e.V. (ed.) (2011) Risiko- und Krisenkommunikation, Berlin (Schriften zur Zukunft der Öffentlichen Sicherheit, Ausgabe 1, 3/2011)

Due to the increasing importance of the Social Web, another challenge to the "LÜKEX 11" crisis staffs was to practise the handling of Internet-based "New Media" (so-called Social Media, Web 2.0). This was done for the first time during a "LÜKEX" exercise.

During the preparation phase, two brief evaluations on the use of the Web 2.0, as part of strategic crisis management, were commissioned in order to prepare for this aspect.[11] Against the background of structural change of the public, expert evaluations recommend an intensive examination of the functionality, the working patterns within the population and the potentials for strategic crisis management. In the course of the exercise preparation, the topic of "Web 2.0" was, for the first time, included on a limited scale, both as part of the coaching for press officers (workshop media and PR work) and media simulation ("LÜKIleck", "LÜKITweet" etc.).

4.2. Conclusions as to the contents

The exercise has shown that crisis communication depends on the availability and integrity of communication means and communication channels. In the course of the exercise preparation phase, e.g. during the workshop for press officers, it became obvious that the development of the "New Media" additionally requires competences in the press and media departments in order to allow a fast response by providing answers, reactions and information. It also allows to monitor contents on the Web, to evaluate and integrate them into the respective overview of the situation.

All crisis staffs understood that the strategic importance of coordinated media and PR work is one of the key aspects during a crisis.

The coordination of the crisis staffs concerning nationally important press releases could be improved.

The cooperation of neighbouring Länder has been beneficial, as the transmission area of the radio stations sometimes includes several Länder.

The exercise showed that so-called "citizens' helplines" and the target-oriented evaluation of social media allow insights into the involvement of the population. In the crisis staff of the Federation, the question whether the coordinated information of the population via the standardised telephone number "D 115" could be achieved, was thoroughly debated.

Furthermore, the following was suggested:

- The question to what extent authorities can use Online-media and social networks as part of their crisis management (including risk and crisis communication) and what behaviour guidelines are necessary for the practice should be investigated.

[11] Krämer, N. (2011) Nutzung sozialer Netzwerke in Krisensituationen. Gutachten für das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Bereich LÜKEX. Supported by J. Klatt, G. Neubaum, A. Von der Pütten, Duisburg; Schmidt, J.-H. (2011) Öffentlichkeiten im Social Web. Praktiken, Strukturen und Einsatzmöglichkeiten in Krisenszenarien. Fachgutachten im Rahmen der LÜKEX 11, Hamburg (Hans-Bredow-Institut für Medienforschung)

4.3. Conclusions concerning media simulation

The basic instruments of media simulation at LÜKEX-exercises (LÜKEX TV, print media, radio) has proved their worth. As the execution of the exercise is concerned, LÜKEX TV has developed to a decisive means for a quick and target group related scenario dissemination.

For the first time in the LÜKEX-exercise, the media simulation was slightly extended by the element of social networks. This addition was favourably received by all participants and valued as in line with modern standards.

Another advantage was the fact that the exercise participants had the opportunity to prepare themselves for the contents and practice of the exercise scenario, thanks to presentations by well-known instructors, practical instructions and the consolidation of the contents in work groups at the workshop "Media and PR work for press officers".

From the point of view of the exercising participants, the central availability of fictitious media, including live radio programmes, was regarded as beneficial.

The tried and tested basic instrument of media simulation at LÜKEX-exercises (print media, LÜKEX TV) should remain unchanged and be slightly further developed in future by doing justice to reality (e. g. live-radio, live-TV-spots, social media).

Picture 12: At "LÜKEX 11", the tools of fictitious media simulation proved useful – in the picture: media products and work during the exercise at the "National Media Centre".

4.4. Dialogue with the population

The exercise showed that, during crisis situations, the crisis staffs must react appropriately to the actions of the population. Furthermore, it became clear that during a critical situation the interactive dealing with the population is necessary and that the absence of reactions can lead to a loss of the legitimation of governmental actions.

During the execution of the exercise, the respective steering group ("Group Population") acted out about 100 scenes about the reaction of citizens to illustrate interactive behaviour.

The exercise proved that the use of Internet-based social media (e. g.: blogs, Online-forums) concerning questions asked by citizens are principally appropriate to make the crisis staffs aware of the psychosocial aspects of crisis management.

Furthermore, the following is recommended:

- In the crisis staffs, the different information requirements of the various groups of the population should be more strongly taken into consideration in the future.

- With the help of scientists, requirements and recommended actions concerning appropriate risk and crisis communication under the extended possibilities of Web 2.0 should be developed. The results should be tested through exercises to further develop the envisaged dialogue with the population.

Crisis communication – important instrument of strategic crisis management

In the context of world-wide information and media societies, crisis communication via media and PR work (in German MÖA) is an important instrument of strategic crisis management during LÜKEX exercises. It can considerably influence form and development of crises. During the LÜKEX exercises, the exercising staffs are therefore expected to pursue the exercise goal of "a broad coordinated active PR work for the situation appropriate information of the population and emergency staff in the context of an anticipatory cross-departmental crisis management" as well as permanent "active information work". To this end, a fictitious media landscape for the exercising staff is developed which is based, as realistically as possible, on the actual media landscape in Germany. During the execution of the exercise, the "National Media Centre" consists of professional media experts and journalists. It installs specific media components which are adapted to the development of the script: news agency reports; reports and comments of regional and national newspapers; radio reports; requests from journalists and citizens. Because of their increasing importance, "LÜKEX 11" was the first exercise to install the new "Social Media".

