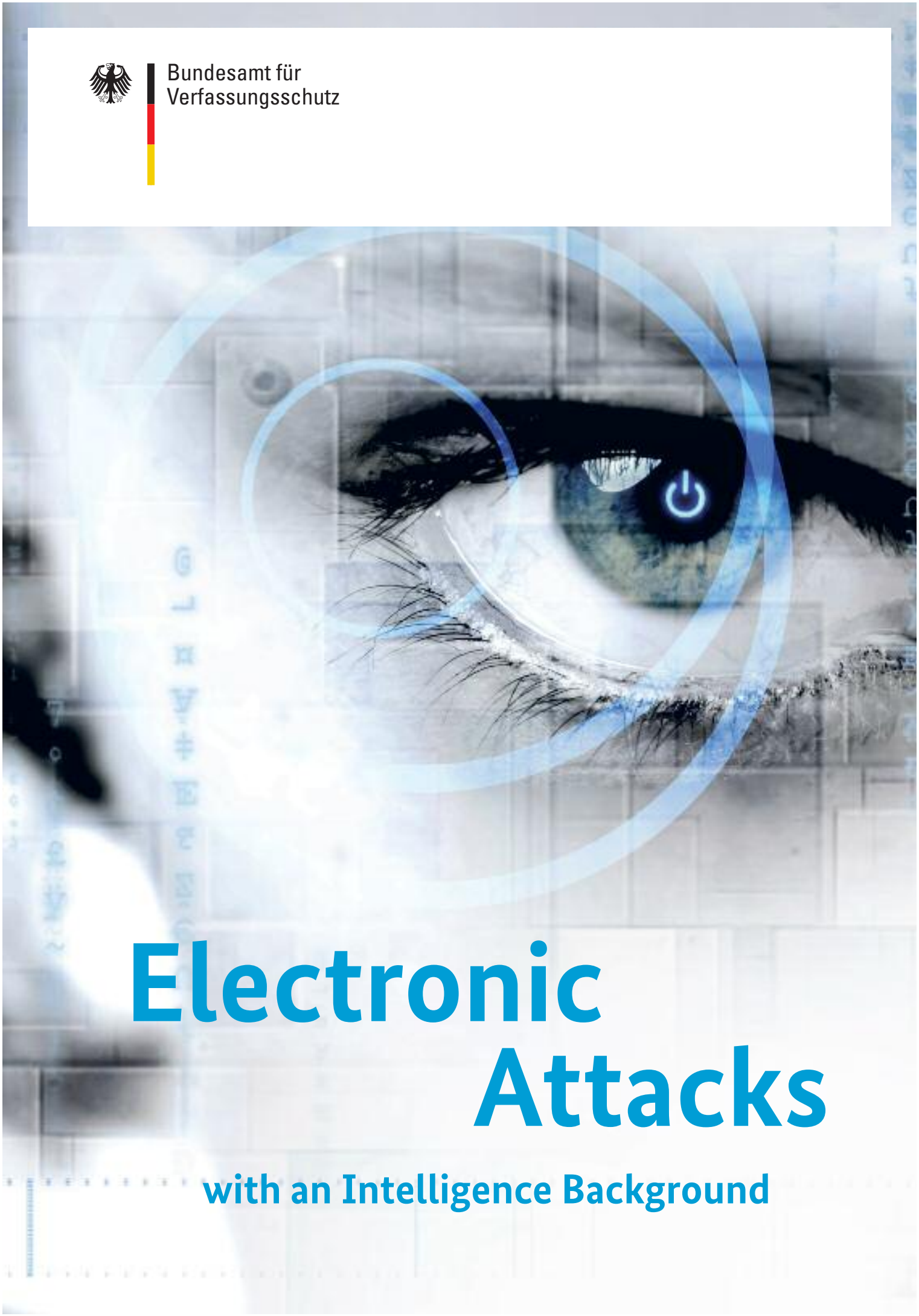
Bundesamt für
Verfassungsschutz



Electronic Attacks

with an Intelligence Background

Electronic Attacks

with an Intelligence Background

Contents

Risks to Modern Information Society

Until 20 years ago, newspapers, radio, and TV as well as phone, fax, and traditional mail prevailed in our everyday communications. In the early nineties, the computer, Internet, emails, mobile phones, and other forms of digital media made an entrance into our everyday lives.

