Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

FRANZÖSISCHE NATIONALE STRATEGIE

FÜR DIE DIGITALE SICHERHEIT

Frankreich setzt sich voll und ganz für den digitalen Übergang ein. Der größte Teil seiner Bevölkerung hat eine Internetverbindung und seine digitale Wirtschaft ist stark im Wachstum begriffen. So verfügt das Land über Talente und Pluspunkte auf Augenhöhe mit der europäischen und weltweiten Innovation.

Aber auch Wettbewerb und Konfrontationen machen vor den digitalen Technologien nicht halt. Unlauterer Wettbewerb und Spionage, Fehlinformationen und Propaganda, Terrorismus und Kriminalität nutzen den Cyberspace, um sich auszudrücken.

Die von der Regierung angestrebte « digitale Republik der Taten » muss unsere Werte und unsere Wirtschaft fördern und die Bürger schützen. Das Engagement für die digitale Sicherheit fördert die Entwicklung eines Cyberspace, der für nachhaltiges Wachstum sorgt und ein Ort der Gelegenheiten für die französischen Unternehmen ist. Es bekräftigt unsere demokratischen Werte und schützt das digitale Leben und die persönlichen Daten der Franzosen.

Ich bringe meinen ganzen Ehrgeiz in diese Domäne ein. Die nationale Strategie für die digitale Sicherheit muss sich besonders die Schulung und die internationale Zusammenarbeit stützen. Sie muss von der ganzen nationalen Gemeinschaft getragen werden: der Regierung, den Behörden, den Gebietskörperschaften, den Unternehmen und von allen Landsleuten. Sie geht alle an.

Die Sicherheitsherausforderungen der digitalen Welt müssen angenommen werden, denn das ist ein Schlüsselfaktor für den gemeinsamen Erfolg. Ich möchte, dass diese nationale Strategie für die digitale Sicherheit eine Dynamik mit schützender und befreiender Energie in Gang setzt.

Manuel Valls
Premierminister

Höflichkeitsübersetzung des Vorworts von dem französischen Premierminister Manuel Valls zur Französischen Nationalen Strategie für die Digitale Sicherheit.

FRANZÖSISCHE NATIONALE STRATEGIE FÜR DIE DIGITALE SICHERHEIT

Die Digitalisierung der französischen Gesellschaft beschleunigt sich: der Anteil digitaler Technologien in Dienstleistungen, Dingen und Berufen verstärkt und ist ein nationales Interessen geworden. Dieser digitale Übergang bringt Innovationen und Wachstum mit sich, aber auch Risiken für den Staat, die Wirtschaftsakteure und die Bürger. Cyberkriminalität, Spionage, Propaganda, Sabotage oder übermäßige Nutzung persönlicher Daten bedrohen das Vertrauen und die Sicherheit der digitalen Technologien. Sie verlangen nach einer gemeinsamen und koordinierten Antwort mit fünf strategischen Zielen.

 # Grundlegende Interessen, Verteidigung und Sicherheit der IT-Systeme des Staates und der kritischen Infrastrukturen, große IT-Krise.

Durch die Entwicklung eines unabhängigen, strategischen Ansatzes, gestützt von hochwertigem technischen Fachwissen, kann Frankreich seine grundlegenden Interessen im Cyberspace von morgen verteidigen. Parallel dazu wird Frankreich die Verstärkung der Sicherheit seiner kritischen Netzwerke und seiner Belastbarkeit bei einem größeren Angriff fortfahren, indem es die Zusammenarbeit auf nationaler Ebene mit den privaten Akteuren und auf internationaler Ebene weiter ausbaut.

 # Digitales Vertrauen, Privatleben, persönliche Daten, Cyberverbrechen.

Damit der Cyberspace ein Raum des Vertrauens für Unternehmen aller Größen und Privatpersonen bleibt, werden Schutz- und Präventivmaßnahmen ergriffen. Dazu zählen erhöhte Wachsamkeit seitens der öffentlichen Stellen bei der Verwendung persönlicher Daten und die Entwicklung eines an die Öffentlichkeit angepassten Angebots digitaler Sicherheitsprodukte. Zur Prävention wird eine Anlaufstelle für Cyberverbrechensopfer eingerichtet werden, die technische und rechtliche Antworten auf solche Taten haben wird.

 # Bewusstmachung, Erstausbildungen, Fortbildungen.

Dem Einzelnen sind die Gefahren der Digitalisierung der Gesellschaft immer noch nicht hinreichend bewusst. Deshalb wird die Bewusstmachung bei Schülern und Studenten verstärkt. Außerdem wird die Schulung von Experten auf diesem Gebiet weiter ausgebaut, um dem wachsenden Bedarf der Unternehmen und Behörden nachzukommen.

 # Umfeld der Unternehmen der digitalen Technologien, Industriepolitik, Export und Internationalisierung.

Das internationale Wachstum der Märkte der digitalen Technologien und der entsprechenden Sicherheitsanforderungen stellt für die französischen Produkte und Dienstleistungen mit einem an die Verwendungen angepassten Sicherheitsniveau eine Gelegenheit dar, sich abzuheben. Durch die Unterstützung bei der Investition, bei der Innovation und beim Export, aber auch durch öffentliche Aufträge, wird der Staat ein günstiges Umfeld für die französischen Unternehmen der digitalen Technologien schaffen, die abgesicherte Produkte und Dienste anbieten.

 # Europa, digitale Souveränität, Stabilität des Cyberspace.

Die Regelung der Beziehungen im Cyberspace ist ein Hauptthema der internationalen Kontakte geworden. Frankreich wird zusammen mit den bereitwilligen Mitgliedsstaaten eine Roadmap für die digitale Souveränität Europas vorantreiben. Es wird auch seinen Einfluss in den internationalen Instanzen verstärken und die bereitwilligen, am wenigsten geschützten Länder beim Einrichten von Cybersicherheit-Kapazitäten unterstützen, um zur internationalen Stabilität des Cyberspace beizutragen.

Die Sicherheit der digitalen Technologien bestärkt das Projekt der digitalen Republik. Der Staat spielt dabei eine Hauptrolle, indem er diese Strategie ausarbeitet und eine Dynamik ins Leben ruft, die von den Profis der digitalen Technologien, den öffentlichen und privaten Entscheidungsträgern und den Bürgern unterstützt werden soll.

INDEX

EINFÜHRUNG

Frankreich vollzieht seinen Übergang zur Digitalisierung. Netzwerke sind im Staat, in der Wirtschaft und im Alltagsleben der Bürger allgegenwärtig.

Die digitalen Technologien sind ein Innovationsfaktor, denn sie sind Träger neuer Nutzungen, neuer Produkte und neuer Services. Sie führen zu einem Umbruch in den meisten Berufen. Sie transformieren Tätigkeitsbereiche und Unternehmen und machen sie flexibler und wettbewerbsfähiger. Diese Sektoren werden durch die digitalen Technologien zwar bereichert, gleichzeitig entstehen dabei aber auch neue Bedrohungen.

Die digitalen Technologien zu meiden oder keinen Zugang zu ihnen zu haben, führt zu einer Form der wirtschaftlichen und sozialen Ausgrenzung. Genauso droht einem Staat ohne die notwendige Selbstständigkeit im digitalen Sektor der Verlust seiner Souveränität.

Damit die digitalen Technologien ein Hort der Freiheit, des Austausches und des Wachstums bleiben, müssen Vertrauen und Sicherheit hergestellt und verteidigt werden. Dieses Ziel kann nur durch kollektive Anstrengungen erreicht werden.

* *
*

Anfang 2010 wurde die erste Strategie zur Cybersicherheit Frankreichs erarbeitet und Anfang 2011 veröffentlicht, kurz nach der Aufdeckung eines Hackerangriffs zwecks Spionage gegen das Wirtschafts- und das Finanzministerium. Die Hacker hatten mehrere Monate lang die Kontrolle über die Zentrale eines der Netzwerke des Ministeriums übernommen und sammelten regelmäßig politische, wirtschaftliche und finanzielle Informationen.

Diese Art von Hackerangriff zielt auf zahlreiche französische Unternehmen aller Größen in allen Tätigkeitsbereichen ab. Die Unternehmen sind auch das Ziel von Betrügereien aller Art, wie zum Beispiel die Infizierung durch Malware, welche die Dateien des Unternehmens unbrauchbar machen, bis über schwer nachverfolgbare Wege ein Lösegeld bezahlt wird.

Parallel dazu nehmen illegale Zugriffe zum Stehlen persönlicher Daten (Identität, Identifizierungsdaten für Online-Shops, Bankdaten) zu. Die Kriminellen begehen meistens die gleichen Delikte wie in der materiellen Welt — Diebstähle, Betrügereien, Erpressung — aber industrialisiert, und das Erkennungs- und Strafverfolgungsrisiko ist geringer. Das organisierte Verbrechen hat sich die Vorteile der elektronischen Kommunikationsnetzwerken zu eigen gemacht. Seine technischen Fähigkeiten sind so weit gediehen, dass es selbstständig oder durch Weitervergabe Sabotageakte begehen oder Produktionswerkzeuge als Geiseln nehmen kann.

In den sozialen Netzwerken entwickeln sich Belästigungskampagnen, wie z.B. betrügerische Appelle an die Gefühle, um gutgläubige Opfer zum Überweisen von Geld ins Ausland zu bewegen.

Die zahlreichen Entstellungen von Internetseiten, vor allem diejenigen von Gebietskörperschaften, nach den Attentaten vom Januar 2015, oder der Hackerangriff gegen ein französisches Medium mit internationaler Ausrichtung einige Wochen später haben den Willen und die Fähigkeit von organisierten Gruppen

gezeigt, IT-Ressourcen außer Gefecht zu setzen, die unser tägliches Leben unterstützen.

Was 2010 gemeinhin « der Bedrohungszustand » genannt wurde, hat sich so bewahrheitet. Die Bedrohung verschärft sich heute durch die raffinierter werdenden Methoden der Angreifer, der Verbreitung der Angriffstechniken und die Entwicklung des organisierten Verbrechens im Cyberspace.

Aber eine Herausforderung anderer Art auftrat. Die Erfassung der digitalen Reichtümer durch ein Oligopol von Unternehmen, die ihre dominante Position ausnutzen, um den Einstieg neuer Unternehmen zu verhindern und den Mehrwert einer entstehenden Wirtschaft abzuschöpfen. Diese nutzt die Daten, um neue Dienste zu erfinden, unser tägliches Leben zu verbessern oder die öffentlichen Dienstleistungen zugänglicher zu machen. Zu diesen Daten zählen in erster Linie unsere persönlichen Daten einschließlich der Daten über unser Privatleben. Die Kontrolle über diese Datenmassen öffnet die Tür zur wirtschaftlichen Destabilisierung und zu hochentwickelten Formen der Propaganda oder der Meinungsbildung von Menschen. In diesem Sinne ist diese Bedrohung wegen ihres nationalen Ausmaßes und ihrer strategischen Bedeutung Sache der nationalen Verteidigung und Sicherheit.