C. Conclusions concerning the exercise

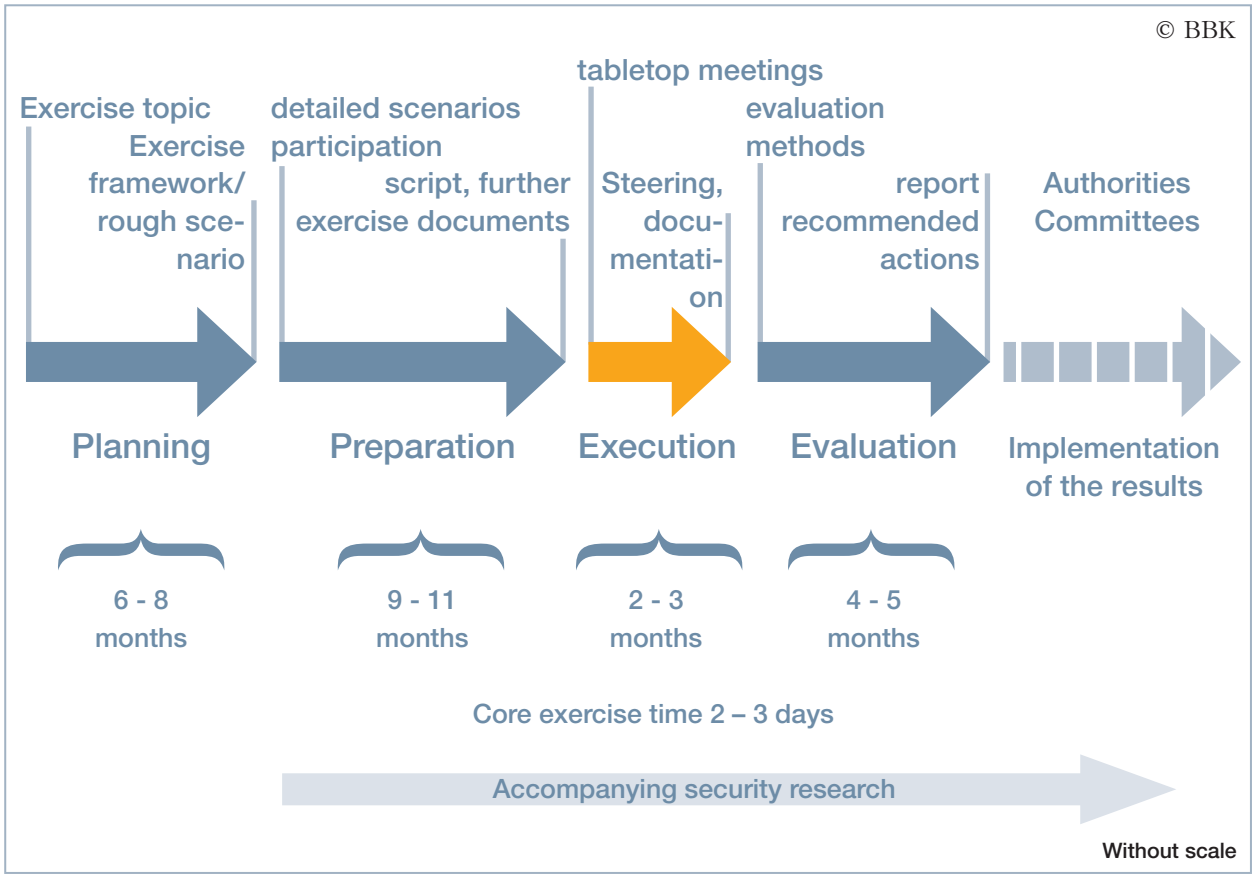
C.1. Preliminary remark

Generally, the "LÜKEX 11" exercise proved that the exercise concept works. In the course of the exercise cycle, the conception of Strategic Crisis Management Exercises, as described in the *Guideline for strategic Crisis Management Exercises,* could be successfully further developed in many respects.

Innovations concerned, above all:

- The development of project management in the sector of the Federation-Länder-coordination by introducing regular "project group head meetings", and the scenario development by organising sector-related "special workshops",
- The development of the script by means of different procedures concerning the "scenario-structure" (visualisation of "script components", "script modules" and injects).
- The implementation of the exercise by organising an "Additional Forum" for exercise visitors.

However, the course of the exercise cycle revealed that some individual aspects need to be optimised. Essential aspects concern the more binding organisation of exercise planning, the reduction of input and the initiation of accompanying research in the course of the exercise preparation as well as the systematic and effective execution of the exercise conclusions in the follow-up phase to the exercise.



Picture 13: Based on the experiences gained from "LÜKEX 11", a new complete exercise cycle for LÜKEX exercises (cf. p. 8, picture 3) was further developed.

