



Bundesministerium  
des Innern

# Cyber-Sicherheitsstrategie für Deutschland







# Inhalt

<b>Einleitung</b>	<b>2</b>
<b>IT-Gefährdungslage</b>	<b>3</b>
<b>Rahmenbedingungen</b>	<b>4</b>
<b>Leitlinie der Cyber-Sicherheitsstrategie</b>	<b>4</b>
<b>Strategische Ziele und Maßnahmen</b>	<b>6</b>
<b>Nachhaltige Umsetzung</b>	<b>13</b>
<b>Abkürzungen</b>	<b>14</b>
<b>Definitionen</b>	<b>14</b>

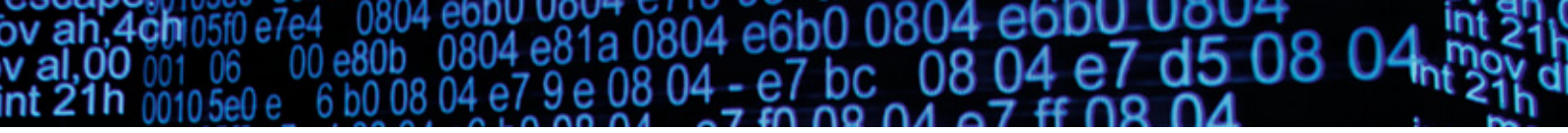


# Einleitung

Der Cyber-Raum umfasst alle durch das Internet über territoriale Grenzen hinweg weltweit erreichbaren Informationsinfrastrukturen. In Deutschland nutzen alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens die vom Cyber-Raum zur Verfügung gestellten Möglichkeiten. Staat, Kritische Infrastrukturen, Wirtschaft und Bevölkerung in Deutschland sind als Teil einer zunehmend vernetzten Welt auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen.

Fehlerbehaftete IT-Produkte und Komponenten, der Ausfall von Informationsinfrastrukturen oder schwerwiegende Angriffe im Cyber-Raum können zu erheblichen Beeinträchtigungen der technischen, wirtschaftlichen und administrativen Leistungsfähigkeit und damit der gesellschaftlichen Lebensgrundlagen Deutschlands führen. Die Verfügbarkeit des Cyber-Raums und die Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Daten sind zu einer existenziellen Frage des 21. Jahrhunderts geworden. Die Gewährleistung von





Cyber-Sicherheit wird damit zur zentralen gemeinsamen Herausforderung für Staat, Wirtschaft und Gesellschaft im nationalen und internationalen Kontext. Die Cyber-Sicherheitsstrategie wird die Rahmenbedingungen hierfür verbessern.

## IT-Gefährdungslage

Angriffe auf Informationsinfrastrukturen sind in den letzten Jahren immer zahlreicher und komplexer geworden; gleichzeitig ist eine zunehmende Professionalisierung zu verzeichnen. Ihren Ursprung haben Cyber-Angriffe sowohl im In- als auch im Ausland. Die Offenheit und Ausdehnung des Cyber-Raums erlauben es, verschleierte Angriffe durchzuführen und dabei verwundbare Opfersysteme als Werkzeug für Angriffe zu missbrauchen. Gegenüber technologisch hoch entwickelten Schadprogrammen sind die Abwehr- und Rückverfolgungsmöglichkeiten sehr begrenzt. Häufig kann bei Angriffen weder auf die Identität noch auf die Hintergründe des Angreifers geschlossen werden. Kriminelle, terroristische und nachrichtendienstliche Akteure nutzen den Cyber-Raum als Feld für ihr Handeln und machen vor Landesgrenzen nicht halt. Auch militärische Operationen können hinter solchen Angriffen stehen.

Der vor allem wirtschaftlich begründete Trend, Informationssysteme in industriellen Bereichen auf Basis von Standard-Komponenten zu entwickeln und zu betreiben sowie mit dem Cyber-Raum zu verbinden, führt zu neuen Verwundbarkeiten. Die Erfahrungen mit dem Schadprogramm Stuxnet zeigen, dass auch wichtige industrielle Infrastrukturbereiche von gezielten IT-Angriffen nicht mehr ausgenommen bleiben.