This continuing digital revolution has rapidly changed the world in the past decades. It has influenced the individual communicative behaviour in society, and it has multiplied the quantity of information quickly available.

Apart from new liberties and conveniences, also new dependences and risks have emerged. The information and communication technology creates new spaces, but it is simultaneously exposed to various threats.

The Bundesamt für Verfassungsschutz (BfV) has been observing for some time how extremists and terrorists use the new technologies for their own purposes and adapt their forms of agitation and their strategies to the new possibilities. There are also various possibilities offered to foreign intelligence services by the rapid development in information and communication technology: possibilities which may be exploited for data spying, data alteration and computer sabotage. So the protection of highly sensitive information as well as of national critical infrastructures has become a priority in the context of internal security in recent years, for almost our entire social dealings depend on a well and reliably working IT infrastructure these days.

Our modern information society is currently being faced with the challenge to maintain a balance between security interests and civil rights and liberties on the one hand and on the other hand to counter the various threats posed by the digital revolution in an efficient and forward-looking way.

It is the task of BfV's counterintelligence in particular to find ways how to reliably protect IT systems against unauthorised access by foreign intelligence services. Thus, we feel it our duty to identify illicit measures of foreign services on German territory in a timely manner and to prevent them.

Germany as a Target of Espionage

The Federal Republic of Germany is, due to its geopolitical position, its role in the European Union and in NATO, as well as its being a site for numerous leading-edge technology enterprises, attractive to foreign intelligence services. Its open and pluralistic society makes it easy for foreign powers to collect information. This intelligence collection takes place both overtly and covertly.

The intelligence and security services of the People's Republic of China and the Russian Federation in particular are engaged in extensive espionage activities against Germany. Their priorities depend on the political guidelines set by their governments.