C.2. Conclusions in detail

2.1. Exercise planning

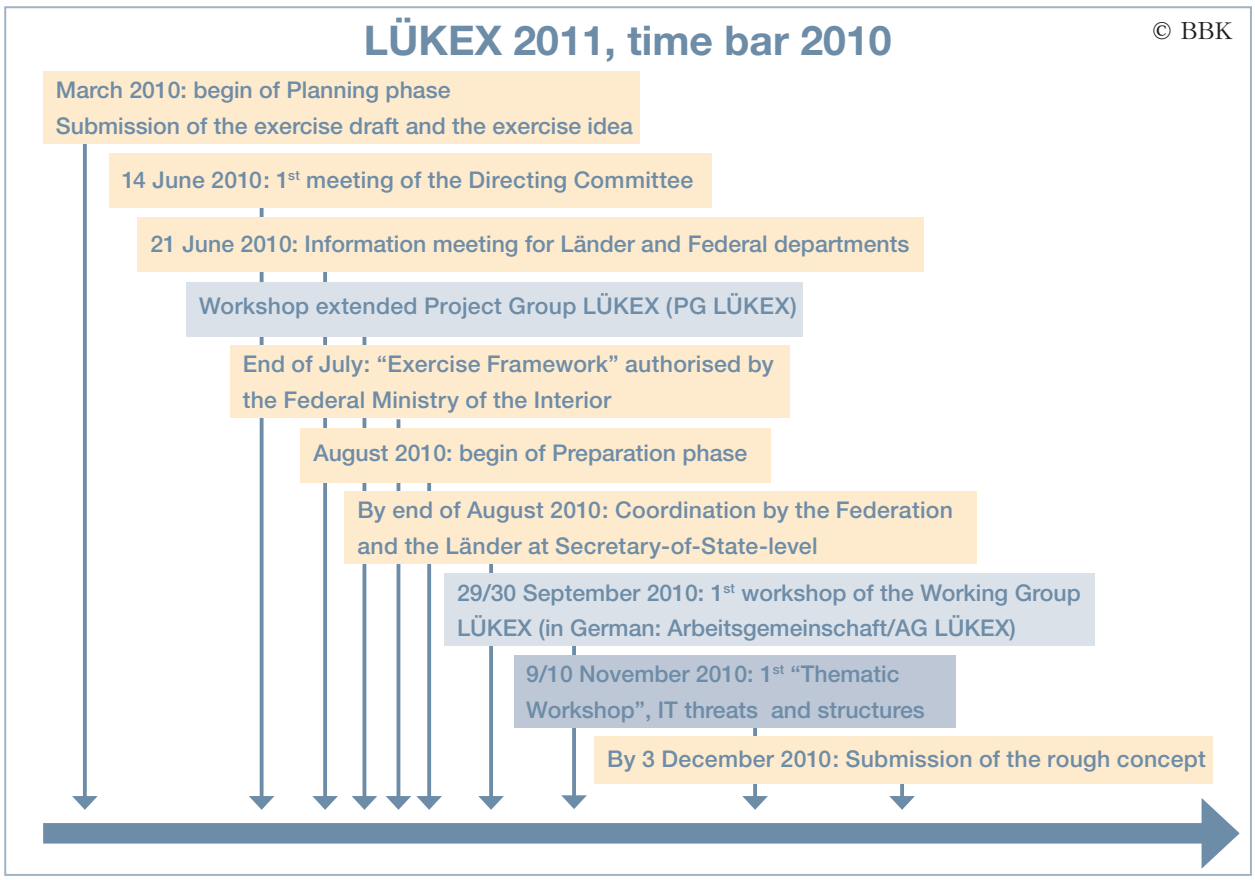
The exercise showed that the "Exercise Framework" as a basic document is indispensable to systematically include all participants. In future, it will be necessary to incorporate standardised exercise scenario key points into the Exercise Framework to generate cross-national and inter-divisional actions. This should already be done during the preparation phase.

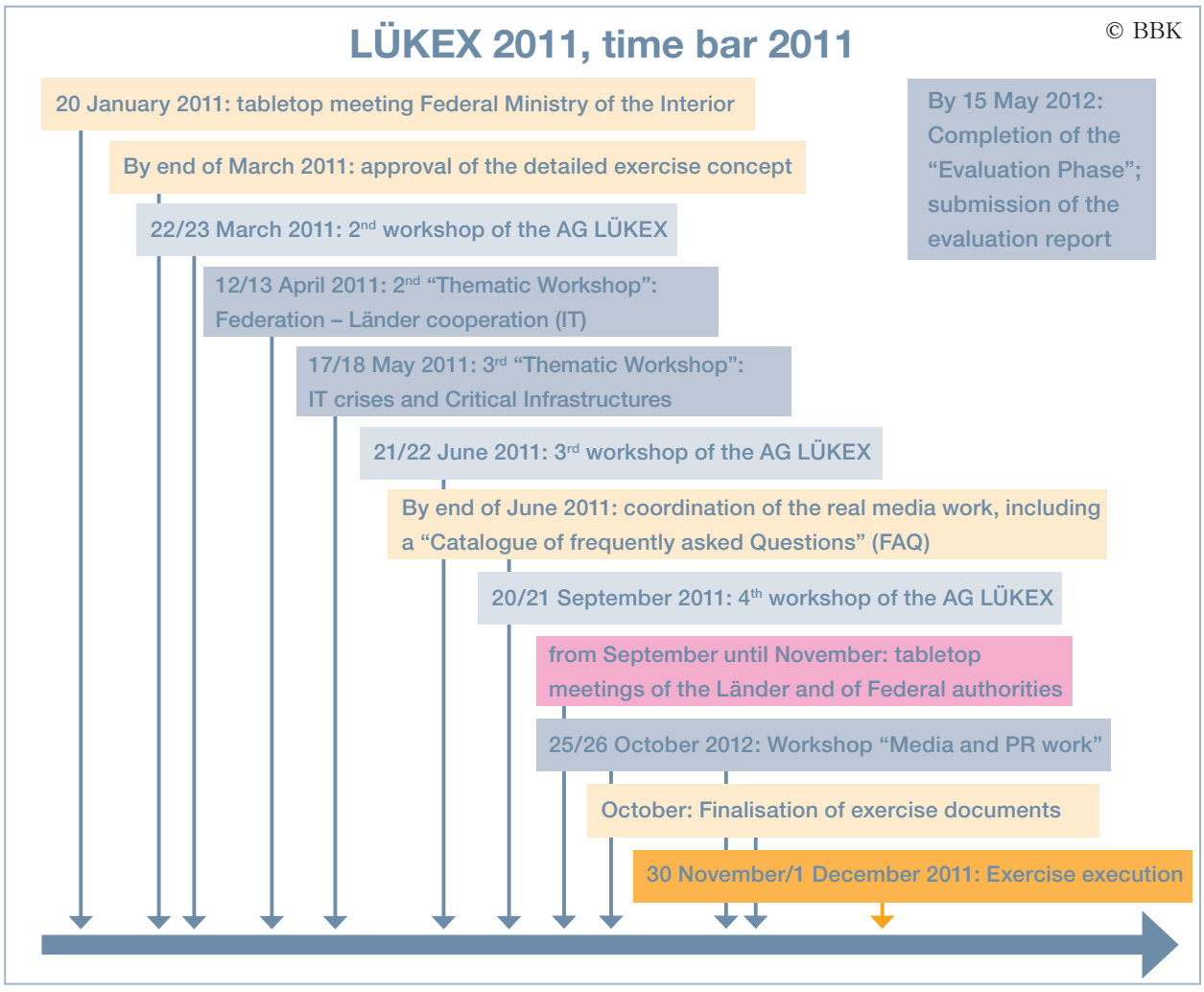
To ensure a scenario as realistic as possible, the affected Critical Infrastructure sectors should be involved in time and their exercise participation within the Exercise Framework planned in a binding way.