Aufgrund der zunehmenden Komplexität und Verwundbarkeit der Informationsinfrastrukturen ist auch zukünftig mit einer kritischen Cyber-Sicherheitslage zu rechnen. Von gezielt herbeigeführten oder auch zufällig eintretenden IT-Ausfällen sind Staat, Wirtschaft und Gesellschaft in Deutschland gleichermaßen betroffen.



# Rahmenbedingungen

Die Gewährleistung von Sicherheit im Cyber-Raum, die Durchsetzung von Recht und der Schutz der kritischen Informationsinfrastrukturen erfordern ein hohes Engagement des Staates im Innern wie im Zusammenschluss mit internationalen Partnern. Aufgrund der verteilten Verantwortung von Staat, Wirtschaft und Gesellschaft wird eine Cyber-Sicherheitsstrategie nur dann erfolgreich sein, wenn alle Akteure gemeinsam und partnerschaftlich ihre jeweilige Aufgabe wahrnehmen. Gleiches gilt im internationalen Kontext.

Durch die globale Vernetzung der IT-Systeme können sich Vorfälle in Informationsinfrastrukturen anderer Länder mittelbar auf Deutschland auswirken. Die Stärkung der Cyber-Sicherheit erfordert daher auch die Durchsetzung von internationalen Verhaltensregeln, Standards und Normen. Nur eine Mischung aus innen- und außenpolitischen Maßnahmen kann der Dimension der Problematik gerecht werden. Mehr Cyber-Sicherheit ist durch die Verbesserung der Rahmenbedingungen für die Ausarbeitung gemeinsamer Mindestregelungen (code of conduct) mit Verbündeten und Partnern zu erwarten. Zur Bekämpfung der rapide anwachsenden Kriminalität im Cyber-Raum ist eine enge Kooperation der Strafverfolgungsbehörden weltweit ein wesentlicher Eckpfeiler.

## Leitlinie der Cyber-Sicherheitsstrategie

Ziel der Bundesregierung ist es, einen signifikanten Beitrag für einen sicheren Cyber-Raum zu leisten. Dadurch sollen die wirtschaftliche und gesellschaftliche Prosperität für Deutschland bewahrt und gefördert werden. Die Cyber-Sicherheit in Deutschland ist auf einem der Bedeutung und der Schutzwürdigkeit der vernetzten Informationsinfrastrukturen angemessenen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen. Der Zustand eines sicheren Cyber-Raums ergibt sich dabei als Summe aller nationalen und internationalen Maßnahmen zum Schutz der Verfügbarkeit der Informations- und Kommunikationstechnik sowie der Integrität, Authentizität und Vertraulichkeit der sich darin befindenden Daten.



Cyber-Sicherheit kann nur in einem umfassenden Ansatz verfolgt werden. Dies erfordert die weitere Intensivierung des Informationsaustausches und der Koordinierung. Zivile Ansätze und Maßnahmen stehen bei der Cyber-Sicherheitsstrategie im Vordergrund. Sie werden ergänzt durch die Maßnahmen der Bundeswehr zum Schutz ihrer eigenen Handlungsfähigkeit und im Rahmen zugrunde liegender Mandate, um auf diese Weise Cyber-Sicherheit als Teil gesamtstaatlicher Sicherheitsvorsorge zu verankern. Aufgrund der Globalität der Informations- und Kommunikationstechnik ist eine internationale Abstimmung und geeignete Vernetzung unter außen- und sicherheitspolitischen Gesichtspunkten unverzichtbar. Hierzu gehört neben der Zusammenarbeit in den Vereinten Nationen auch die Zusammenarbeit in der EU, dem Europarat, in der NATO, im G8-Kreis, in der OSZE und anderen multinationalen Organisationen. Ziel ist es, Kohärenz und Handlungsfähigkeit der Staatengemeinschaft für den Schutz des Cyber-Raums zu erzielen.