* *
*

Es wurde schon viel gegen diese leider erwiesenen Risiken erreicht.

Wie schon im Weißbuch zur Verteidigungs- und Sicherheitspolitik 2008 angekündigt, wurde 2009 ein nationales Amt geschaffen, um gegen Hackerangriffe vorzugehen und die Informationssysteme des Staates und kritischer Infrastrukturen zu schützen.

So fördern das Programm für zukünftige Investitionen und der Plan « Industrie der Zukunft » die inländischen Cybersicherheits-Industrie.

Das Parlament hat 2013 die von der Regierung vorgelegten Maßnahmen zur Verstärkung der IT-Sicherheit der Operatoren mit entscheidender Bedeutung und derjenigen, die an ihren kritischsten IT-Systemen beteiligt sind, verabschiedet.

Für die Positionen Frankreichs wird in allen internationalen Instanzen und vor allem bei den Vereinten Nationen (UNO) geworben, die 2013 die Anwendung internationalen Rechts auf den Cyberspace anerkannt haben. Darüber hinaus wurden funktionierende bilaterale Beziehungen zu mehreren Ländern aufgebaut.

Den Ministerien sind die politischen und technischen Auswirkungen der IT-Technologien auf ihre Aufträge und die Tätigkeit ihrer Verwaltung bewusst geworden, und sie sehen Koordinatoren vor, welche für die digitalen Technologien und deren Sicherheit zuständig sind. Es wurde eine Sicherheitspolitik der IT-Systeme des Staates erarbeitet, die progressiv umgesetzt wird.

In den kommenden Jahren müssen die Ergebnisse der Maßnahmen erfasst werden, um den Umfang der öffentlichen Aktionen und der beteiligten Akteure zu erweitern. Es muss sich ein Bewusstsein dafür entwickeln, dass die Verteidigung und die Sicherheit der digitalen Technologien eine Angelegenheit der nationalen Gemeinschaft ist, und der Staat nicht allein handeln kann.

* *
*

Noch bis vor wenigen Jahren hingen unsere nationale Verteidigung und Sicherheit von den Erfahrungen, dem Verhalten und den Entscheidungen derjenigen Menschen ab, die Zugang zu den hochentwickelsten, am besten geschützten und geheimsten Installationen und Ausrüstungen haben. Indem eine massiv vernetzte Gesellschaft entsteht, wird diese Verantwortung zum Teil auch vom ganzen französischen Volk getragen. Ein Online-Gerät oder ein von seinen Entwicklern unzureichend abgesicherter Dienst, die Nachlässigkeit eines Entscheidungsträgers bei der Sicherheit von IT-Systemen, das gefährliche Verhalten eines Dienstleisters oder ein Mitarbeiter, der Privat- und Berufsleben unvorsichtig miteinander vermischt: all dies kann

zu Verlusten in der Verfügbarkeit, der Vertraulichkeit oder der Integrität von wesentlichen Informationen, zu Tätigkeitsunterbrechungen und wirtschaftlichen Einbußen, Industrieunfällen und Toten oder Umweltkatastrophen und Störungen der öffentlichen Ordnung führen, welche sich auf das Leben im Land auswirken können.

Nie zuvor hing die von den digitalen Technologien getragene Stabilität unserer Zukunft so sehr von der Verantwortung jedes einzelnen und von der kollektiven Verantwortung der drei Akteurgemeinschaften ab.

Die erste dieser Gemeinschaften ist verantwortlich für die Einführung von Technologien, Produkten und Dienstleistungen mit ausreichendem Sicherheitsniveau, um die erkannten Risiken abzuwehren. Die wichtigsten Akteure dieser Gemeinschaft sind Forscher, Erfinder von Produkten und Dienstleistungen sowie deren Integratoren, d.h. die Unternehmen auf dem Sektor der Cybersicherheit, die Betreiber von elektronischen Kommunikationsnetzwerken, die Anbieter von Internetzugängen sowie die Anbieter von Remote IT-Dienstleistungen.

Die zweite Gemeinschaft ist verantwortlich für den Schutz der Nation vor den Raubtieren der digitalen Technologien. Sie muss nicht nur eine Cybersicherheitspolitik umsetzen, sondern auch zielstrebig eine Politik zur Entwicklung der notwendigen technischen Kompetenzen vorantreiben und ein Ökosystem des gegenseitigen Vertrauens schaffen, welche den digitalen Wandel der Gesellschaft begleitet und die Bürger, unsere Werte und unsere Interessen im Cyberspace verteidigt. Aufgrund dieser Verantwortlichkeit muss sich diese Gemeinschaft für qualifizierte Sicherheitslösungen aussprechen und die nationale Industrie auch beim Export fördern. Diese Gemeinschaft besteht aus Abgeordneten, der Regierung, den nationalen und regionalen Behörden sowie den Gewerkschaften.

Die dritte Gemeinschaft ist dafür verantwortlich, die verfügbaren Dienste und Technologien überlegt zu nutzen, eine vernünftige Wahl zu treffen und risikovolle Verhaltensweisen im digitalen Alltag zu vermeiden. Diese Gemeinschaft besteht aus allen Nutzern, Akteuren der Zivilgesellschaft und Bürgern.

Dank dieser gegenseitigen Verpflichtungen der Akteure kann Frankreich den Beitrag der digitalen Technologien vollständig nutzen und die Herausforderungen der digitalen Sicherheit, die allzu häufig nur als Einschränkung für die Wirtschaft und Verhaltenweisen empfunden werden, in einen nationalen Wettbewerbsvorteil verwandeln, um unsere Werte, unsere Produkte und unsere Dienstleistungen zu fördern.

Der Staat muss im Cyberspace die Meinungs- und Handlungsfreiheit Frankreichs garantieren und die Sicherheit seiner kritischen Infrastrukturen im Falle eines größeren Hackerangriffs gewährleisten (Ziel 1), das digitale Leben der Bürger und Unternehmen schützen, die Cyberkriminalität bekämpfen (Ziel 2), das Bewusstsein für die digitale Sicherheit wecken und Schulungen in diese Richtung gewährleisten (Ziel 3), die Entwicklung eines Ökosystems begünstigen, das Vertrauen in die digitalen Technologien schafft (Ziel 4) und die Zusammenarbeit zwischen den Mitgliedsstaaten der EU fördern, damit eine digitale Souveränität Europas entsteht, als langfristiger Garant für einen sichereren Cyberspace, der unsere Werte achtet (Ziel 5).

FÜNF STRATEGISCHE ZIELE

1

#GRUNDLEGENDE INTERESSEN, VERTEIDIGUNG UND SICHERHEIT DER IT-SYSTEME DES STAATES UND DER KRITISCHEN INFRASTRUKTUREN, GROSSE IT-KRISE

HERAUSFORDERUNGEN

Frankreich ist Ziel von Hackerangriffen, die sich gegen seine grundlegenden Interessen richten.

Wenn ein Hacker heute auf den Staat, Operatoren mit wesentlicher Bedeutung oder strategische Unternehmen abzielt, versucht er, sich dauerhaft im angegriffenen IT-System einzunisten, um vertrauliche (politische, diplomatische, militärische, technologische, wirtschaftliche, finanzielle oder gewerbliche) Daten zu stehlen. Morgen könnte ein Hacker die Kontrolle über Online-Geräte übernehmen, ferngesteuert eine industrielle Tätigkeit unterbrechen oder sein Ziel zerstören. Seit 2011 wurden rund hundert bedeutende Hackerangriffe von Behörden und kompetenten Dienstleistern meistens vertraulich abgewehrt.

Parallel dazu versuchen Hackerangriffe, die öffentliche Meinung zu beeinflussen, wenn Frankreich auf internationaler Ebene Position bezieht, Militäroperationen durchführt oder öffentliche Debatten anstößt. Die Entstellungen von Internetseiten nach den Attentaten in Frankreich am Anfang 2015 haben zum Beispiel geringe technische Auswirkungen gehabt, aber die von den Hackern gewünschte symbolische Aufmerksamkeit bekommen. Der Hackerangriff, der ein französisches Medium mit internationaler Ausrichtung lahmlegte, wollte ebenfalls die Öffentlichkeit schockieren und die Radikalisierung fördern, welche zu Terrorakten führt. Dieser Angriff hat auch gezeigt, dass entschlossene Hacker den Betrieb einer Infrastruktur mit großem symbolischen Wert stören können.

Seit mehreren Jahren haben mehrere Staaten mit politischem Willen und erheblichen menschlichen, technischen und finanziellen Mitteln groß angelegte IT-Operationen im Cyberspace gegen uns durchgeführt.

Sie werden häufig durch veröffentlichte Dokumente oder beim Abwehren von Hackerangriffen entlarvt. Das Übermaß solcher Praktiken ziehen die Glaubwürdigkeit einiger dieser Staaten in der internationalen Szene in Leidenschaft und ruinieren das Vertrauen, das normalerweise in die Produkte und digitalen Dienstleistungen ihrer Unternehmen gesetzt würde.

« Das Übermaß solcher Praktiken ziehen die Glaubwürdigkeit einiger dieser Staaten in der internationalen Szene in Leidenschaft und ruinieren das Vertrauen, das normalerweise in die Produkte und digitalen Dienstleistungen ihrer Unternehmen gesetzt würde. »

So hat das Cyber-Risiko, das vom Weißbuch zur Verteidigungs- und Sicherheitspolitik 2013 auf den dritten Platz der größten Bedrohungen für Frankreich gesetzt wurde, heute zugenommen und stellt eine der großen Herausforderungen für Frankreich dar.

ZIEL

Frankreich wird sich die Mittel geben, um seine grundlegenden Interessen im Cyberspace zu verteidigen. Es wird die digitale Sicherheit seiner kritischen Infrastrukturen konsolidieren und sich für die digitale Sicherheit seiner wesentlichen Wirtschaftsteilnehmer einsetzen.

AUSRICHTUNGEN

> **Über die notwendigen wissenschaftlichen, technischen und industriellen Fähigkeiten für den Schutz der Information unser Souveränität, für die Cybersicherheit und für die Entwicklung einer vertrauenswürdigen digitalen Wirtschaft verfügen.**

Unter der Federführung des Staatssekretariats für digitale Technologien und der nationalen Sicherheitsbehörde für IT-Systeme wird eine Expertengruppe für das digitale Vertrauen gebildet.