The LÜKEX steering committee allowed a systematic execution of the coordinated Exercise Framework. Thanks to the participation of representatives from the concerned Federal departments and the Federation-Länder-committees (AK V, IT-Planning Council), it also ensured an appropriate political oversight of the entire process. Further recommended actions are the following:

- In the future, essential cornerstones of the scenario and the exercise participation should already be defined during the planning phase. They should be taken into account for the exercise concept and be of a more binding nature.
- In the future, Critical Infrastructure enterprises which are close to the scenario should be involved as early and in as binding a way as possible to be able to take account of special conditions during the scenario development phase.
- In the planning phase, a joint Federation-Länder project structure should establish itself in the future, which consists of the Federal project group LÜKEX (PG LÜKEX Bund) and the respective project groups of the intensely exercising Länder as well as of LÜKEX representatives of the affected Critical infrastructure enterprises.

Picture 14: The Exercise Framework is the central basic document of each Strategic Exercise.


LÜKEX 2011, time bar 2010
© BBK
March 2010: begin of Planning phase
Submission of the exercise draft and the exercise idea
14 June 2010: 1st meeting of the Directing Committee
21 June 2010: Information meeting for Länder and Federal departments
Workshop extended Project Group LÜKEX (PG LÜKEX)
End of July: "Exercise Framework" authorised by the Federal Ministry of the Interior
August 2010: begin of Preparation phase
By end of August 2010: Coordination by the Federation and the Länder at Secretary-of-State-level
29/30 September 2010: 1st workshop of the Working Group LÜKEX (in German: Arbeitsgemeinschaft/AG LÜKEX)
9/10 November 2010: 1st "Thematic Workshop", IT threats and structures
By 3 December 2010: Submission of the rough concept


LÜKEX 2011, time bar 2011
© BBK
20 January 2011: tabletop meeting Federal Ministry of the Interior
By end of March 2011: approval of the detailed exercise concept
22/23 March 2011: 2nd workshop of the AG LÜKEX
12/13 April 2011: 2nd "Thematic Workshop": Federation – Länder cooperation (IT)
17/18 May 2011: 3rd "Thematic Workshop": IT crises and Critical Infrastructures
21/22 June 2011: 3rd workshop of the AG LÜKEX
By end of June 2011: coordination of the real media work, including a "Catalogue of frequently asked Questions" (FAQ)
20/21 September 2011: 4th workshop of the AG LÜKEX
from September until November: tabletop meetings of the Länder and of Federal authorities
25/26 October 2012: Workshop "Media and PR work"
October: Finalisation of exercise documents
30 November/1 December 2011: Exercise execution
By 15 May 2012: Completion of the "Evaluation Phase"; submission of the evaluation report

2.2. Exercise preparation

The exercise showed that during the preparation phase – the "centre piece" of the exercise – a considerable effort had to be made to come to a close, cross-national agreement concerning the development of the scenario and the work on the script.

However, the dimensions and impact of some cross-national basic scenarios were not sufficiently or differently perceived. Therefore, the Federation should have a greater influence on the development of the scenario in future to result in a greater involvement of the Federation and the Länder, i.e. to achieve the consolidation and concentration of the scenario approach.

In this respect, the regular meetings of the Federal project group with the project heads of the intensively exercising Länder have proved particularly useful. As "LÜKEX 11" is concerned, these meetings took place, for the first time, during the exercise preparation phase. Therefore, the development of the scenario and the script could be systematically advanced and questions concerning the exercise organisation and support of the project work be discussed appropriately within the Länder groups.

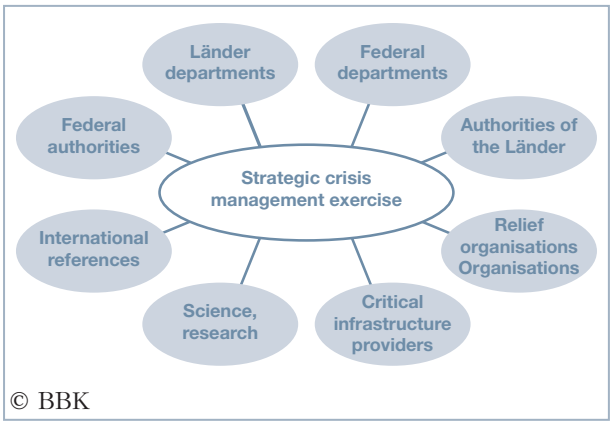
The organisation of sector-related "special workshops" about closed subject areas (air traffic, finance etc.) proved particularly efficient to assess and further develop systematically chosen script components as to their conclusiveness.