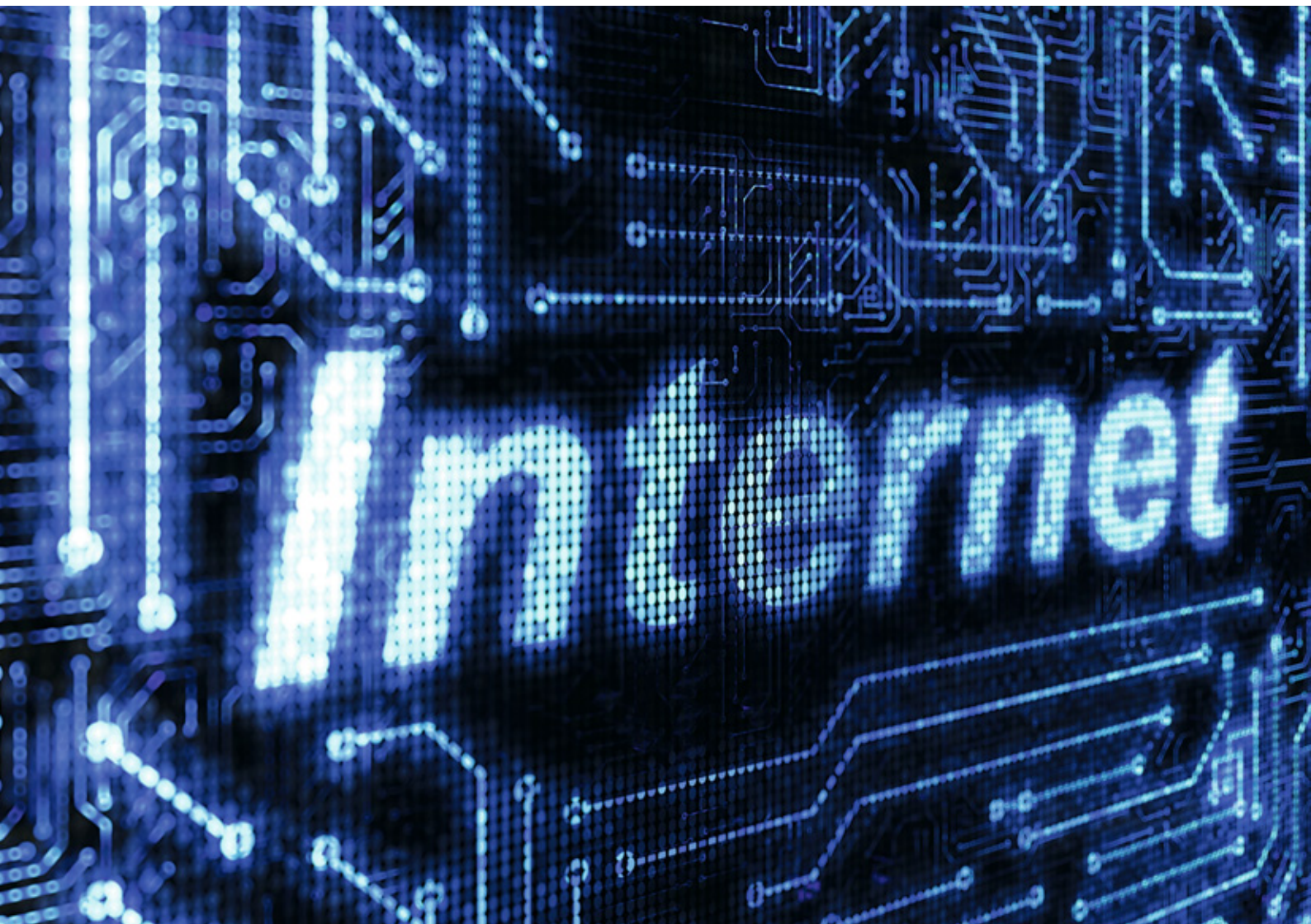


# Strategische Ziele und Maßnahmen

Mit der vorliegenden Cyber-Sicherheitsstrategie passt die Bundesregierung ihre Maßnahmen auf der Basis der mit den Umsetzungsplänen KRITIS und Bund bereits aufgebauten Strukturen an die Gefährdungslage an. Die Bundesregierung wird Maßnahmen in zehn strategischen Bereichen ergreifen:

## 1. Schutz kritischer Informationsinfrastrukturen

Im Kern der Cyber-Sicherheit steht der Schutz kritischer Informationsinfrastrukturen. Diese sind zentraler und in ihrer Bedeutung wachsender Bestandteil nahezu aller Kritischen Infrastrukturen. Staat und Wirtschaft müssen eine engere strategische und organisatorische Basis für eine stärkere Verzahnung auf der Grundlage eines intensiven Informationsaustausches schaffen. Hierzu wird die durch den „Umsetzungsplan KRITIS“ bestehende Zusammenarbeit systematisch








ausgebaut und werden gegebenenfalls rechtliche Verpflichtungen des Umsetzungsplans KRITIS geprüft. Unter Beteiligung des Nationalen Cyber-Sicherheitsrates (siehe Ziel 5) wird die Einbeziehung zusätzlicher Branchen geprüft und die Einführung neuer relevanter Technologien stärker berücksichtigt. Es ist weiterhin zu klären, ob und an welchen Stellen Schutzmaßnahmen vorgegeben werden müssen und ob und an welchen Stellen bei konkreten Bedrohungen zusätzliche Befugnisse erforderlich sind. Weiterhin werden wir die Notwendigkeit für eine Harmonisierung der Regelungen zur Aufrechterhaltung der Kritischen Infrastrukturen in IT-Krisen prüfen.

## **2. Sichere IT-Systeme in Deutschland**

Der Schutz der Infrastrukturen erfordert mehr Sicherheit auf den IT-Systemen der Bürgerinnen und Bürger sowie der kleinen und mittelständischen Unternehmen. Nutzer brauchen bedarfsgerechte und konsistente Informationen über Risiken im Umgang mit IT-Systemen und selbst zu ergreifende Sicherheitsmaßnahmen für ein sicherheitsbewusstes Verhalten im Cyber-Raum. Wir werden in gemeinsamen Initiativen mit gesellschaftlichen Gruppen für eine zielgerichtete Bündelung von Informations- und Beratungsangeboten sorgen. Darüber hinaus werden wir eine stärkere Verantwortung der Provider prüfen und darauf hinwirken, dass geeignete providerseitige Sicherheitsprodukte und -services für Nutzer als Basisangebote verfügbar sind. Wir wollen durch gezielte Anreize und Förderung staatlich zertifizierte Basissicherheitsfunktionen (z. B. elektronische Identitätsnachweise oder De-Mail) zur Massennutzung bringen. Um auch kleine und mittelständische Unternehmen bei dem sicheren Einsatz von IT-Systemen zu unterstützen, wird im Bundesministerium für Wirtschaft und Technologie unter Beteiligung der Wirtschaft eine Task Force „IT-Sicherheit in der Wirtschaft“ eingerichtet.

## **3. Stärkung der IT-Sicherheit in der öffentlichen Verwaltung**

Die öffentliche Verwaltung wird ihre IT-Systeme noch stärker schützen. Staatliche Stellen müssen Vorbild sein in Bezug auf Datensicherheit. Als Grundlage für die elektronische Sprach- und Datenkommunikation werden wir eine gemeinsame, einheitliche und sichere Netzinfrastruktur der Bundesverwaltung schaffen („Netze des Bundes“). Wir werden den für die Bundesverwaltung bestehenden



„Umsetzungsplan Bund“ mit Nachdruck weiter realisieren. Bei einer Verschärfung der IT-Sicherheitslage kommt auch eine Anpassung in Betracht. Wirksame IT-Sicherheit braucht starke Strukturen in allen Behörden der Bundesverwaltung; Ressourcen müssen deshalb angemessen zentral und dezentral eingesetzt werden. Zur Erleichterung der Umsetzung durch einheitliches Handeln der Behörden sollen gemeinsame IT-Sicherheitsinvestitionen des Bundes im Rahmen haushalterischer Möglichkeiten dauerhaft vorgesehen werden. Die operative Zusammenarbeit mit den Ländern, insbesondere im CERT-Bereich<sup>1</sup>, werden wir unter Verantwortung des IT-Planungsrates intensivieren.