Die Expertengruppe für das digitale Vertrauen wird

sehr regelmäßig die zuständigen Behörden des Premierministers, der Ministerien für nationale Bildung, für Hochschulbildung, für Forschung, für Verteidigung, für Soziales, für Gesundheit und die Rechte der Frau, für Inneres, für Wirtschaft, für Industrie und digitale Technologien, das Generalkommissariat für Investitionen, die nationale Forschungsagentur und die betreffenden Forschungseinrichtungen zusammenführen. Die Gruppe kann Akteure des privaten Sektors und qualifizierte Personen in seine Arbeiten einbinden.

Als Hauptaufgabe muss diese Gruppe herausfinden, welche Schlüsseltechnologien für die Berufe der Cybersicherheit und darüber hinaus für die Entwicklung eines vertrauenswürdigen digitalen Umfelds angewendet werden müssen. Sie wird den Bedarf an Erstausbildungen und Fortbildungen bewerten, an der Verbesserung der Unterstützung für Promovierte mitarbeiten, die Forschungsarbeiten verfolgen und deren Umsetzung begleiten. Im Bereich der digitalen Technologien wird Sie zur Definition der strategischen Leitlinien für die Finanzierung und Unterstützung der Forschungsarbeiten und der industriellen Entwicklung beitragen. Diese Arbeiten decken sich mit den bereits eingerichteten Strukturen wie z.B. dem Fachausschuss der Sicherheitsindustrien (comité de filière des industries de sécurité - CoFIS) sein.

Allgemein gesagt kann die Wahl von großen privaten Akteuren als Wirtschafts- oder Technologiemodell, manchmal außerhalb jeglichen Normierungsrahmens, oder die Wahl bestimmter Innovationen beim Gebrauch der digitalen Technologien das Vertrauen konsolidieren oder Misstrauen auslösen. Die Expertengruppe für das digitale Vertrauen wird die technologische und wirtschaftliche Mitverfolgung organisieren, um Weiterentwicklungen vorherzusehen. Gegebenenfalls werden angemessene Maßnahmen vorgeschlagen, um diese Weiterentwicklungen zu unterstützen oder zu lenken. Diese Maßnahmen können zum Beispiel den Schutz des wissenschaftlichen und technischen Potenzials der Nation oder die Kontrolle ausländischer Investitionen in kritische nationale Unternehmen betreffen.

Die ministeriellen Koordinatoren für Cyberspace-Fragen werden in einem Ausschuss der Expertengruppe mit dem Generalsekretär für Verteidigung und nationale Sicherheit zusammentreffen, wenn es um Themen geht, die in seinen Zuständigkeitsbereich fallen.

Diese Expertengruppe wird dem Premierminister jährlich über ihre Aktivitäten Bericht erstatten.

> Die Sicherheitbeobachtung der Technologien und der Nutzungen zugunsten des Staates, der Unternehmen und der Bürger aktiv mitverfolgen.

In Anbetracht bevorstehender, größerer, technologischer Entwicklungen wie zum Beispiel der 5. Mobilfunkgeneration oder den « Software-definierten Netzwerken » behält Frankreich die Art und die Leistungen der Hardware und Software in seinen Kommunikationsnetzwerken genau im Auge, um die Vertraulichkeit des Schriftverkehrs, des Privatlebens seiner Bürger und die Belastbarkeit dieser Infrastrukturen zu schützen, und wird die Anpassung seines Rechtsrahmens an die neuen Technologien fortsetzen.

Die Nationale Sicherheitsbehörde für IT-Systeme wird die Ministerien, Unternehmen, Gebietskörperschaften und Bürger mit Mitteln, die an das jeweilige Zielpublikum angepasst sind, über Elemente informieren, die eine Gefahr bei ihrer Nutzung der digitalen Technologien darstellen können. Diese Informationen werden vorher mit den zuständigen Behörden konsolidiert.

> Die Sicherheit der IT-Systeme des Staates schneller verstärken.

Seit 2010 gab es mehrere Aktionen, um das Sicherheitsniveau der IT-Systeme des Staates zu steigern. Es wurde eine Sicherheitspolitik der IT-Systeme des Staates (politique de sécurité des systèmes d'information de l'État - PSSIE) erarbeitet, das interministerielle elektronische Kommunikationsnetzwerk expandiert und die Einführung abgesicherter tragbarer Endgeräte hat begonnen. Diese Maßnahmen benötigen genauso wie die Maßnahmen zum Erzeugen von Sicherheitsausrüstungen für den Schutz der Souveränitätsinformation menschliche und finanzielle Ressourcen. Sie werden fortgesetzt, um den Entscheidungen der Regierung und unseren militärischen Fähigkeiten ein angemessenes Sicherheitsniveau zu bieten, welches die Entscheidungs- und Handlungsautonomie Frankreichs langfristig aufre-

chterhält.

Die Anwendung der Sicherheitspolitik der IT-Systeme des Staates und die Wirksamkeit der ergriffenen Maßnahmen werden jährlich bewertet. Jedes Ministerium übermittelt dem Premierminister eine vertrauliche Jahresbilanz, und das Parlament wird mit Hilfe von Indikatoren informiert.

Mit demselben Ziel, das Parlament zu informieren, werden die Gesetzentwürfe in ihrer Wirkungsanalyse ab 2016 einen Abschnitt über die digitalen Technologien und innerhalb dieses Abschnitts einen über die Cybersicherheit enthalten.

> Frankreich und die multilateralen Organisationen, deren Mitglied es ist, darauf vorbereiten, einer großen IT-Krise standzuhalten.

Wie im Weißbuch zur Verteidigungs- und Sicherheitspolitik 2013 angekündigt, wurden gesetzliche Maßnahmen zur Verstärkung der Sicherheit der vertraulichsten IT-Systeme der Operatoren mit entscheidender Bedeutung ergriffen (Artikel 21 und 22 des Gesetzes Nr. 2013-1168 vom 18. Dezember 2013). Die mit diesen Operatoren begonnenen Arbeiten werden vor allem durch die regelmäßige Aktualisierung der Gesetzestexte nachhaltig fortgesetzt. Diese Arbeiten werden gemäß dem Gesetz progressiv auf die öffentlichen oder privaten Operatoren ausgeweitet, die an diesen vertraulichen IT-Systemen beteiligt sind.

Frankreich konnte durch diese Entscheidung aktiv an der Ausarbeitung der Ausrichtungen der europäischen Richtlinie über die Sicherheit von IT-Systemen der kritischen Infrastrukturen der Mitgliedsländer der Union teilnehmen und ihre Umsetzung vorhersehen. Im richtigen Augenblick wird Frankreich in Übereinstimmung mit den Ausrichtungen der Richtlinie seine wesentlichen Wirtschaftsteilnehmer definieren und an den europäischen Initiativen zur Verstärkung der digitalen Sicherheit teilnehmen.

Die auf nationaler Ebene durchgeführten Übungen zur Verwaltung von Cyber-Krisen werden mit der Zeit das ganze Land und alle Tätigkeitsbereiche mit entscheidender Bedeutung betreffen. Das Verteidigungsministerium wird in Zusammenarbeit mit der nationalen Sicherheitsbehörde für IT-Systeme eine einsatzbereite Cyberverteidigungs-Reserve einrichten, um einer größeren IT-Krise zu entgegnen.

Parallel dazu trägt Frankreich weiterhin zum Aufbau eines freiwilligen gemeinsamen Cyber-Krisenverwaltungsprogramms auf europäischer Ebene bei. Dabei werden insbesondere die Arbeiten der europäischen Agentur ENISA unterstützt.

Das CERT-EU der Europäischen Union (EU) und das NCIRC des nordatlantischen Verteidigungsbündnisses (NATO) sind für die Cyberverteidigung ihrer jeweiligen Institutionen zuständig. Frankreich leistet seinen Beitrag zu diesen Institutionen und ihren Mitgliedsstaaten unter Beachtung der Zuständigkeiten der anderen, indem es sich an Cyberkrisen-Übungen dieser Organisationen beteiligt und indem es stark in den Instanzen vertreten ist, welche die Entscheidungen der EU und der NATO hinsichtlich der abgesicherten digitalen Technologien lenken.

Frankreich trägt in politischer und technischer Hinsicht auch zur Cybersicherheit anderer internationaler Organisationen bei, deren Mitglied es ist. Dies gilt vor allem für diejenigen mit Sitz in Frankreich, die das nationale, technische Ökosystem nutzen.

> Eine autonome, mit unseren Werten vereinbare Denkweise entwickeln.

Durch die strategischen Entscheidungen Frankreichs nach dem zweiten Weltkrieg entstanden eine autonome strategische Denkweise und eine Doktrin, die Frankreich einen einzigartigen Platz auf der internationalen Bühne verschafft hat. Sie beeinflusst noch heute seine Diplomatie und die Einsatzkonzepte seiner Streitkräfte.

Sicher verändern die digitalen Technologien unsere Gesellschaften tiefgründig. Ihre Auswirkungen auf andere Realitäten, Konzepte oder Vorstellungen wie z.B. auf die Souveränität, das Staatsgebiet, die Währung oder grundsätzliche Interessen der Nation müssen jedoch erst noch gemessen, und die Organisation und die Mittel der öffentlichen Aktionen zur Anwendung bzw. zum Schutz des Gesetzes überdacht werden. Unter der Leitung des Generalsekretärs für Verteidigung und nationale Sicherheit werden Überlegungen zur Ausarbeitung eines geistigen Werks zum Cyberspace angestellt.

2

#DIGITALES VERTRAUEN, PRIVATLEBEN, PERSÖNLICHE DATEN, CYBERVERBRECHEN

ENJEUX

Die Franzosen haben zwar im allgemeinen Vertrauen in die digitalen Technologien, misstrauen aber deren Auswirkungen auf ihr tägliches, vor allem ihr persönliches, Leben. Einerseits sorgen sie sich um die Nutzung und Aufbewahrung ihrer persönlichen Daten, andererseits vertrauen sie sie jedoch Plattformen an, deren Nutzungsbedingungen auf Kosten der Benutzer gehen können.

Die Vorgehensweise bei einigen Hackerangriffen auf Unternehmen oder Behörden zeigt ebenfalls, wie schwer Privat- und Berufsleben bei der Nutzung von Geräten und Dienstleistungen voneinander zu trennen sind.

Bei Hackerangriffen auf Privatpersonen geht es meistens um finanzielle Bereicherung. Die Bauernfängerei wird im großen Maßstab von immer besser organisierten Verbrechern mit immer wirksameren Methoden betrieben: Die Kontrolle über ein benutztes persönliches Gerät — Computer, Tablet, Smartphone — übernehmen, Identitätsdiebstahl, die Zugangsdaten von Bankkonten oder Online-Shops stehlen, eine virtuelle Liebesbeziehung beginnen, um die Überweisung von Geld zu fordern, die Daten einer ahnungslosen Person verschlüsseln und dann ein Lösegeld verlangen usw.

Wenn es auch keine spezielle Hackertechnik anwendet, so ist das durch die elektronischen Kommunikationsnetzwerke erleichterte und verstärkte Mobbing doch ein Cyberangriff auf Personen, der manchmal dramatisch ausgehen kann.