The scenario, on which the exercise was based, included different attack vectors and numerous individual incidents in different areas. Altogether, the IT-specific script components, which were based on a comprehensive approach, involving the considerable involvement of IT and telecommunication structures, of IT structures in the banking and finance sector as well as local and air traffic carriers, were designed close to reality. Therefore, the exercise participants evaluated the entire scenario as predominantly suitable to reach the exercise targets.

To generate a comprehensive and national involvement, a great number of local single events should be given up in favour of a few major cross- national and inter-divisional basic scenarios, which need coordinated Federation-Länder-decisions ("depth before width"). On an individual basis, lines of action and critical business processes can be thus reproduced from the very top to the lowest level.

Generally, like in the previous exercises, the establishment of a national "Working Group LÜKEX" (AG LÜKEX) proved its worth, where representatives of all exercise participants (Federal departments, Critical Infrastructure providers, Länder as well as participating experts from science, universities, organisations and associations) are represented. As the number and contents of the AG LÜKEX meetings is concerned, there is still room for improvement.

The involvement of the exercising Länder into the exercise preparation phase, above all their participation in the preparatory AG LÜKEX meetings, was useful. Thus, national awareness and exchange concerning the core topics of the scenario could be achieved.



Picture 17: in the course of the long-lasting cooperation of all those responsible for crisis management from the Federation, the Länder, social organisations and enterprises, "cooperation networks" are developed during the preparation phase which considerably contribute to ensuring the functionality of the relief system in real crisis situations beyond the exercise.

Again, the „Thematic Workshops“, which were organised parallel to the preparation of the exercise, were particularly useful. They covered the following selected topics:

- Introduction to IT-threats and structures
- IT-crisis management of the Federation and the Länder
- IT-crises and Critical Infrastructures

Furthermore, the following was recommended:

- The design of the scenario should be based on the principle of “depth before width”.
- The practice of regular project group head meetings should be continued.
- Meetings involving fewer people (e.g. expert workshops with Critical Infrastructure enterprises, meetings of script coordinators) should be organised on a more frequent basis.
- The efficient method of „Thematic Workshops“ should be continued.

2.3. Exercise execution

In the course of the exercise, the preceding tabletop meetings (in German: “Planbesprechungen”) were particularly useful. The tabletop meetings, which took place in the intensively exercising Länder and with some Federal authorities on the fictitious date of 25/11/2011 and at different appointed times, preceded the execution of the exercise (30/11-01/12/2011). The tabletop meetings served the following purposes:

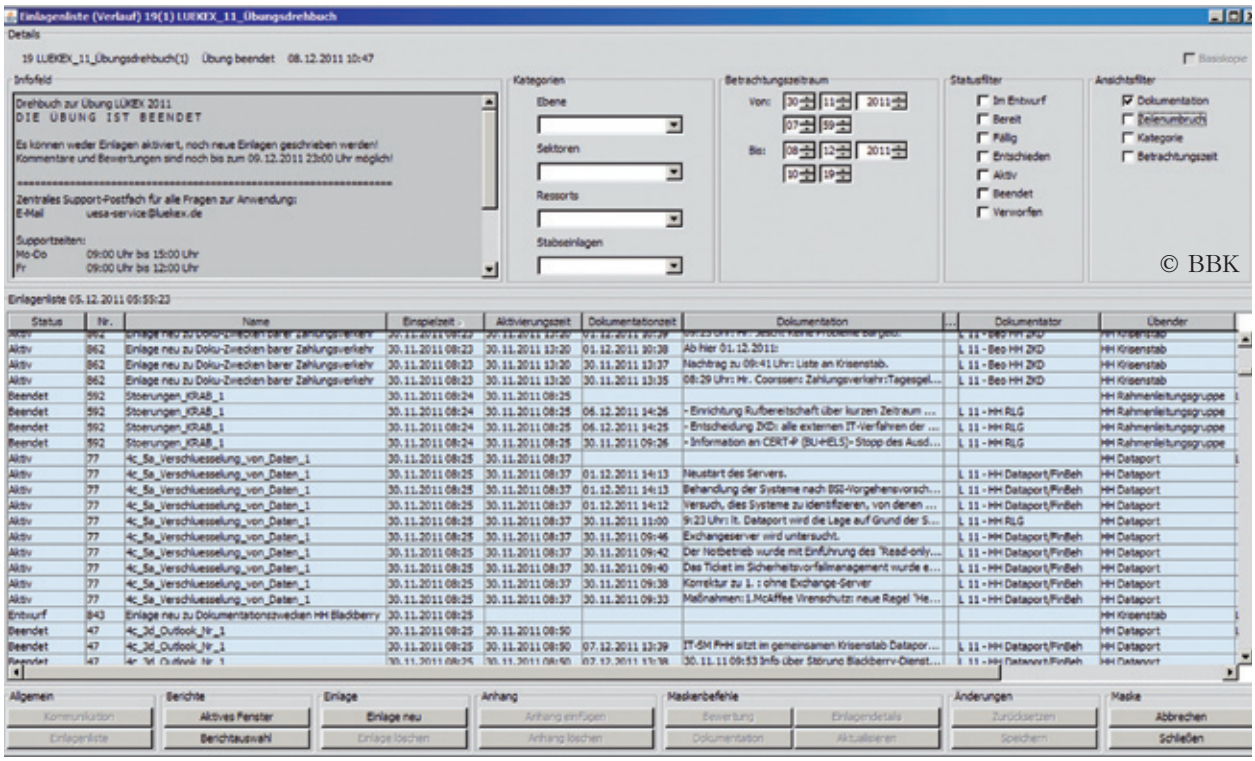
- Identification of one‘s own potential involvement
- Exercising of decision processes in the crisis staffs - some of them met for the first time in such circumstances.
- Discussion and decision about preventative measures on the basis of the fictitious starting point.