#### **4. Nationales Cyber-Abwehrzentrum**

Zur Optimierung der operativen Zusammenarbeit aller staatlichen Stellen und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle richten wir ein Nationales Cyber-Abwehrzentrum ein. Es arbeitet unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und direkter Beteiligung des Bundesamtes für Verfassungsschutz (BfV) und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK). Die Zusammenarbeit im Nationalen Cyber-Abwehrzentrum erfolgt unter strikter Wahrung der gesetzlichen Aufgaben und Befugnisse aller mitwirkenden Stellen auf der Basis von Kooperationsvereinbarungen. Bundeskriminalamt (BKA), Bundespolizei (BPol), das Zollkriminalamt (ZKA), Bundesnachrichtendienst (BND), die Bundeswehr sowie die aufsichtsführenden Stellen über die Betreiber der Kritischen Infrastrukturen wirken ebenfalls unter Wahrung ihrer gesetzlichen Aufgaben und Befugnisse mit.

Ein schneller und enger Informationsaustausch über Schwachstellen in IT-Produkten, Verwundbarkeiten, Angriffsformen und Täterbilder befähigt das Nationale Cyber-Abwehrzentrum, IT-Vorfälle zu analysieren und abgestimmte Handlungsempfehlungen zu geben. Auch die Interessen der Wirtschaft, sich vor Kriminalität und Spionage im Cyber-Raum zu schützen, sollen angemessen berücksichtigt werden. Dabei sind die Verantwortlichkeiten zu wahren. Jeder mitwirkende Akteur leitet aus der gemeinsam erstellten nationalen Cyber-Sicherheitslage die von ihm zu ergreifenden Maßnahmen ab und stimmt diese mit den zuständigen Stellen und im Übrigen mit den Partnern aus der Wirtschaft und der Wissenschaft ab.

Da Sicherheitsvorsorge am wirksamsten durch Frühwarnung und präventives Handeln erreicht werden kann, wird das Cyber-Abwehrzentrum dem Nationalen