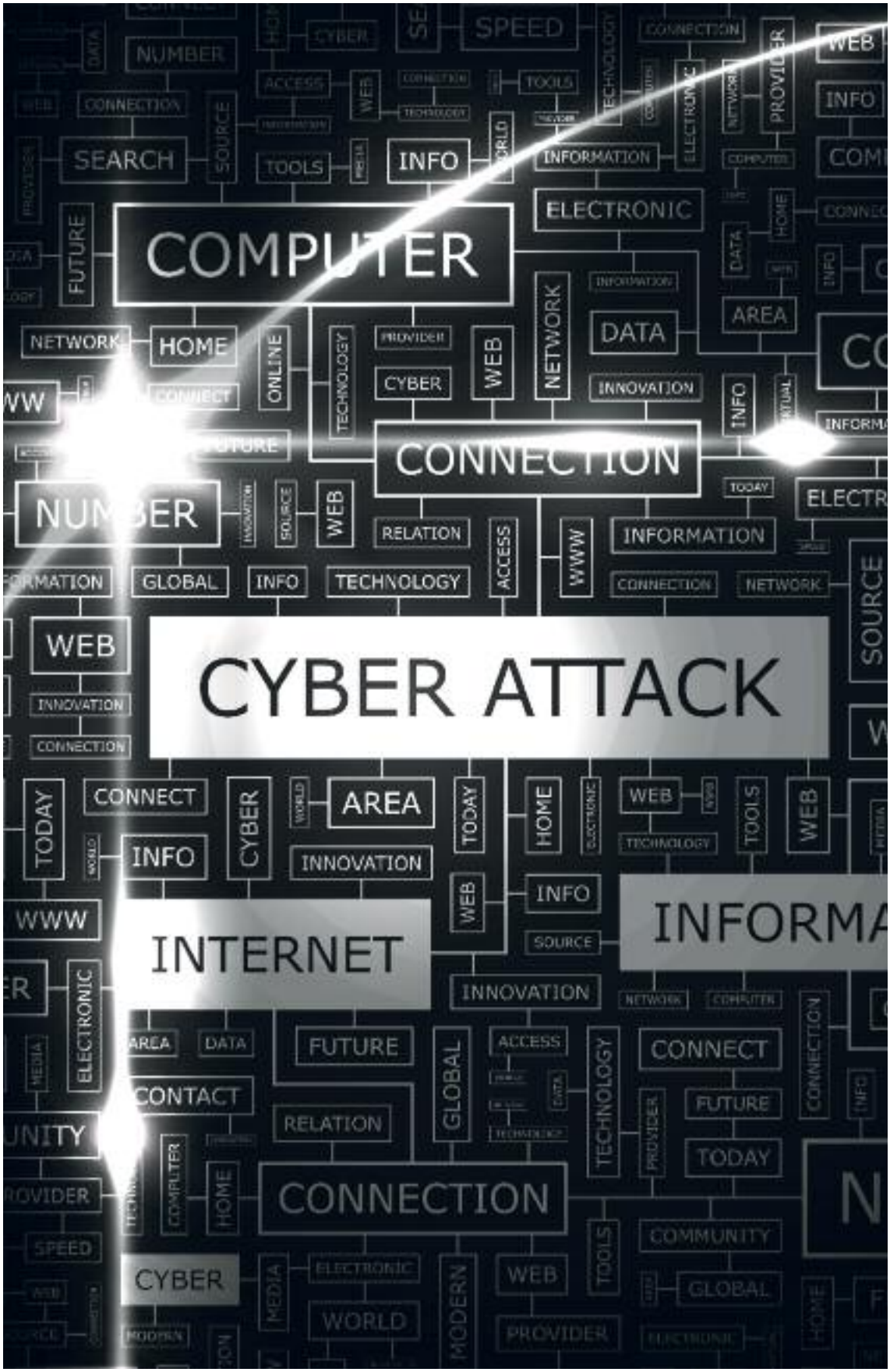
This includes the statutory or official task to support the country's national economy by providing information collected by intelligence methods.

The sustainability and global orientation which characterises the presumed attackers' intelligence collection efforts are clear evidence of a strategic intelligence collection approach.

The „classical" means of espionage such as the use of human sources continue to be a major part of espionage activities against Germany. This has recently been confirmed by a couple sentenced to several years in prison (in 2013). For more than twenty years, both the husband and his wife had worked, using false identities, for a Russian external intelligence service.


OK
OK

Besides, technical intelligence collection methods have continuously been gaining in importance. Another undisputed fact is that apart from China and Russia also the intelligence services of other states have the resources to be able to carry out similar technical intelligence collection measures against German targets from abroad.


COMPUTER
CYBER ATTACK
CONNECTION
INTERNET
INFORMATION
NETWORK
DATA
WEB
INFO
SEARCH
TOOLS
SPEED
ELECTRONIC
TECHNOLOGY
HOME
AREA
FUTURE
GLOBAL
INNOVATION
CONNECT
TODAY
CYBER
WWW
CONTACT
RELATION
ACCESS
SOURCE
PROVIDER
COMMUNITY
MODERN
WORLD

Definition of Electronic Attacks

Since 2005, extensive targeted electronic attacks against federal agencies, political decision-makers and commercial enterprises have been noted, which have been and continue to be of a high quality standard and which pose a serious threat to information security in these areas.

The large number of sophisticated cyber-espionage attacks solely against German federal agencies observed by us for many years has shown that there is a serious threat to the security of German IT systems. Of special interest to the attackers are the fields of foreign affairs and security policy, finance as well as the military and armaments.