Bei schweren IT-Zwischenfällen, welche Behörden oder Operatoren mit entscheidender Bedeutung betreffen, ist die nationale Sicherheitsbehörde für IT-Systeme klar und eindeutig der staatliche Ansprechpartner. Das öffentliche Angebot ist jedoch schwerer auszumachen, wenn es um die Unterstützung von Cyberverbrechensopfern geht. Diese können kleinere und mittlere Unternehmen, Freiberufler, Gebietskörperschaften oder Privatpersonen sein.

Die Opfer von Cyberverbrechen werden empfohlen, bei der Polizei Anzeige zu erstatten. Sie hat sich auf die Bearbeitung solcher Streitsachen eingestellt. In diesem Rahmen geht es jedoch in erster Linie um die Identifizierung der mutmaßlichen Täter des Cyberverbrechens und die strafrechtliche Verfolgung dieser Täter. Die Opfer müssen sich an einen Unterstützungsdienst für die Bearbeitung des IT-Ereignisses wenden können, das zu dem Cyberverbrechen geführt hat.

Die sozialen Netzwerke und Plattformen bilden schleichend Meinungen und übermitteln Werte, die manchmal nicht diejenigen der französischen Republik sind. In einigen Fällen, können sie für Fehlinformationen und Propagandazwecke gegenüber den französischen Bürgern instrumentalisiert werden. In einigen Fällen richten sich die Meinungen gegen unsere grundsätzlichen Interessen und stellen einen strafbaren Angriff auf die Verteidigung oder die nationale Sicherheit dar.

Darüber hinaus begünstigen die neuesten und gleichzeitigen Entwicklungen neuer Nutzungen und neuer Techniken zur Datenspeicherung und -verarbeitung das Risiko eines wirtschaftlichen Ungleichgewichts und eines Angriffs auf die individuelle Sicherheit von Personen und Staaten. Zwar ist ein freier Datenverkehr einschließlich der Erfassung persönlicher Daten über Online-Geräte, der zum Beispiel durch einen Handelsvertrag geregelt wird, wünschenswert. Jedoch haben es Oligopole auf diese Daten abgesehen, deren Werte und Praktiken weder dem französischen noch dem europäischen Konzept des Privatlebens noch deren rechtlichem Rahmen entspricht. Die massive und unrechtmäßige Erfassung bestimmter persönlicher Datenarten, wie z.B.

« Die sozialen Netzwerke und Plattformen bilden schleichend Meinungen und übermitteln Werte, die manchmal nicht diejenigen der französischen Republik sind. »

« Die digitale Entwicklung kann in einem Cyberspace nicht nachhaltig sein, in dem Staaten nicht die richtigen Verhaltensweisen für einen ausgewogenen und für alle Nationen vorteilhaften digitalen Übergang einhalten »

der Gesundheitsdaten, kann in der Tat zu Angriffen auf die individuelle und kollektive Sicherheit oder einfacher zu einer missbräuchlichen kommerziellen Nutzung führen (Weiterverkauf an Versicherungsgesellschaften, zum Beispiel).

Die digitale Entwicklung kann in einem Cyberspace nicht nachhaltig sein, in dem Staaten nicht die richtigen Verhaltensweisen für einen ausgewogenen und für alle Nationen vorteilhaften digitalen Übergang einhalten und in dem einige Wirtschaftsakteure den ganzen digitalen Datenreichtum, vor allem persönliche Daten, d.h. Ressourcen für zukünftige Generationen, in Beschlag nehmen.

ZIEL

Frankreich wird eine Nutzung des Cyberspace in Übereinstimmung mit seinen Werten entwickeln und dort das digitale Leben seiner Bürger schützen. Es wird seinen Kampf gegen die Cyberkriminalität und die Unterstützung von Cyberverbrechensopfern verstärken.

AUSRICHTUNGEN

> Unsere Werte in den elektronischen Kommunikationsnetzwerken und in den internationalen Instanzen fördern und verteidigen.

Die Menschenrechte gelten sowohl « online » als auch « offline » . Deshalb muss der Cyberspace ein Ort der freien Meinungsäußerung für alle Bürger bleiben, wo Missbräuchen nur innerhalb der gesetzlich festgesetzten Grenzen und in Übereinstimmung mit unseren internationalen Verpflichtungen vorgebeugt werden kann. Frankreich fördert diesen Ansatz, der einen freien und offenen Cyberspace in den internationalen Instanzen erhalten soll.

Es obliegt dem Staat, die Bürger über die Manipulationsrisiken und Propagandatechniken Krimineller im Internet zu informieren. Nach den Attentaten in Frankreich im Januar 2015 hat die Regierung eine Informationsplattform zu den Risiken der islamistischen Radikalisierung über die elektronischen Kommunikationsnetzwerke eingerichtet. « Stop-djihadisme.gouv.fr ». Dieser Ansatz könnte auf andere Propaganda- oder Destabilisierungsphänomene ausgeweitet werden. Es obliegt den für Verteidigung und Sicherheit zuständigen Diensten, diese Phänomene zu erkennen und der Regierung die Anwendung dieser Mittel zu empfehlen.

> Den Opfern von Cyberverbrechen vor Ort Unterstützung gewähren.

Das Innenministerium und die nationale Sicherheitsbehörde für IT-Systeme werden 2016 mit der Unterstützung der Ministerien für Justiz, für Haushalt und öffentliche Finanzen, für Verteidigung, für Wirtschaft, für Industrie und für digitale Technologien eine nationale Anlaufstelle für Cyberverbrechensopfer einrichten.

Aufgabe dieser Anlaufstelle wird es auch sein, die Wichtigkeit des Schutzes des digitalen Privatlebens und der Vorbeugung bewusst zu machen. Diese Aufgabe soll lokal durch die Präfekturen und die Dienste des Staates unterstützt werden. An diesem Auftrag werden sich das territoriale Netz der ANSSI, regionale Delegierte mit wirtschaftlichen Kompetenzen und die für Wirtschaftssicherheit zuständigen Dienste des Innenministeriums, das Netzwerk « digitaler Übergang » und das Netzwerk der Banque de France teilnehmen. Letztere könnte in ihre Unternehmensbewertungen bald das Cyber-Risiko als Kriterium aufnehmen. Die Industrie- und Handelskammern, die Handwerkskammern und alle beruflichen Netzwerke im weiteren Sinne werden ebenfalls beteiligt sein.

Die Rechtsform und Organisation der Anlaufstelle

wird die Unterstützung der Wirtschaftsakteure des Cybersicherheit-Sektors ermöglichen — Softwarehersteller, digitale Plattformen, Anbieter von Lösungen. Dank der eingesetzten Technologien soll die Anlaufstelle den Opfern technische Lösungen mit Akteuren vor Ort anbieten und die Behördengänge vor allem was die Anzeigenerstattung angeht vereinfachen.

> Die Cyberkriminalität messen.

Die seit 2013 laufenden interministeriellen Arbeiten auf Initiative des Innenministeriums haben zu der Feststellung geführt, dass es bisher keine zuverlässigen Statistiken speziell zur IT-Kriminalität gibt, da die meisten dieser Straftaten unter einem anderen Namen registriert wurden, der dieser bisher in den Regelwerken fehlenden Dimension keine Rechnung trägt.

Weil solche Statistiken fehlen, können die öffentlichen Stellen keine angemessenen politischen Strategien und Mittel umsetzen. Deshalb wird das Innenministerium neue Verfolgungstools für die Entwicklung der Cyberkriminalität einführen, um die öffentlichen Maßnahmen zu klären. Die nationale Beobachtungsstelle für Kriminalität und strafrechtliches Vorgehen wird ebenfalls dazu beitragen, indem sie einen Teil ihrer Arbeiten der statistischen Untersuchung der Cyberkriminalität widmen wird. Dieser in Zusammenarbeit mit der nationalen Sicherheitsbehörde für IT-Systeme und der Anlaufstelle für Cyberverbrechensopfer entworfene Teil wird die Daten enthalten, über die die Beobachtungsstelle verfügt.

> Das digitale Leben, das Privatleben und die persönlichen Daten der Franzosen schützen.

Anhand der europäischen Bestimmungen zur elektronischen Identität (eIDAS) stattet sich Frankreich mit einer Roadmap aus, die zur vom Staat ausgestellten digitalen Identität klare Angaben macht. Diese Roadmap wird vor Ende 2015 unter der Federführung des Innenministeriums und der für digitale Technologien und die Reform des Staates zuständigen Staatssekretariate mit Unterstützung der Dienste des Premierministers ausgearbeitet. Sie wird einen territorialen Teil umfassen, der einen Referenzrahmen für die Verwendung der digitalen Identität durch die Körperschaften definiert.

Diese Roadmap wird die digitale Strategie der Regierung berücksichtigen, welche die Einführung von

Vorrichtungen für die Identitätszusammenlegung vorsieht, um dieselbe digitale Identität zur Authentifizierung in verschiedenen Diensten benutzen zu können. Dank dieser Vorrichtungen kann ein Dritter, der die Identitätszusammenlegung verwaltet, feststellen, ob die von verschiedenen Stellen ausgegebenen digitalen Identitäten einer bestimmten Identitätszusammenlegung vertrauenswürdig sind.

Vorbehaltlich der Einhaltung der angemessenen Sicherheitsanforderungen für die Nutzungen und Bedrohungen, verstärken diese Vorrichtungen das Vertrauen der Nutzer in ihr digitales Leben, denn sie verbessern den Informationsfluss und schränken gleichzeitig das Risiko einer ungewünschten Nutzung ihrer persönlichen Daten ein. Für vertraulichere Nutzungen wie z.B. solche, die das demokratische Leben betreffen, oder der internationale Austausch rechtlicher Informationen, werden systematisch hohe Vertrauensniveaus in den Vorrichtungen und Diensten angewendet. Diese erhöhten Vertrauensniveaus werden sich auf die vorhandenen nationalen industriellen Strukturen und Sicherheitszertifizierungs-Schemata stützen.

Frankreich wird das Privatleben und die persönlichen Daten seiner Staatsangehörigen schützen. Auf das Recht auf Privatleben und die individuelle und kollektive Kontrolle über die persönlichen Daten wird immer wenn notwendig bestanden. Dies gilt besonders bei bilateralen und multilateralen Handelsverhandlungen zwischen Staaten.

Um die Franzosen über die Verwendungsweise der Daten durch die digitalen Dienste zu informieren, wird im Laufe des Jahres 2016 eine angemessene Kennzeichnung eingeführt und mit den dazu gewillten Staaten geteilt. Diese Kennzeichnung wird mit den europäischen Arbeiten übereinstimmen, die im Rahmen der europäischen Verordnung zum Schutz der persönlichen Daten durchgeführt werden. Sie zeigt die wesentlichen Merkmale der Verwendungsbedingungen der digitalen Plattformen und Dienste oder der Zahlungsmittel.