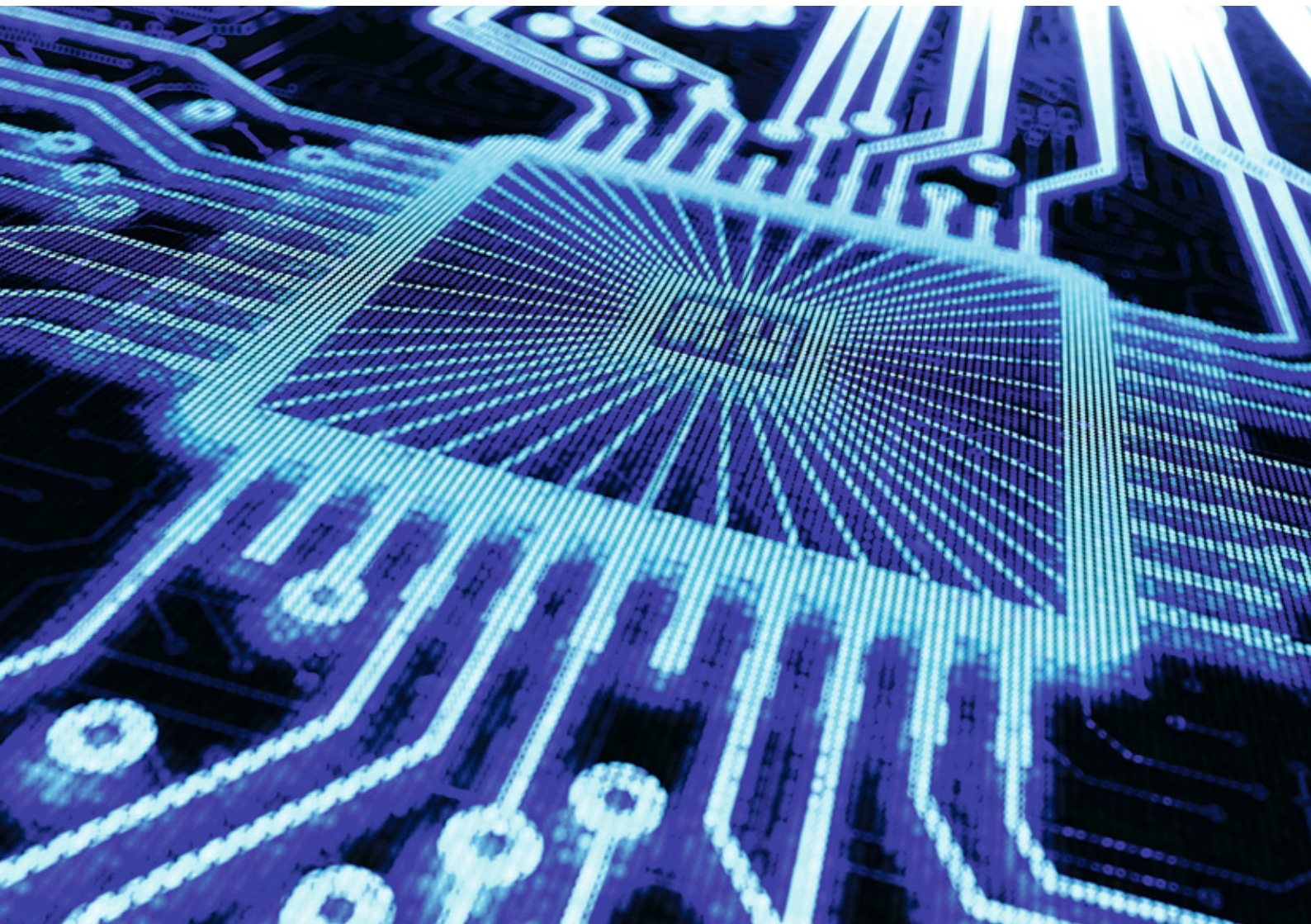
<sup>1</sup> CERT: Computer Emergency Response Team



Cyber-Sicherheitsrat regelmäßig und anlassbezogen entsprechende Empfehlungen vorlegen. Erreicht die Cyber-Sicherheitslage die Dimension einer unmittelbar bevorstehenden oder eingetretenen Krise, berichtet das Nationale Cyber-Abwehrzentrum unmittelbar an den vom Staatssekretär des Bundesministeriums des Innern geleiteten Krisenstab.

## **5. Nationaler Cyber-Sicherheitsrat**

Die Identifikation und Beseitigung struktureller Krisenursachen wird als ein wichtiger präventiver Schlüssel für Cyber-Sicherheit verstanden. Wir wollen daher die Zusammenarbeit innerhalb der Bundesregierung sowie zwischen Staat und Wirtschaft unter Verantwortung der Beauftragten der Bundesregierung für Informationstechnik sichtbarer organisieren und einen Nationalen Cyber-Sicherheitsrat ins Leben rufen. Vertreten sind das Bundeskanzleramt sowie, mit jeweils einem Staatssekretär, die Ressorts Auswärtiges Amt, Bundesministerium des Innern, Bundesministerium der Verteidigung, Bundesministerium für Wirtschaft und Technologie, Bundesministerium der Justiz, Bundesministerium der Finanzen, Bundesministerium für Bildung und Forschung sowie Vertreter der Länder.





Anlassbezogen wird der Kreis um weitere Ressorts erweitert. Wirtschaftsvertreter werden als assoziierte Mitglieder eingeladen. Vertreter der Wissenschaft werden bei Bedarf hinzugezogen. Der Nationale Cyber-Sicherheitsrat soll die präventiven Instrumente und die zwischen Staat und Wirtschaft übergreifenden Politikansätze für Cyber-Sicherheit koordinieren. Die Arbeit des Nationalen Cyber-Sicherheitsrates ergänzt und verzahnt die Aufgaben mit der IT-Steuerung Bund und dem IT-Planungsrat im Bereich der Cyber-Sicherheit auf einer politisch-strategischen Ebene.