In Germany, the BfV and the LfVs are responsible for the investigation of intelligence activities or activities endangering security on behalf of a foreign power. Other responsibilities of the BfV as part of the German security architecture are

- countering electronic attacks carried out by foreign intelligence services against targets at home and against German diplomatic missions abroad;
- countering electronic attacks carried out by extremists or terrorists against targets at home and against German diplomatic missions abroad.

The term ‘electronic attacks’ commonly refers to targeted manoeuvres by means of and against IT infrastructures. These include activities aimed at collecting information, but also efforts designed to destroy or sabotage those systems.

Such activities are

- spying out, copying and modifying data,
- taking over third parties' electronic identities,
- misusing or sabotaging IT infrastructures, as well as
- taking over computer-controlled web-based manufacturing and control systems.

These attacks may be carried out:

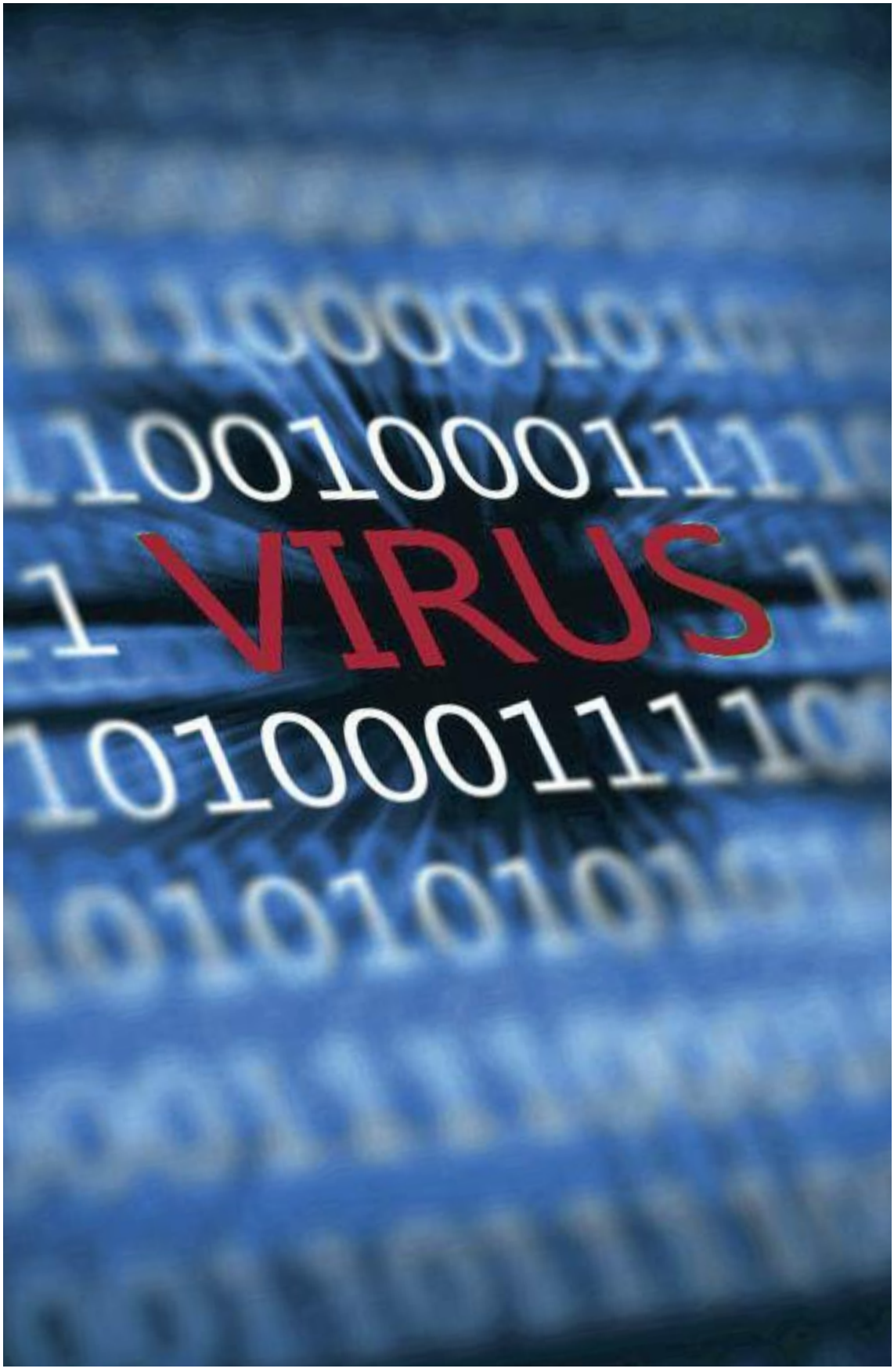
- from outside via computer networks (such as the Internet)