> Für alle Unternehmen und die Öffentlichkeit zugängliche technische Lösungen zum Absichern des digitalen Lebens vorschlagen.

Die staatlichen Stellen werden Sicherungslösungen für persönliche Endgeräte kennzeichnen. Diese Kennzeichnung wird mit der oben genannten abgestimmt, damit die Benutzer über eventuelle Informationsübertragungen an einen Dritten im Rahmen dieses Schutzes informiert werden. Nach ihrer Schaffung wird die oben genannte Anlaufstelle für Cyberverbrechensopfer diese Kennzeichnungen im Rahmen ihres Vorbeugungsauftrags bei den betroffenen Publikumskreisen bekannt machen.

Darüber hinaus wird das zugängliche und angemessene Lösungsangebot zur Sicherung des digitalen Lebens kleinerer und mittlerer Unternehmen unterstützt, sofern dies durch das Investitionsprogramm in die Zukunft begonnen werden konnte.

Die Entwicklungen französischer Lösungen werden genauso unterstützt wie Freeware-Communities, die Sicherheitslösungen entwickeln.

> Die bereits bestehende gegenseitige internationale Rechtshilfe verstärken und die Grundlagen der Budapester Konvention zur Bekämpfung der Cyberkriminalität universell verbreiten.

Die 2001 im Europarat verabschiedete Budapester Konvention ist ein Referenzwerk für die Zusammenarbeit von Staaten auf allen fünf Kontinenten im Kampf gegen die Cyberkriminalität geworden. Dieses von 46 Staaten, einschließlich 7 Nichtmitgliedern des Europarats, ratifizierte Werk wird schon auf die eine oder andere Weise von 125 Staaten anerkannt (Unterzeichner; zur Mitgliedschaft eingeladene Staaten; Staaten, die wegen der Aussicht auf zukünftige Mitgliedschaft technische Hilfe erhalten; Staaten, die internes Recht an das Modell der Konvention angepasst haben).

Es ist heute sehr wichtig, sowohl das Normengerüst als auch die Zusammenarbeit, die in diesem Text festgelegt werden, universell zu verbreiten und zu konsolidieren.

Darüber hinaus wird Frankreich in der Europäischen Union für die Definition einer vereinfachten justiziellen Zusammenarbeit zwischen den Mitgliedsstaaten werben, um die Datenübertragung zu beschleunigen und illegale Aktivitäten auszumerzen.

3

#BEWUSSTMACHUNG, ERSTAUSBILDUNGEN, FORTBILDUNGEN

HERAUSFORDERUNGEN

Frankreich ist im Vergleich zu seinen Partnern in Verzug, was die Bewusstmachung der Bevölkerung für die Gefahren bei der Nutzung der digitalen Technologien und die Cybersicherheit-Ausbildung angeht.

Die Franzosen vernachlässigen im Allgemeinen die richtigen Verhaltensweisen bei der Verwendung der elektronischen Kommunikationsnetzwerke.

Bei der privaten Nutzung der elektronischen Kommunikationsnetzwerke sind Kinder und Jugendliche die ersten Opfer, wenn sie mit unangemessenen Inhalten konfrontiert und Mobbing oder Ködern ausgesetzt werden. Um das Schweigen zu brechen und die Strafverfolgung aufnehmen zu können, müsste den Jüngsten gelehrt werden, wie sie sich zu verhalten haben, wenn sie Opfer von Cyberverbrechen werden.

Diese Bewusstmachung aller ist die unbedingte Voraussetzung, damit Abgeordnete und Leiter von Verwaltungen oder Unternehmen das « Cyberrisiko » angemessen einschätzen können. So können sie Maßnahmen beschließen, um die Bürger, die sie vertreten, oder die Organisationen, die sie leiten, vor Diebstahl von Informationen oder geistigem Eigentum, Angriffe auf persönliche Daten oder sogar vor Aktivitätsausfällen und Produktionsunfällen mit den entsprechenden Folgen für Technologie und Umwelt zu schützen.

Aber nicht nur die Bewusstmachung der Jüngsten ist wichtig, sondern auch die Ausbildung in den Berufen der digitalen Technologien, damit die zukünftigen Fachleute dieses Bereichs gut in der Sicherheit der IT-Systeme unterrichtet werden, denn dies fehlt bisher in vielen höheren Berufsausbildungen.

Außerdem gibt es nicht genug Erstausbildungen und Fortbildungen für die Cybersicherheitsberufe, um die Nachfrage der Unternehmen und Verwaltungen zu decken.

ZIEL

Schon in der Schule wird in Frankreich auf die digitale Sicherheit und verantwortliche Verhaltensweisen im Cyberspace aufmerksam gemacht. Die höheren Erstausbildungen und Fortbildungen werden einen Teil enthalten, der sich der digitalen Sicherheit des entsprechenden Fachbereichs widmet.

AUSRICHTUNGEN

> **Bewusstmachung bei allen Franzosen.**

Ein ehrgeiziges Programm der Bewusstmachung bei allen Franzosen muss begonnen werden.

Unter der Leitung des nationalen Ministeriums für Bildung, Hochschulwesen und Forschung sowie des Staatssekretariats für digitale Technologien, mit der Unterstützung des Informationsdienstes der Regierung und der nationalen Sicherheitsbehörde für IT-Systeme wird ein Aufruf zur Interessenbekundung für die Erstellung von Bewusstmachungsinhalten für die Öffentlichkeit gestartet.

Das Innenministerium setzt die Operation « Internetführerschein » fort, die 2014 von der Gendarmerie nationale in Partnerschaft mit einer privaten Stiftung begonnen und Anfang 2015 von der Police nationale übernommen wurde. Diese Operation macht auf die

Risiken aufmerksam und berät jedes Jahr mehr als 300.000 Schülern der CM2, um sie bei ihrer Internetnavigation zu schützen.

Verbände werden aufgefordert, Kommunikationskampagnen-Projekte auszuarbeiten, die das Vertrauen in die digitalen Technologien verstärken sollen und in den Rahmen einer « großen nationalen Sache » passen.

> Die Bewusstmachung der Cybersicherheit in alle höheren Berufsausbildungen und Fortbildungen integrieren.

Das nationale Ministerium für Bildung, Hochschulwesen und Forschung wird sich zusammen mit der Universitätspräsidentenkonferenz, der Hochschulkonferenz und den zuständigen Behörden ab dem Schulbeginn 2016 dafür einsetzen, dass Bewusstmachungen der Cybersicherheit in allen höheren Erstausbildungen an die Fachrichtung angepasst eingeführt werden.

Das Ministerium für Arbeit, Berufsausbildung und sozialen Dialog wird unterstützt durch die für Cybersicherheit zuständigen, staatlichen Behörden die notwendigen Beratungen aufnehmen, damit die Fortbildungsinstitute ab 2016 eine an die Ausbildung angepasste Bewusstmachung der Cybersicherheitsfragen in ihre Lehrpläne aufnehmen.

Schließlich werden diejenigen Berufskategorien, bei denen die Cybersicherheit wegen ihrer sozialen Verantwortung eine besonders wichtige Rolle spielt, unter der Leitung des für digitale Technologien zuständigen Staatssekretariats zusammen mit den betroffenen Ministerien und der Unterstützung der ANSSI auf diese Fragen aufmerksam gemacht. Diese Kategorien werden vom strategischen Ausschuss für das digitale Vertrauen angegeben.

> Die Cybersicherheits-Ausbildung in alle höheren Berufsausbildungen integrieren, die einen IT-Teil haben.

Die 2013 ins Leben gerufene Initiative « Cyber-Edu » hat bestätigt, dass die Hochschullehrkräfte für IT-Berufe ein Interesse an dem Thema Sicherheit in IT-Systemen haben. Diese Initiative muss gestärkt werden.

Das nationale Ministerium für Bildung, Hochschulwesen und Forschung wird zusammen mit der Universitätspräsidentenkonferenz, der Hochschulkonferenz und den zuständigen Behörden und Berufsorganisationen ab dem Schulbeginn 2016 dafür sorgen, dass eine an die Fachrichtung angepasste Ausbildung zur Sicherheit in IT-Systemen in allen höheren Erstausbildungen, in denen digitale Themen vorkommen, erteilt wird. Es muss prioritär versucht werden, diese Sicherheitselemente in die existierenden Kurse einzubauen und passend in den größeren Kontext jeder unterrichteten Spezialität zu integrieren. Im Rahmen des CyberÉdu-Projekts können sich diese Schritte in enger Zusammenarbeit mit dem Lehrkörper nützlicherweise auf pädagogische Inhalte stützen, die gerade ausgearbeitet werden.

Das Ministerium für Dezentralisierung und öffentlichen Dienst bemüht sich darum, dass in den Ausbildungen für führende Positionen im öffentlichen Dienst auch auf die Cybersicherheit aufmerksam gemacht wird. Zusammen mit dem Innenministerium wird es darauf achten, dass die Auswahlverfahren für IT- und Kommunikations-Ingenieure gemäß Verordnung Nr. 2015-576 vom 27. Mai 2015 sowie deren Ausbildungen einen Cybersicherheitsteil umfassen.

Angesichts der zunehmenden Nachfrage durch unsere Partner sollte ein Teil des Ausbildungs- und Bewusstmachungsangebots im Bereich des Möglichen an ein internationales Publikum angepasst werden, indem Programme auf Englisch angeboten werden.

> Den Bedarf an Erstausbildungen und Fortbildungen erfassen und vorhersehen.

Unter der Federführung der Expertengruppe für das digitale Vertrauen wird der kurz-, lang- und mittelfristige Bedarf an Erstausbildungen in Zusammenarbeit mit alle betroffenen Akteuren der Verwaltung und des privaten Sektors erstellt.

Die Berufsverbände werden an den Bedarf der Mitarbeiter und Unternehmen angepasste Fortbildungen ausarbeiten und umsetzen.

4

#UMFELD DER UNTERNEHMEN DER DIGITALEN TECHNOLOGIEN, INDUSTRIEPOLITIK, EXPORT UND INTERNATIONALISIERUNG

HERAUSFORDERUNGEN

Der Cyberspace entwickelt sich rasch. Jede Stunde verbinden sich 100.000 neue Objekte mit dem Internet. Die Präsenz vieler französischer Unternehmen auf internationalen Messen und der Erfolg der Initiative « French Tech » zeigen, wie dynamisch die französische Innovation bei Produkten und digitalen Dienstleistungen ist. Diese Wirklichkeit darf jedoch nicht über einen gewissen Kontrollverlust und eine technologische Abhängigkeit hinwegtäuschen.