Picture 18: In the course of the Exercise execution, the preceding tabletop meetings proved particularly useful – in the picture: tabletop meeting of the Crisis staff Hamburg

The preceding communication test in the exercise week turned out to be essential to ensure the smooth development of the exercise, whilst using different means of communication (telephone, fax, mail, exercise steering application). During the course of the exercise, the exercise steering application (in German abbreviated as ÜSA) worked well. According to the feedback, the functionality, ergonomics and system administration of the steering needs to be improved.

Furthermore, the following should be optimised:

- In the future, tabletop meetings should be an integral component of the exercise execution as part of the exercise cycle.
- In the future, the communication test in the exercise week should be extended to a small "communication preliminary exercise" to prepare all participants early enough for the exercise and to ensure a smooth start of the exercise.
- The Exercise Steering Application (in German: ÜSA) should be adapted to the needs. The functionalities should be restricted to the scope of functions which are absolutely necessary for the exercise.



Picture 19: The Exercise Steering Application (ÜSA) supported the execution of the exercise – in the picture: screenshot from the exercise script

2.4. Exercise evaluation

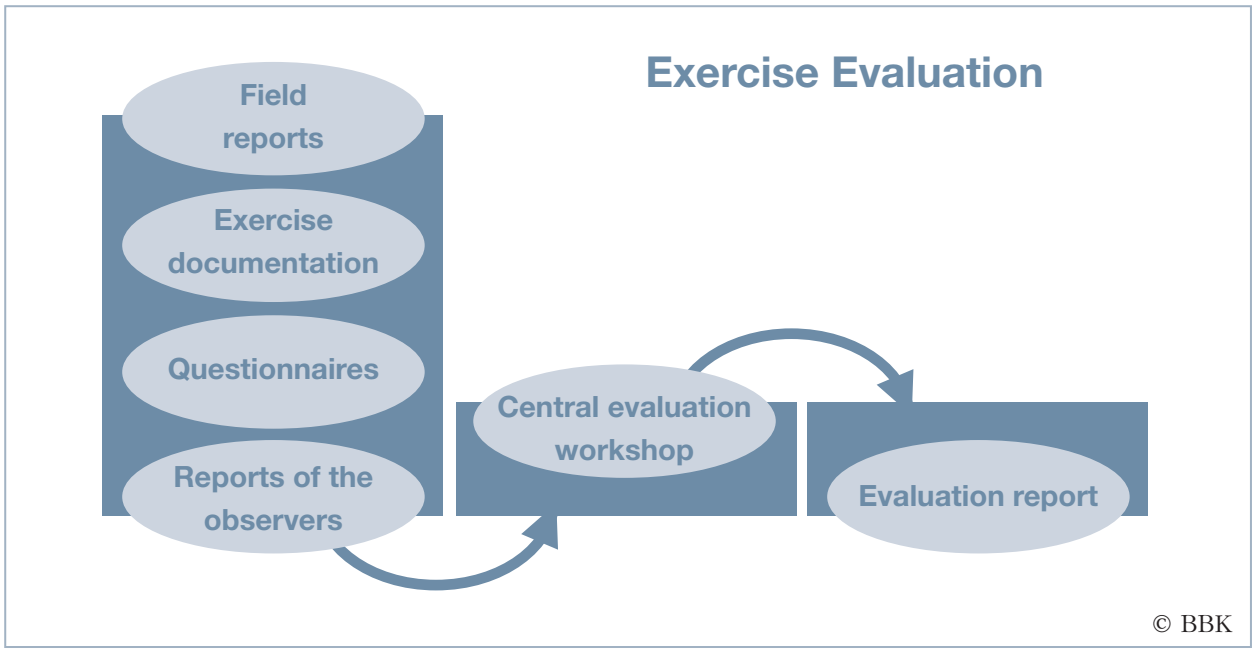
Generally, the qualitative overall approach to the exercise evaluation, by means of different methods and sources of insight (interview, monitoring, contents analysis and consensual agreement between all exercise participants), has made sense. The conceptual framework for exercise evaluation purposes, which was coordinated on this basis, should be further developed, in line with the practice, to support and facilitate the exercise evaluation of future exercises.

The preparation phase showed that valuable insights can be gained, which should be systematically collected and increasingly used for exercise evaluation purposes.

Thanks to the increased deployment of exercise observers and liaison officers during the execution of the exercise, valuable conclusions could be drawn about the work of the exercising staffs which could then be used for the evaluation of the exercise. Whether the mutual exercise observation by the Länder might also help to get an insight, has to be assessed in detail. In the context of the exercise follow-up phase, different exercise participants demanded the increased continuation of the initiatives which were started during the exercise by focussing on the aspect of sustainability. Insights and results, gained form the LÜKEX-process, should therefore be consistently accounted for as part of the strategy development by the authorities and the Federation-Länder committee work.