## 6. Wirksame Kriminalitätsbekämpfung auch im Cyber-Raum

Die Fähigkeiten der Strafverfolgungsbehörden, des Bundesamtes für Sicherheit in der Informationstechnik und der Wirtschaft im Zusammenhang mit der Bekämpfung der IuK-Kriminalität, auch im Hinblick auf den Schutz vor Spionage und Sabotage, sind zu stärken. Um den Austausch von Know-how in diesem Bereich zu verbessern, streben wir gemeinsame Einrichtungen mit der Wirtschaft unter beratender Beteiligung der zuständigen Strafverfolgungsbehörden an. Projekte zur Förderung strukturschwacher Partnerländer dienen auch der Bekämpfung der Cyber-Kriminalität. Um den wachsenden Herausforderungen









## **8. Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie**

Die Verfügbarkeit verlässlicher IT-Systeme und -Komponenten muss dauerhaft sichergestellt werden. Die Entwicklung innovativer Schutzkonzepte für die verbesserte Sicherheit unter Berücksichtigung gesellschaftlicher und wirtschaftlicher Dimensionen wird vorangetrieben. Hierzu werden wir die relevante Forschung zur IT-Sicherheit und zum Schutz der Kritischen Infrastrukturen fortsetzen und ausbauen. Wir werden außerdem die technologische Souveränität und wissenschaftliche Kapazität Deutschlands über die gesamte Bandbreite strategischer IT-Kernkompetenzen stärken, in unsere politischen Strategien übernehmen und diese weiterentwickeln. Überall wo es sinnvoll ist, wollen wir unsere Kräfte mit denen unserer Partner und Verbündeten, insbesondere in Europa, bündeln. Wir setzen uns für technologische Pluralität ein. Unser Ziel ist es, in sicherheitskritischen Bereichen Komponenten einzusetzen, die sich einer Zertifizierung nach einem international anerkannten Zertifizierungsstandard unterzogen haben.

## **9. Personalentwicklung der Bundesbehörden**

Aufgrund der strategischen Bedeutung der Cyber-Sicherheit muss der Ausbau der personellen Kapazitäten der Behörden für Zwecke der Cyber-Sicherheit durch Priorisierung geprüft werden. Außerdem werden ein verstärkter Personalaustausch zwischen den Bundesbehörden und entsprechende Fortbildungsmaßnahmen die ressortübergreifende Zusammenarbeit stärken.

## **10. Instrumentarium zur Abwehr von Cyber-Angriffen**

Die Gewährleistung gesamtstaatlicher Sicherheitsvorsorge verpflichtet dazu, ein mit den zuständigen staatlichen Stellen abgestimmtes und vollständiges Instrumentarium für die Abwehr von Angriffen im Cyber-Raum zu schaffen. Wir werden weiterhin die Bedrohungslage regelmäßig prüfen und geeignete Schutzmaßnahmen ergreifen. Gegebenenfalls ist der Bedarf für die Schaffung von notwendigen weiteren gesetzlichen Befugnissen auf der Bundes- und der Landesebene zu evaluieren. Darüber hinaus gilt es, die vorstehend genannten Ziele, Mechanismen und Einrichtungen in einem stetigen Übungsprozess mit den beteiligten Stellen in Bund, Ländern und Wirtschaftsunternehmen zu verfestigen.



# Nachhaltige Umsetzung

Mit der Umsetzung der strategischen Ziele und Maßnahmen leistet die Bundesregierung einen Beitrag zur Gewährleistung der Sicherheit im Cyber-Raum und damit zu Freiheit und Wohlstand in Deutschland. Viel wird auch davon abhängen, wie es uns gelingt, auf internationaler Ebene effektive Maßnahmen zum Schutz des Cyber-Raums zu ergreifen.