  or

- by direct, not web-based access to a computer (e.g. by means of manipulated hardware components).

Electronic attacks have become an additional major means of information collection for foreign intelligence services in recent years. There are various reasons for that:

- Electronic attacks are an efficient means of information collection whose investigation by those concerned is complex, with the anonymity of the Internet making an identification and tracing of the perpetrators extremely difficult.
- In addition, such attacks are inexpensive, can be carried out in real time and have excellent prospects of success.


VIRUS

The potential threat posed by electronic attacks against German targets which are controlled by an intelligence service is much more serious at present than that from electronic attacks carried out by extremists or terrorists, such as defacements or DDoS attacks. The attacks differ considerably in quantity and quality as well as in the financial and human resources available to the perpetrators.

Foreign intelligence services are mainly interested in information which can be gathered from state institutions. The persistent electronic attacks with a presumed intelligence background against federal agencies demonstrate the important role of this modus operandi.

The length of some attack operations and the global orientation in selecting subjects and victims clearly point to strategic state-controlled intelligence procurement activities.


8GB
micro

Methods of Attack

The number of undetected electronic attacks must still be assessed as being large, because the methods have become more and more sophisticated. The attackers have continuously been developing and refining the malware used, thus increasing the efficiency of such attacks.

Even the latest antivirus software cannot detect such malware!

Electronic attacks are so dangerous (and „successful“) because they are hard to detect and are often not recognised even by victims with pronounced security awareness. Malicious mails are generally characterised by excellent „social engineering“, i.e. they are tailor-made so that they meet the victims' fields of interest or responsibility, thus raising no suspicion at first view. Furthermore, the senders' addresses of such emails are forged in a way that they seem to belong to a sender known to the victim.

Apart from the classical email involving a Trojan, where the malicious program is mostly contained in the annex and will only be activated when the annex is opened, other very sophisticated and scarcely identifiable methods of attack have meanwhile been used. These include so-called drive-by infections: The attackers create websites containing malicious software or hack and manipulate existing websites. The selected victims are systematically approached by sending emails and induced to visit the infected websites via links. In addition, data carriers distributed as advertising media for example (USB sticks, flash cards, CDs etc.) are used to infiltrate malware.

Example: G20 Summit

In connection with major financial and/or economic meetings, there has regularly been an increase in the number of electronic attacks. So in 2013, as reflected by trends in previous years, attacks were noted which were related with the G20 Summit held in Saint Petersburg (Russia) on 5 and 6 September 2013. Apart from several federal ministries, also the banking sector was targeted. In skilfully arranged emails sent to senior decision-makers and their direct assistants, a communication of the Sherpa Group was faked. This was done in an effort to make the unsuspecting recipients of the mails rashly open the malicious annex, thus setting off an infection of the systems.

The information obtained in this way would - in theory - have allowed the attacker to assess the decisions of this meeting on issues of international financial and economic policies, of energy, climate and development policies, as well as of anti-corruption policy already in advance and to react accordingly.