Die großen Ausrüstungen, mit denen die in Frankreich gelegenen Infrastrukturen elektronischer Kommunikationsnetzwerke betrieben werden, werden häufig außerhalb Europas entworfen, entwickelt und verwaltet. Dasselbe gilt für die wesentlichen Kommunikations- und IT-Sicherheitsausrüstungen unserer Operatoren mit entscheidender Bedeutung. Der Betrieb von immer mehr Unternehmen beruht auf Anwendungen und Datenverarbeitungen, die in unkontrollierten, immateriellen Räumen gehostet und von physischen Infrastrukturen getragen werden, welche sich außerhalb des Landes befinden und nicht dem europäischen Recht unterliegen.

Die allgemeine Entwicklung geht dahin, dass sich dieser Kontrollverlust über den nationalen Cyberspace in technologischer und wirtschaftlicher Hinsicht noch verstärkt, zum Beispiel durch die Zunahme der verbundenen Objekte oder die Konzentration der Online-Dienstleistungsplattformen auf einige wenige Akteure. Im Krisenfall könnte uns der Zugriff auf große Teile des Cyberspace verwehrt werden.

Um auf diese Gefahr für die Souveränität antworten zu können, muss die nationale und europäische Industrie auf dem Spezialgebiet der Cybersicherheitsprodukte und -dienstleistungen stark und wettbewerbsfähig bleiben. Weiterhin muss in Frankreich und Europa ein Angebot an digitalen Ausrüstungen und Dienstleistungen entwickelt werden, das den Kunden angemessene Sicherheits- und Vertrauensgarantien für die Herausforderungen und Nutzungen bietet.

« Die Entwicklung eines abgesicherten Produkt- und Dienstleistungsangebots durch die nationalen Unternehmen des digitalen Sektors muss auch als wesentlicher Wettbewerbsfaktor für diese Unternehmen gesehen werden. »

Die Nutzer haben nicht die Mittel, um die Sicherheit digitaler Objekte und Dienstleistungen selbst zu gewährleisten. Die Förderung der Sicherheit wird in der Werbung immer mehr angepriesen, ohne dass das tatsächlich erreichte Sicherheitsniveau objektiv bewertet werden kann. Eine größere Nachvollziehbarkeit der Sicherheit des digitalen Angebots anhand objektiver und von einem Dritten überprüfbarer Elemente ist eine der großen Herausforderungen, um das Vertrauen in die digitale Wirtschaft zu gewährleisten.

Die Entwicklung eines abgesicherten Produkt- und Dienstleistungsangebots durch die nationalen Unternehmen des digitalen Sektors muss auch als wesentlicher Wettbewerbsfaktor für diese Unternehmen gesehen werden. Der Bereich der Zahlungsmittel (Kreditkarten, Zahlungsterminals usw.) ist der Archetyp eines Wirtschaftssektors, in dem ein an die Bedrohung angepasstes und durch einen Dritten überprüfbares Sicherheitsniveau ein wesentliches Verkaufsargument darstellt. Mehrere nationale Unternehmen verfügen auf diesem Sektor über eine weltweit wettbewerbsfähige Position, die ihrem hervorragenden Fachwissen bei der Entwicklung von Sicherheitslösungen zu verdanken ist.

Die Zunahme der Cyberbedrohungen und das immer größere Bewusstsein für die Ernsthaftigkeit dieser Bedrohungen werden in einigen Jahren dazu führen, dass die Sicherheit ein wesentliches Verkaufskriterium in vielen weiteren Sektoren werden wird. Ein sofortiges Handeln zum Verbessern der Sicherheit und der Transparenz des nationalen Angebots an digitalen Lösungen bereitet auch ihre zukünftige Wettbewerbsfähigkeit vor.

2015 liegt der Anteil der französischen Unternehmen, und vor allem der kleinen und mittle-

ren Betriebe, die sich im großen Maße der digitalen Technologien bedienen, nur im Mittelfeld der europäischen Länder. Das Aufholen dieses Verzugs muss von einer besseren Absicherung des digitalen Lebens der Unternehmen und in erster Linie einer besseren Sicherheit ihrer IT-Systeme begleitet werden. Dasselbe gilt für unsere Wettbewerbsfähigkeit und unsere Arbeitsplätze.

Die Herausforderung der französischen Unternehmen besteht darin, Produktivität, Einsparungen, Rentabilität und Verwendung oder Entwicklung von digitalen Produkten und Dienstleistungen mit ihrer eigenen Sicherheit, der Sicherheit ihrer Partner und der Sicherheit ihrer Kunden zu vereinbaren.

Die meisten heute am Markt verfügbaren, digitalen Ausrüstungen, Objekte und Dienstleistungen sind nicht genügend abgesichert, um einen Zwischenfall wie z.B. Datenverluste, Funktionsstörungen oder Dienstausfälle zu verhindern. Für die französischen Unternehmen müssen die Ergonomie, der Schutz der persönlichen Daten und das Sicherheitsniveau der von ihnen entwickelten digitalen Produkte und Dienstleistungen kurzfristig ein Differenzierungsmerkmal und ein Wettbewerbsvorteil werden, von dem die Nation profitieren kann.

Wenn Fälschungen zwar nicht direkt für die Sicherheit von IT-Systemen relevant sind, können gefälschte IT-Sicherheitsprodukte die Aktivität derjenigen Organisationen gefährden, die sie erwerben.

Angesichts einer erbitterten internationalen Konkurrenz, wo unsere Partner ihre Industrie systematisch unterstützen, müssen sich die staatlichen Dienststellen dauerhaft organisieren, um die französischen Cybersicherheit-Unternehmen bei ihrer Internationalisierung und ihrem Export zu unterstützen.

Die Mobilisierung und die Koordination aller verfügbaren öffentlichen und privaten Ressourcen ist wesentlich, um die internationale Sichtbarkeit und Wettbewerbsfähigkeit des französischen Angebots zu steigern, das Wissen und das Feedback gemeinsam zu nutzen und so das Teilen von Informationen zwischen den Akteuren des Fachbereichs zu begünstigen.

« Für die französischen Unternehmen müssen die Ergonomie, der Schutz der persönlichen Daten und das Sicherheitsniveau der von ihnen entwickelten digitalen Produkte und Dienstleistungen kurzfristig ein Differenzierungsmerkmal und ein Wettbewerbsvorteil werden, von dem die Nation profitieren kann. »

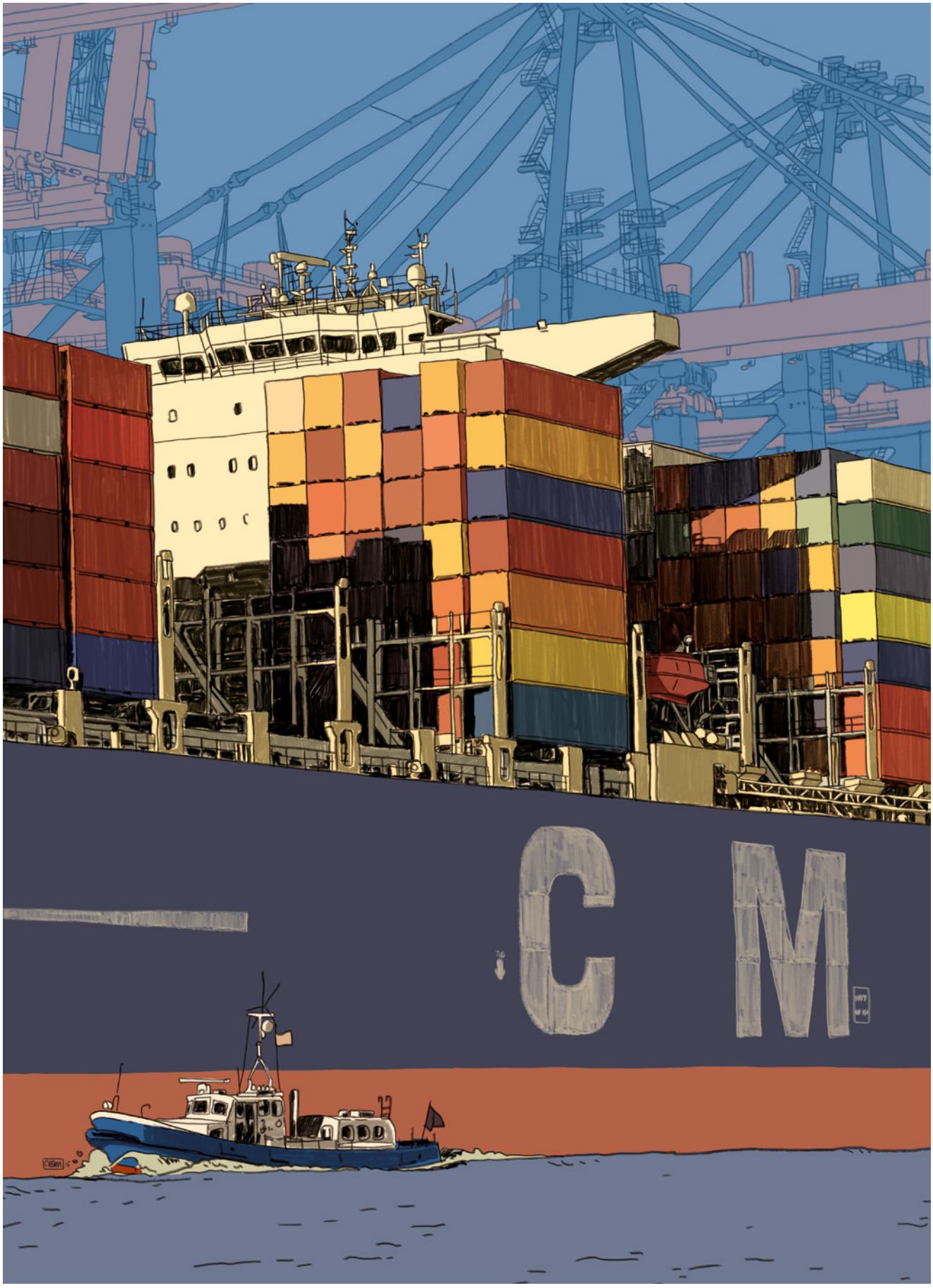
ZIEL

Frankreich wird ein günstiges Ökosystem für die Forschung und die Innovation schaffen und die digitale Sicherheit in einen Wettbewerbsfaktor verwandeln. Es wird die Entwicklung der Wirtschaft und der internationalen Förderung seiner digitalen Produkte und Dienstleistungen begleiten. Es wird gewährleisten, dass seinen Bürgern, seinen Unternehmen und seinen Behörden digitale Produkte und Dienstleistungen zur Verfügung stehen, deren Ergonomie, Vertrauen und Sicherheit an die Nutzungen und Cyberbedrohungen angepasst ist.