Die genutzten Informationstechnologien unterliegen kurzen Innovationszyklen. Entsprechend wird sich die technische und gesellschaftliche Ausgestaltung des Cyber-Raums weiter verändern und neben neuen Perspektiven auch neue Risiken mit sich bringen. Die Bundesregierung wird daher die Erreichung der Ziele der Cyber-Sicherheitsstrategie unter Federführung des Nationalen Cyber-Sicherheitsrates in regelmäßigem Abstand überprüfen und die verfolgten Strategien und Maßnahmen den aktuellen Erfordernissen und Rahmenbedingungen anpassen.



# Abkürzungen

BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BND	Bundesnachrichtendienst
BPOL	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
ENISA	European Network and Information Security Agency
EU	Europäische Union
G8	Gruppe führender Industrienationen der Welt (Deutschland, USA, Japan, Vereinigtes Königreich, Kanada, Frankreich, Italien und Russische Föderation)
IT	Informationstechnik
IuK	Information und Kommunikation
KRITIS	Kritische Infrastrukturen
NATO	North Atlantic Treaty Organization
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
ZKA	Zollkriminalamt

# Definitionen


(Erläuterungen und Begriffsverständnis in diesem Dokument)

## Cyber-Raum

Der Cyber-Raum ist der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab. Dem Cyber-Raum liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann. IT-Systeme in einem isolierten virtuellen Raum sind kein Teil des Cyber-Raums.

## Cyber-Angriff, Cyber-Spionage, Cyber-Ausspähung und Cyber-Sabotage

Ein Cyber-Angriff ist ein IT-Angriff im Cyber-Raum, der sich gegen einen oder mehrere andere IT-Systeme richtet und zum Ziel hat, die IT-Sicherheit zu brechen. Die Ziele der IT-Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit können



dabei als Teil oder Ganzes verletzt sein. Cyber-Angriffe, die sich gegen die Vertraulichkeit eines IT-Systems richten, werden, wenn sie von fremden Nachrichtendiensten ausgehen oder gesteuert werden, als Cyber-Spionage, ansonsten als Cyber-Ausspähung bezeichnet. Cyber-Angriffe gegen die Integrität und Verfügbarkeit eines IT-Systems werden als Cyber-Sabotage bezeichnet.

### **Cyber-Sicherheit sowie zivile und militärische Cyber-Sicherheit**

(Globale) Cyber-Sicherheit ist der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des globalen Cyber-Raums auf ein tragbares Maß reduziert sind.

Cyber-Sicherheit in Deutschland ist demnach der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des deutschen Cyber-Raums auf ein tragbares Maß reduziert sind. Cyber-Sicherheit (in Deutschland) entsteht durch die Summe von geeigneten und angemessenen Maßnahmen.

Zivile Cyber-Sicherheit betrachtet die Menge der zivil genutzten IT-Systeme des deutschen Cyber-Raums. Militärische Cyber-Sicherheit betrachtet die Menge der militärisch genutzten IT-Systeme des deutschen Cyber-Raums.

### **Kritische Infrastrukturen**

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Auf Bundesebene gibt es dazu folgende Sektoreneinteilung:

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Staat und Verwaltung
- Medien und Kultur





Diese Broschüre wird im Rahmen der Öffentlichkeitsarbeit des Bundesministeriums des Innern kostenlos herausgegeben. Sie darf weder von Parteien noch von Wahlbewerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Europa-, Bundestags-, Landtags- und Kommunalwahlen. Missbräuchlich sind insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung. Unabhängig davon, wann, auf welchem Weg und in welcher Anzahl diese Schrift dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Bundesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte.

## **Impressum**

### **Herausgeber:**

Bundesministerium des Innern  
Alt-Moabit 101 D  
10559 Berlin

### **Redaktion:**

Referat IT 3

### **Gestaltung und Produktion:**

MEDIA CONSULTA Deutschland GmbH

### **Bildnachweis:**

iStockphoto, shutterstock

### **Druck:**

Silber Druck oHG, Niestetal

### **Stand:**

Februar 2011

[www.bmi.bund.de](http://www.bmi.bund.de)