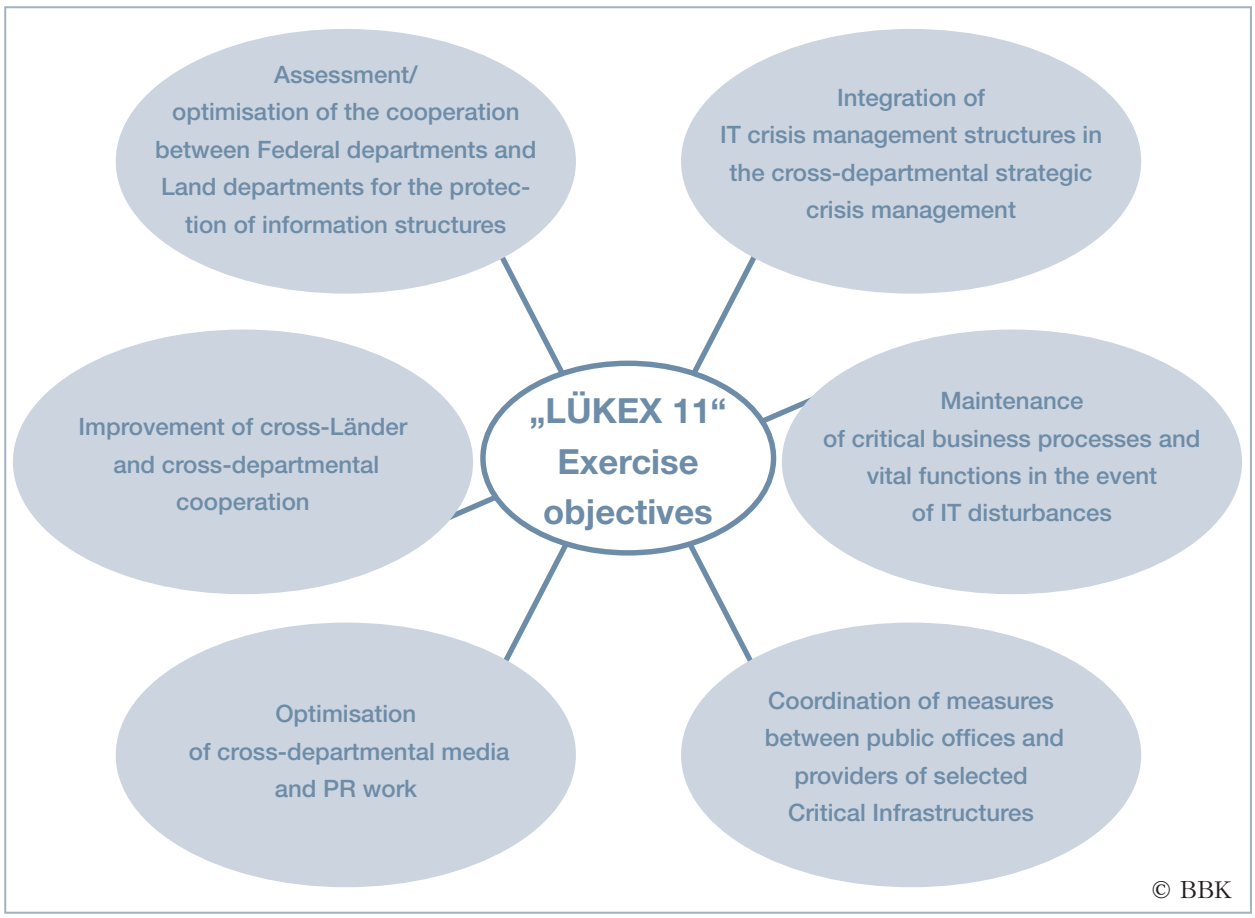
Furthermore, the following is recommended:

- The coordinated framework for the evaluation of the exercise and introduced evaluation sheets should be further developed in a practice oriented way to support and facilitate the exercise evaluation.
- It should be assessed whether a process-related exercise evaluation, possibly supported by external scientific evaluation measures, might be considered to support the exercise evaluation during the preparation phase.
- It should also be assessed how the assignment of exercise observers could be optimised. Especially, the mutual exercise observation between exercise participants should be more strongly considered.



Picture 20: Process of the exercise evaluation

D. Conclusion



Picture 21: General exercise objectives of “LÜKEX 11”

The exercise “LÜKEX 11” was a success. This is particularly true with regard to the higher ranking exercise objectives of the exercise framework and, here, to the sensitisation for issues relating to “IT-Security” and the initiation of appropriate integration processes (e. g. the combination of IT-crisis management and general crisis management).

During the exercise, irrespective of further rules, which still have to be set up by the IT planning council, for the first time, the information exchange between the Federation and the Länder could be successfully tested via defined reporting channels. Thus, the establishment of an „AdministrationCERT-Association“ („VerwaltungsCERT-Verbund“) could be triggered. The development of networks, which could be achieved via “LÜKEX 11”, is a good basis for the future cooperation in general crisis management, such as in the IT-crisis management of the Federation, the Länder and the involved Critical Infrastructure enterprises and associations.

In terms of sustainability, the systematic implementation of the exercise results and the transfer of relevant expert knowledge beyond the circle of the exercise participants will be an essential key aspect of subsequent activities, and, above all, of committee work.

To achieve this, the insights gained from the exercise should be circulated at expert congresses or within further training courses at the Academy for Crisis Management, Emergency Planning and Civil Protection (in German abbreviated as AKNZ) and comparable training institutions of the Federation and the Länder (Federal College for Security Studies, Military Academy of the Armed Forces, German Police University, Land fire brigade colleges, universities of the Länder etc.) to impart incentives for the consolidation of cross-national strategic crisis management, by including the respective IT-crisis management.

Additionally, “little” exercises should be regularly organised at executive level to be able to further develop the exercise culture and to look into individual questions in more detail.

Furthermore, the exercise results should more often be circulated within politics and the media and be used for accompanying security research.