AUSRICHTUNGEN

> **Das nationale und europäische Angebot an Sicherheitsprodukten und -dienstleistungen entwickeln und aufwerten.**

Zusammen mit den zuständigen Behörden des Ministeriums für Wirtschaft, Industrie und digitale Tech-


C M

nologien und des Verteidigungsministeriums hat die nationale Sicherheitsbehörde für IT-Systeme 2012 eine Industriepolitik zum Ausbau der nationalen Strukturen derjenigen Unternehmen begonnen, die Produkte und Dienstleistungen für die IT-Sicherheit entwickeln.

Der Fachbereich konnte durch die Einführung des « Cybersicherheit »-Plans 2013 im Rahmen des Reindustrialisierungsprojekts « Nouvelle France industrielle », der jetzt in die Lösung « digitales Vertrauen » aufgenommen wurde, und durch die Unterstützung des Generalkommissariats für Investitionen und von BpiFrance besser organisiert werden. Dadurch konnten auch Projektausschreibungen zum Erstellen von Vertrauensausrüstungen für die Erkennung von Hackerangriffen gegen Operatoren mit entscheidender Bedeutung und von abgesicherten, mobilen Produkten für alle Unternehmen stattfinden.

Die staatlichen Dienststellen werden die Qualifizierung und Nachverfolgung von Produkten und Dienstleistungen der IT-Sicherheit sowie die Entwicklung neuer Sicherheitsprodukte, welche der Weiterentwicklung der Nutzungen gerecht werden, verstärken. Sie werden auch die Aufwertung und Dauerhaftigkeit dieser Angebote durch einen öffentlichen Auftrag unterstützen, der gut qualifizierte Sicherheitsprodukte und -dienstleistungen bevorzugt, sowie durch Kommunikations- und Bewusstmachungsaktionen an die Adresse des privaten Sektors.

Darüber hinaus werden die staatlichen Dienststellen die Ergebnisse der Forschungs- und Entwicklungsarbeiten verbreiten, die für Ausrüstungen mit hohem Sicherheitsniveau finanziert wurden, um die Sicherheit der Produkte für die Unternehmen und die Öffentlichkeit zu steigern.

Schließlich wird Frankreich die von der Europäischen Union gebotenen Hebel vollständig nutzen, um die wissenschaftlichen, technologischen und industriellen Kompetenzen Frankreichs in den Bereichen der Cybersicherheit zu unterstützen, zu fördern und zu verteidigen. Es wird die EU darüber hinaus ermutigen, sich nicht auf die Rolle des Verbrauchers zu beschränken, sondern sich als unumgänglicher globaler Akteur des Angebots in diesem Sektor durchzusetzen.

> Das erworbene Know-How auf den privaten Sektor übertragen, damit er für seine IT-Sicherheit sorgen kann.

Frankreich kann seit fünf Jahren Hackerangriffe erkennen und bearbeiten, so wie es das Weißbuch zur Verteidigungs- und Sicherheitspolitik von 2008 angekündigt hat. Wenn diese Bemühungen vor allem seitens der ANSSI auch fortgesetzt werden müssen, so obliegt es doch dem privaten Sektor, seine eigene Sicherheit im IT-Bereich genauso wie in anderen Bereichen zu gewährleisten, sodass der Staat nur bei schweren Krisen einschreiten muss.

Unterstützt durch den Wissenstransfer von den Behörden auf den privaten Sektor sollte die Kennzeichnung von kompetenten und vertrauenswürdigen Dienstleistern dafür sorgen, die unvermeidliche Zunahme von Hackerangriffen auf die Unternehmen zu erkennen und zu bearbeiten.

> Durch eine bessere Voraussage der Nutzungen und eine angemessene Begleitung eine sicherere digitale Welt vorbereiten.

Für die nächsten fünf Jahre muss die Priorität der für die Sicherheit der IT-Systeme zuständigen Behörden die Voraussage und die Vorbeugung sein.

Es muss erreicht werden, dass die in Frankreich entworfenen, entwickelten und produzierten digitalen Produkte und Dienstleistungen oder solche, die digitale Technologien integrieren, zu den sichersten auf der Welt zählen. Zum Erreichen dieses Zieles müssen die zuständigen Behörden ihre Kommunikationsbemühungen auf die wissenschaftliche, öffentliche und private Gemeinschaft und auf Innovationsorte wie z.B. Wettbewerbscluster, technologische Forschungsinstitute, Gründerzentren, « Fab Labs » richten und ihnen nach Bedarf spezielle Mittel zur Verfügung zu stellen, wie dies im Verteidigungsministerium und seit neuestem im Innenministerium der Fall ist.

Wenn digitale Produkte und Dienstleistungen persönliche Daten hosten oder für Tätigkeitsbereiche mit entscheidender Bedeutung bestimmt sind, tragen die staatlichen Dienststellen die Elemente für die Risikoanalyse oder die Ratschläge bei, um das Sicherheits-

niveau zu erreichen, das der Nutzung des Produktes oder der Dienstleistung während des Entwurfes oder der Entwicklung entspricht. Bei Nutzungen, die dies rechtfertigen, tragen sie auch zum Einrichten von Vorrichtungen ein, mit denen das Sicherheits- und Vertrauensniveau dieser Produkte und Dienstleistungen unabhängig bewertet werden kann und ihren potenziellen Benutzern über eine Kennzeichnung angemessene Garantien geboten werden können.

Parallel dazu muss der rechtliche Rahmen für diese neuen Produkte und Dienstleistungen vorhergesehen werden. Zum Beispiel muss der Gesetzgeber angesichts der baldigen Einführung von selbstfahrenden Fahrzeugen die Bedingungen für ihre sichere Verkehrsteilnahme vorbereiten. Die Cybersicherheit muss in den internationalen Arbeitsgruppen berücksichtigt werden, die das Regelwerk und die technischen Kontrollverfahren definieren.

Für andere Produkt- oder Dienstleistungsarten muss eine angemessene Kennzeichnung den Verbraucher über ihre wesentlichen digitalen Merkmale und insbesondere über die Verarbeitung der erfassten Daten informieren. Für bestimmte Sektoren, wie z.B. dem Gesundheitssektor, wird eine systematische Kennzeichnung der digitalen Produkte und Dienstleistungen untersucht.

Frankreich wird versuchen, weitere Mitgliedsstaaten der Europäischen Union an der Umsetzung dieser Praktiken zu beteiligen, um eine digitale Vertrauens- und Sicherheitszone zu schaffen. Die mit Deutschland begonnenen Arbeiten zum Cloud Computing und zum gesicherten E-Mail-Austausch gehen in diese Richtung.

> Die Anforderung der Cybersicherheit in öffentliche Aufträge und Unterstützungen integrieren.

Zum Schutz seiner Souveränität und vor allem zum Schutz seiner Informationen, die unter die Geheimhaltung der nationalen Verteidigung fallen, bewahrt Frankreich seine finanziellen und industriellen Fähigkeiten zum Entwickeln von Lösungen, die die höchsten Sicherheitsniveaus erreichen.

Allgemein muss die gesamte Verwaltung bei der Vergabe von öffentlichen Aufträgen als Vorbild dienen, indem sie Sicherheitskriterien angemessener Niveaus in die Wahl digitaler Produkte und Dienstleistungen mit einbezieht.

Ab 2016 profitieren alle Produkte oder Dienstleistungen, die in ein IT-System eingebettet sind oder sich darauf stützen und an einer öffentlichen Ausschreibung oder Projektausschreibung teilnehmen oder öffentliche Gelder in Anspruch nehmen wollen, von einem Bonusfaktor, wenn ihnen eine Risikoanalyse zur Cybersicherheit, die der vorgesehenen Nutzung des Produktes oder der Dienstleistung entspricht, und die technische Antwort beiliegt.

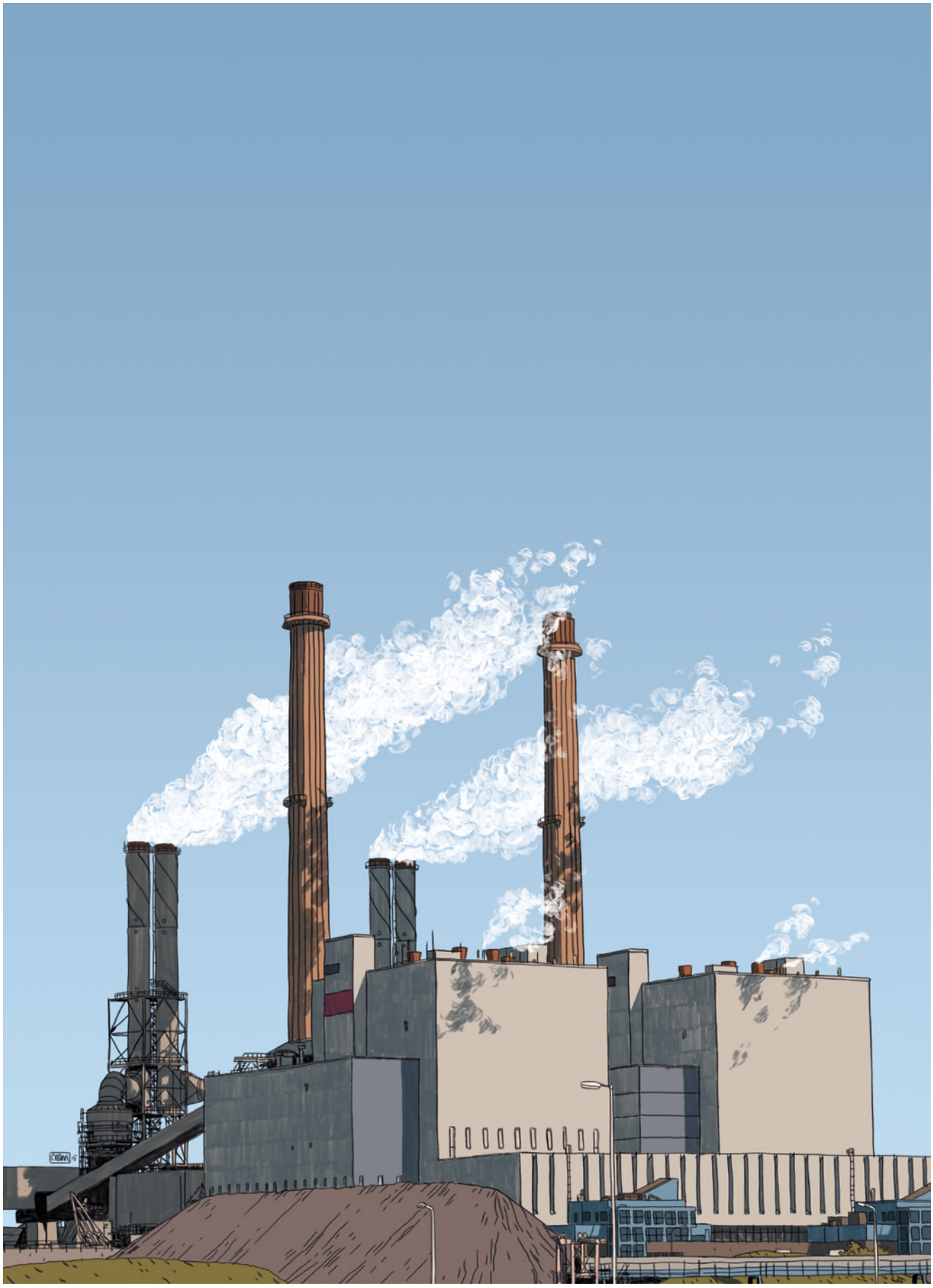
> Den Export und die Internationalisierung der Unternehmen des Sektors unterstützen.