Such information is of particular interest to foreign intelligence services. On account of the characteristics and existing parallels with other attacks on the German government's network, the origin of these attacks of 2013 is supposed to be in China.

Attacks on Trade and Industry

Apart from guaranteeing the integrity of the government's IT systems, the security of IT systems in the economic sector is one of BfV's priorities.

It is clear that cyber-espionage is an efficient method of intelligence collection not only in the public sector, but especially in the industrial sector and research area.

For economic reasons mainly, potential victims often rely on standard IT components, which may contain vulnerabilities that can be exploited by attackers. Also the increasing use of mobile devices (smartphones, tablet computers) with access to the company's network offers new possibilities of infiltrating a system.

Successful attacks of espionage – either by traditional methods of intelligence gathering or by means of electronic attacks – may cause immense damage to the country's national economy if there is an outflow of intellectual property from research centres and private companies. On the whole, electronic attacks by all the various groups of perpetrators have already caused financial damage to Germany's economy which is estimated at several billions of euros up to now.

The main targets include companies specialised in the fields of armaments, automobiles, aerospace as well as satellite technology. In addition, technological enterprises and research institutes close to industry are the focus of attention.

As opposed to attacks on federal agencies, electronic attacks on private companies are more prone to escape the security agencies' notice because of the companies' decentralised IT structures, to which state authorities have no access.

Another factor is that private companies only rarely contact the security agencies on their own initiative in order to report relevant IT incidents.

- **We are aware of the companies' fears to lose prestige and to sustain drops in turnover if a successful attack of espionage or sabotage becomes public knowledge.**
- **We are, however, able to offer advice, without the necessity of reporting the relevant incidents to the police.**
- **We can also refer companies seeking advice to competent members of other German security agencies, who can provide support.**

Confidentiality is one of our top priorities in our offer of advice and support!

Cyber-Sabotage Targeting National Critical Infrastructures

The term ‘electronic attacks’ does not only refer to activities aimed at collecting information by electronic means. It also includes electronic acts of sabotage systematically carried out against so-called national critical infrastructures, acts which pose a considerable potential threat to internal security.

The malware used for electronic attacks to gather information, i.e. espionage malware, can basically also be used for the purposes of sabotage. If an attacker has gained access to an IT system, he can perform a variety of manoeuvres there without being hampered, including those against its integrity and availability.

A country’s national critical infrastructures include organisations and facilities of primary importance to the community. They are essential for the functioning of a society and economy, their failure or disruption would entail severe supply shortages, considerable disturbances of public security or have other dramatic effects.

A medium-term or long-term paralysation of power stations, hospitals, railway stations or airports, for example, would certainly cause immense chaos.


0
2
4
6
8
10
bar

Sectors defined as critical infrastructures are:

- **Energy**
- **Information technology and telecommunications**
- **Transport and traffic**
- **Health**
- **Water**
- **Food**
- **Finance and insurance industry**
- **Government and public administration**
- **Media and culture**

So national critical infrastructures are facilities we depend on, facilities which are vital to our modern society. Nobody wants to imagine the chaos which might arise in case of long-term breakdowns or system failures in above-mentioned sectors.

There is no evidence of a direct threat to national critical infrastructures in Germany from extremists or terrorists at present. There are no indications that the latter do have the IT expertise required and the human as well as financial resources to carry out attacks on complex IT systems provided that those systems are appropriately protected and safeguarded.

Nevertheless, there have been some efforts by extremist and/or terrorist groups to acquire such know-how.

Military agencies and intelligence services of foreign states are currently judged to be more capable of carrying out attacks on national critical infrastructures – though this threat must be described as being rather abstract at present. Some states are supposed to be able - considering their financial, technical and human resources - to commit electronic acts of sabotage. But there is currently no evidence of such activities which might be directed against Germany.