With respect to increasing international networks, the European dimension, which was rudimentarily represented in “LÜKEX 11” by the involved supranational institutions ECB and EUROCONTROL, should, in future, be considered even more strongly.

If you have any questions concerning strategic management exercises, “LÜKEX” in general and “LÜKEX 11”, the LÜKEX-Team would be pleased to assist you. You can contact us via the following address:

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Projektgruppe LÜKEX Bund - Geschäftsstelle
Ramersbacher Str. 95
53474 Bad Neuenahr-Ahrweiler
Tel.: 0228/99550-5610
Fax: 0228/99550-5630
Mail: luekex.info@bbk.bund.de
www.bbk.bund.de / www.luekex.de

Afterword

Dear readers!

The evaluation report "LÜKEX 11" is the visible result of the concerted action of the Federation, the Länder and Critical Infrastructure enterprises. It was the first time that these bodies met the new challenges of IT-security in Germany to such an extent in the context of a LÜKEX exercise, here the 5th Strategic Crisis Management Exercise. The report aims at making the experiences gained from "LÜKEX 11" available to all parties concerned from the wider exercise environment – training institutions, science, media, security experts and others. At the same time, the experiences – or *lessons learned* – are meant to stimulate the further optimisation of structures and procedures in strategic crisis management.

The report is also the final step of intensive project work which went on for two years. Special mention must be made of the great personal commitment which the people in charge at the Federal and Land authorities as well as participants from economy, science and society have shown in the course of the entire exercise cycle.

The development of the scenario and the work on the script and, indeed, the exercise preparation and implementation – including the exercise evaluation – would not have been possible without the specific knowledge and the personal commitment of the different exercise participants. As a consequence, the highly complex exercise topic "IT-security" could be made manageable and tangible even to untrained users and, of course, to those who, in the event of an overall crisis, were also affected. It is important to take these less apparent exercise results of "LÜKEX 11", the knowledge transfer and the networking effects into account as well.

On behalf of the project group, I would like to thank all participants for the professional and fruitful co-operation, which was a "collaboration" in the best sense of the word.

Norbert Reez
Project Leader
PG LÜKEX Bund

Federal Office of Civil Protection and Disaster Assistance

BBK was founded in May 2004 as an important contribution of the Federal Government to the new strategy for the protection of the population in Germany. Together with the Federal Agency for Technical Relief (THW), BBK as a supreme federal office within the portfolio of the Federal Ministry of the Interior (BMI) fulfils tasks relating to civil security measures, above all in the sector of civil protection and disaster assistance. It supports the BMI in these areas and also, by consent of BMI, the responsible supreme offices. Above all, BBK is responsible for the following tasks:

- Development of a national risk analysis
- Development of standards and framework concepts for civil protection
- Warning and information of the population
- Development of a modular warning system with the core element of satellite-based warning information by including the existing and future alert and warning media
- Information of the population about protection and support possibilities
- Promotion of training measures for the population
- Education, further education and training of decision makers and managers from the sector of civil security measures
- Support of the municipalities concerning self-protection measures
- Technical and scientific research
- Evaluation and collection of publications
- Assessment of equipment and procedures as well as participation in their standardisation and registration
- Complementary equipment and training of units active in disaster management, i.e. in the areas of fire prevention, CBRN-protection, medical service and support
- Complementary procurement of first aid equipment
- Protection of cultural assets according to the Hague Convention
- Office of the Commission for the Protection of the Civil Population

Furthermore, the competences in the sector of civil protection which, according to clause 85, par. 4 of the German Constitution are within the remit of the Federal Government, were assigned to BBK.


© BBK

BBK attaches high importance to the implementation of a personnel policy which is aware of the demands of family life. Flexible working hours, rooms for parents and children and home offices are examples of BBK's endeavours to effectively promote a balance of work and family thanks to well-established and future-oriented measures. At the end of February 2009, BBK was certified in the framework of an audit concerning the balance of work and family. To this end, the existing catalogue of such offers will be further developed and their implementation optimised in the years to come.

Certified since 2009
Audit work and family

BBK attaches high importance to the implementation of a personnel policy which is aware of the demands of family life. Flexible working hours, rooms for parents and children and home offices are examples of BBK's endeavours to effectively promote a balance of work and family thanks to well-established and future-oriented measures. At the end of February 2009 BBK, was certified in the framework of an audit concerning the balance of work and family. To this end, the existing catalogue of such offers will be further developed and their implementation optimised in the years to come.

List of abbreviations

AG	Working Group
AKNZ	Academy for Crisis Management, Emergency Planning and Civil Protection
BfIT	The Federal Government Commissioner for Information Technology
BfV	German Office for the Protection of the Constitution
BKA	Federal Criminal Police Office
BPOL	Federal Police
BSI	Federal Office for Information Security
BVA	Federal Office of Administration
CERT	Computer Emergency Response Team
Cyber-AZ	National Cyber Defence Centre
EZB	European Central Bank
FAQ	Frequently Asked Questions
GMLZ	German Joint Information and Situation Centre (of the Federation and the Länder)
IKT	Information and Communication Technology
IT	Information Technology
KRITIS	Critical Infrastructures
LÜKEX	Cross-Länder Crisis Management Exercise
NPSI	National Plan for the Protection of Information Structures
SKUKdo	Armed Forces Support Command
SPOC	Single Point of Contact
THW	Federal Agency for Technical Relief
ÜSA	Exercise Steering Application
WBK	Military District Command
ZMZ	Civil-military Cooperation
ZSKG	Law on the Civil Protection and Disaster Management of the Federation (Civil protection and disaster management law)
ZÜST	Central Exercise Steering