Um die wirtschaftliche Entwicklung der Cybersicherheitsindustrie zu unterstützen, bemüht sich Frankreich um eine verstärkte Sichtbarkeit und Wettbewerbsfähigkeit des französischen Angebots auf internationaler Ebene und um einen leichteren Zugang der KMU und Startups zu den internationalen Märkten.

Die Koordination zwischen den Ministerien wird strukturiert und verstärkt. Über die derzeit oft einzeln und isoliert stattfindenden Aktionen der Ministerien und staatlichen Stellen hinaus wird eine angemessene Organisation zur Unterstützung der französischen Unternehmen eingerichtet.

Zusätzlich zur möglichen Erstellung von speziellen Unterstützungsvorrichtungen für die Akteure des Bereichs der Cybersicherheit, werden die Zugangsbedingungen zu den existierenden Unterstützungsvorrichtungen sowie ihre Umsetzungsmodalitäten geklärt und optimiert. Die Kontrollverfahren für den Export von Cybersicherheitslösungen werden geklärt und optimiert.

Darüber hinaus werden die aus dem privaten Sektor stammenden Initiativen zur Zusammenarbeit für die Begleitung von KMU und Startups auf der internationalen Ebene ähnlich wie die « French tech » Realisierungen unterstützt.



5

#EUROPA, DIGITALE SOUVERÄNITÄT, STABILITÄT DES CYBERSPACE

HERAUSFORDERUNGEN

« Der Cyberspace mag das weltweite Wachstum tragen, so ist er doch ein Ort eines oft unlauteren Wettbewerbs, von Konflikten (...) geworden. »

Der Cyberspace ist ein wichtiges Verhandlungsthema in den internationalen Organisationen geworden, deren Arbeiten sich mittlerweile auf den gesamten politischen Bereich auswirken.

2013 haben die Staaten anerkannt, dass der Cyberspace unter dem existierenden internationalen Recht steht und kein Ort ohne Regeln ist. Trotzdem wird der internationale Normenrahmen noch debattiert, was dem Erhalt eines stabilen und sicheren, die Grundrechte respektierenden, eine blühende Wirtschaft entwickelnden und das Vertrauen in die digitale Ära stärkenden Cyberspace schaden könnte, wenn es keine Fortschritte in den Verhandlungen gibt.

Solange immer mehr Länder behaupten, sich mit offensiven Mitteln auszustatten, wird es im Cyberspace zu immer mehr Konflikten zwischen Staaten kommen. Die Enthüllungen bestimmer Praktiken und Spionagetechniken, die von großen Staaten oder von Staatenbündnissen gegen andere, manchmal verbündete Staaten, Personen und Unternehmen eingesetzt wurden, haben den politischen Argwohn gegen die Urheberländer dieser Praktiken und das technische Misstrauen gegenüber ihren Produkten und Dienstleistungen gesteigert. Diese Enthüllungen begünstigen auch die Verbreitung ähnlicher technischer Mittel.

Parallel dazu führen Gruppen mit verschiedenen Motivationen und Unterstützungen, weltweit rekrutierte Söldner und je nach den Umständen Verbündete im Cyberspace regelmäßig Hackerangriffe durch, um zu versuchen, die Regierungsbehörden zahlreicher Länder oder Unternehmen, die diese symbolisch vertreten, zu destabilisieren. Terrororganisationen profitieren von der Zuhörerschaft, die ihnen die Netzwerke zutragen, um Propaganda zu verbreiten, die Freiwillige anziehen und die Bevölkerung terrorisieren soll. Diese Gruppen nutzen die konstanten medialen Auswirkungen.

In wirtschaftlicher Hinsicht bestätigt sich die Tendenz des Anfangs dieses Jahrzehnts. Einige wenige Unternehmen unterstützt von den Staaten, die ihre Entwicklung ermöglichten, nutzen ihren technologischen Vorsprung, ihre Marktdominanz und ihre finanziellen Kapazitäten, um die digitale Innovation zu vereinnahmen. Diese Privatisierung des Cyberspace zum Nutzen einiger Monopole verdammt die anderen Akteure der digitalen Technologien zur Abhängigkeit und bindet einen zu großen Teil des Mehrwerts der digitalen Technologien, als dass diese Situation für die Wirtschaft der anderen Länder akzeptabel sei.

Der Cyberspace mag das weltweite Wachstum tragen, so ist er doch ein Ort eines oft unlauteren Wettbewerbs, von Konflikten, von politischer Destabilisierung und von wirtschaftlicher Hegemonie geworden.

Europa konnte diese Gefahren erkennen und versucht durch den Dialog und die Reglementierung Ideen und Lösungen für eine nachhaltige digitale Entwicklung beizusteuern, sowohl hinsichtlich einer Internet-Governance, als auch zum Schutz der persönlichen Daten oder zur IT-Sicherheit der wesentlichen Wirtschaftsteilnehmer. Europa hat 2013 zwar eine Cybersicherheitsstrategie eingerichtet, tut sich aber mit der digitalen Souveränität und den Tools für einen Neuausgleich des Cyberspace zu seinen Gunsten schwer, obwohl dieses Thema auf der Tagesordnung zahlreicher europäischer Diskussionen und Verhandlungen steht.

Da es Werte mit den anderen Mitgliedsstaaten der Europäischen Union teilt, muss Frankreich zusammen mit ihnen eine führende Rolle bei den digitalen Technologien spielen.

Frankreich möchte über Bündnisse am digitalen Wandel in Europa teilnehmen. Das Europa von gestern war ein Bündnis für Rohstoffe. Das digitale Europa baut auf Bündnisse, Vertrauen und die Kontrolle über die Daten auf, die Rohstoffe der nächsten Jahrzehnte.

ZIEL

Frankreich wird zusammen mit den bereitwilligen Mitgliedsstaaten der Motor einer europäischen digitalen Souveränität. Es wird eine aktive Rolle in der Förderung eines sicheren, stabilen und offenen Cyberspace spielen.

AUSRICHTUNGEN

> **Mit den bereitwilligen Mitgliedsstaaten eine Roadmap für die digitale Souveränität Europas erstellen.**

Diese Roadmap, die den Mitgliedsstaaten der Europäischen Union offensteht, wird die Erfolgs-Schlüsselfaktoren für die kurzfristige Einrichtung der geeigneten Politik für eine europäische digitale Souveränität bestimmen. Dies betrifft vor allem die Reglementierung, die Normalisierung, die Zertifizierung, die Forschung und Entwicklung, das Vertrauen in die digitalen Technologien, die Verteidigung und Sicherheit der IT-Systeme — wobei die Einhaltung der Souveränität der Mitgliedstaaten, des Schutzes des Privatlebens und der persönlichen Daten, die als ein Gut des öffentlichen Interesses zu achten ist.

Genauso wird Frankreich darauf achten, dass die im Namen Europas ausgehandelten internationalen Verträge nicht zur technologischen oder wirtschaftlichen Abhängigkeit der europäischen Akteure führen und dass diese Verträge die persönlichen Daten seiner Bürger oder die vertraulichen Daten seiner Behörden nicht gefährden. Es wäre eine Quelle möglicher Destabilisierung der Cyberspace.

Es geht darum, Europa zum digitalen Gebiet zu machen, dass die Grund- und Einzelrechte am meisten achtet, und eine Zone des Vertrauens und des wirtschaftlichen Reichtums zu schaffen, im Sinne der Pionierarbeiten zwischen Frankreich und Deutschland hinsichtlich dem Cloud Computing oder dem verschlüsselten Austausch von Mails zwischen den beiden Ländern.

> **Die Präsenz und den Einfluss Frankreichs in den internationalen Diskussionen über die Cybersicherheit verstärken.**

Um das Vertrauen auf internationaler Ebene zu verstärken und neue Regelungsmechanismen zum Verhindern von Konflikten im Cyberspace zu prüfen, wird Frankreich seine Kontakte mit allen Beteiligten

verstärken, die den Dialog über die Herausforderungen der Cybersicherheit aufnehmen wollen.

Die Teilnahme an den multilateralen Verhandlungen über die Cybersicherheit (UNO, OSZE) wird intensiviert, um ein globales Verpflichtungsfundament zu anständigem Verhalten der Staaten im Cyberspace unter Einhaltung des internationalen Rechts zu festigen.

Die bilateralen Kontakte werden insbesondere im Rahmen diplomatischer Dialoge über die Herausforderungen des Cyberspace zwischen Ministerien verstärkt. Sie werden vom Ministerium für auswärtige Angelegenheiten und internationale Entwicklung geleitet.

Um Einfluss nehmen zu können, wird sich Frankreich mehr an internationalen eher informellen Foren beteiligen, in denen die technischen und akademischen Communities sowie die politischen Entscheidungsträger zusammen über das zukünftige Gleichgewicht nachdenken.

> Zur globalen Stabilität des Cyberspace beitragen, indem bereitwillige Länder beim Einrichten von Cybersicherheitskapazitäten unterstützt werden.

Der digitale Übergang als Träger politischer, sozialer und wirtschaftlicher Gelegenheiten, wird noch lange nicht in allen Ländern homogen beherrscht. Dies ist zum Nachteil der Sicherheit und der Entwicklung der weniger geschützten Staaten und schwächt auf internationaler Ebene das gesamte digitale Ökosystem.

Um zu einer zuverlässigen und nachhaltigen Verbreitung der IKT in allen Ländern und vor allem in den Entwicklungsländern beizutragen, will Frankreich zur Verstärkung der Kapazitäten der Länder beisteuern, die die Belastbarkeit und Sicherheit ihrer Informationssysteme vor allem hinsichtlich des Schutzes der kritischen Infrastrukturen und der Bekämpfung der Cyberkriminalität stärken wollen.

Um die Dauerhaftigkeit und Nachhaltigkeit der Kapazitätsverstärkungsprojekte zu gewährleisten, wird Frankreich seine Aktionen vorzugsweise in langfristig vertrauenswürdige Partnerschaften investieren. Durch diese Aktionen muss Frankreich auch seine eigene Cybersicherheit verstärken können.