This assessment, however, just represents a snapshot. There are still political and military imponderables as well as other factors which make it absolutely necessary to call attention to the risk of cyber-sabotage as a major challenge, which must be put on the security policy agenda.

In view of the immense damage such attacks could cause, we are going to heighten our awareness and alertness in this respect even more.

Besides, we must not forget that attacks on IT infrastructures of other countries might have an impact on Germany, too, due to the increasing degree of international networking in the field of IT systems.

BfV as Germany's domestic intelligence service is quite aware of its role as the early warning system in our society and takes it seriously. So one of our priorities is to be ahead of the attackers, to know their aims and their modi operandi, and to prevent – in co-operation with national and international security agencies – electronic attacks from happening or at least to diminish the effects of a serious act of sabotage.

Co-operation in the National Cyber Response Centre

The increase in electronic attacks involves increasing challenges to and requirements on the security agencies.

On 23 February 2011, the Federal Cabinet adopted the „Cyber Security Strategy for Germany“ developed by the Federal Ministry of the Interior. Its aim is to improve the security and safety of IT infrastructures as well as of information and communications technology in Germany.

A major component of this strategy is constituted by the National Cyber Response Centre (Cyber-Abwehrzentrum - Cyber-AZ) established in Bonn in April 2011. The agencies involved, including BfV, have been co-operating trustfully and efficiently within this centre for more than three years now, with the Federal Office for Information Security being the lead authority and each agency keeping its own responsibilities and regulations.

The aim of the Cyber-AZ is to optimise co-operation between state authorities in operational matters as well as to better coordinate security measures and countermeasures to be taken against potential cyber attacks.

The role of the Cyber-AZ is mainly that of a centre for the prompt and uncomplicated exchange of information between the agencies involved, allowing it to respond quickly and in a concerted manner to a cyber security incident. Especially in case of electronic attacks, where several security agencies are involved according to their respective responsibilities, close co-operation, particularly in terms of a daily exchange, is of utmost importance.

Conclusion

Due to the various threats posed by electronic attacks, not only the state authorities are required to take action to deal with this issue. We can only protect our community effectively if state and trade and industry jointly counter this increasing threat in close co-operation and in an environment of trust. Security agencies such as the BfV can give private enterprises advice in a discreet way and without any financial interests.

BfV's essential role in this context is to provide a precise assessment of the threats and risks posed by electronic attacks, to analyse and attribute attacks which have occurred and finally to make the results of these analyses available and usable for threat prevention by taking protective measures.

Only reliable information on the intensity of a threat and the attribution of activities to an originator allows a legal categorisation and thus the right (also consequential) political decision. We receive intelligence from various internal and external sources of information such as human sources, malware detection systems, communications intelligence and other sorts of intelligence information collection.

Only an overall view and assessment of all this information allow BfV and its partners to make precise and solid statements on actors, their targets and modi operandi.

Imprint

Publisher
Bundesamt für Verfassungsschutz
Public Relations Section
Merianstraße 100
50765 Köln
oeffentlichkeitsarbeit@bfv.bund.de
www.verfassungsschutz.de
Phone: +49 (0) 221/792-0
Fax: +49 (0) 221/792-2915

Layout and Printing
Bundesamt für Verfassungsschutz
Print and Media Centre

Photo Credits
© Production Pering - Fotolia.com
© pressmaster - Fotolia.com
© Nmedia - Fotolia.com
© VRD - Fotolia.com
© Konstantin Yolshin - Fotolia.com
© Login - Fotolia.com
© Victoria - Fotolia.com
© Sergey Nivens - Fotolia.com
© seen - Fotolia.com
© Claireliot - Fotolia.com
© industrieblick - Fotolia.com
© peshkova - Fotolia.com
© mmmx - Fotolia.com
© FotolEdhar - Fotolia.com

Date of Information
July 2014

For further information on the Bundesamt für Verfassungsschutz see:

www.verfassungsschutz.de