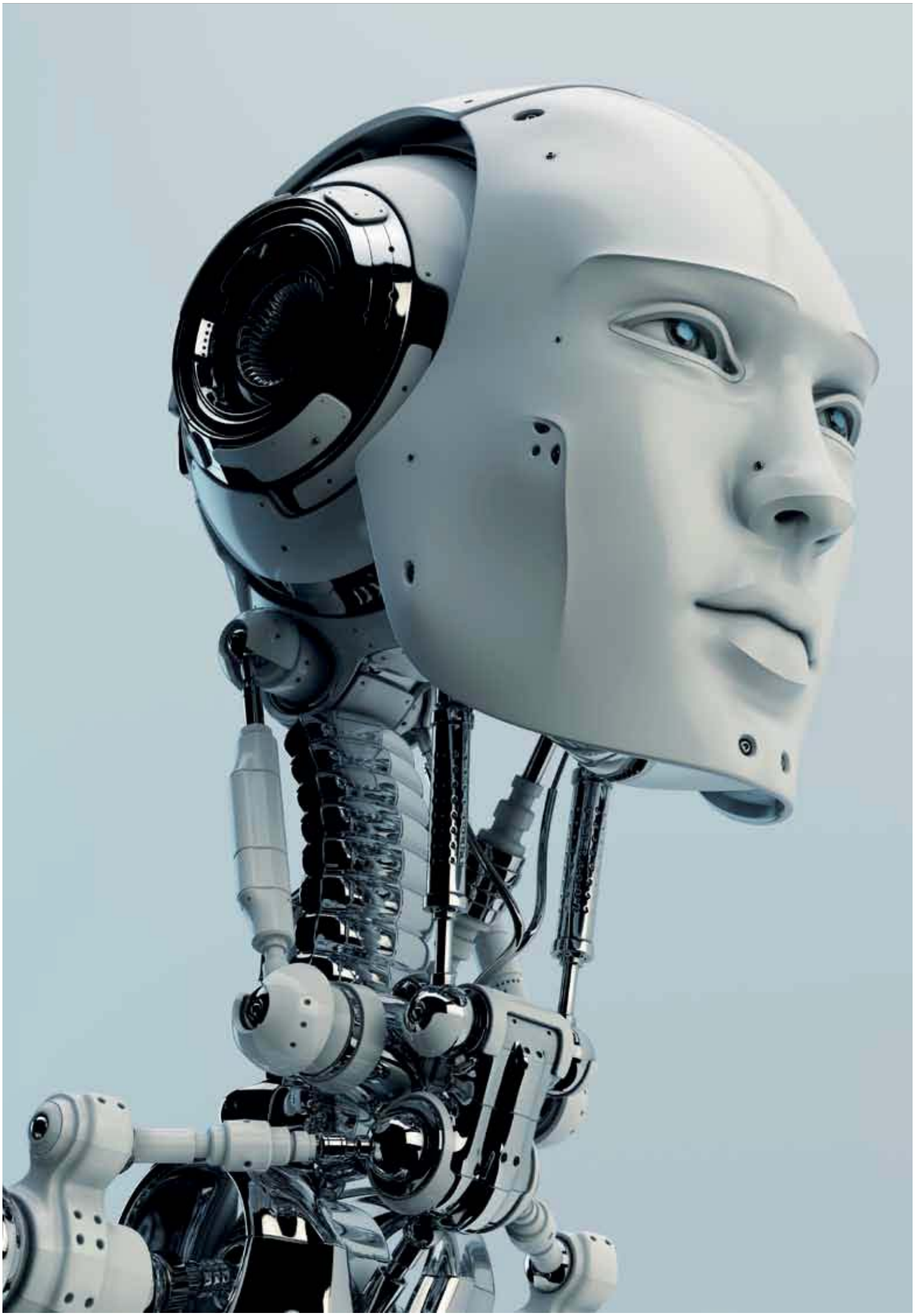
Deloitte.

European Cyber Defense
Teil 2: Cybersicherheit in Europa 2030



Scenario Thinking

Ein Blick in die Zukunft der Cybersicherheitslandschaft in Europa

Wie sich die Cybersicherheitslandschaft in Zukunft entwickeln wird, ist eine der unsichersten Fragen, mit denen wir heute konfrontiert sind. Exponentielle technologische Entwicklungen, sich ändernde Vorschriften und dynamische politische Rahmenbedingungen führen zu ständigen Veränderungen. Neue Akteure werden aktiv, und die Rolle von Cybersicherheit im politischen und militärischen Bereich verlagert sich. Dies sind nur einige der vielen starken Kräfte, die die Cybersicherheitslandschaft reformieren.

Die Entscheidungen der verschiedenen Akteure in diesem unsicheren Umfeld werden die Zukunft der öffentlichen und privaten Sektoren sowie der Zivilgesellschaft und der Staatsbürger bestimmen. Entscheider von heute haben damit die Möglichkeit, die Weichen für die zukünftige Cybersicherheitslandschaft zu stellen.

Es ist zweifelsohne schwierig, diese Komplexität zu erfassen – insbesondere, wenn man auf konventionelle Politik- bzw. Strategieanalyse zurückgreift. Auch wenn es unmöglich ist, die Zukunft vorherzusagen, kann die Szenarioanalyse die Komplexität begreifbar machen, indem sie plausible Geschichten über die Zukunft erzählt und die Risiken und Chancen aufzeigt. Szenarien sind Erzählungen alternativer Zukunftsmöglichkeiten. Sie dienen als Grundlage für strategische Entscheidungen privater, öffentlicher oder zivilgesellschaftlicher Akteure, die sich mit Fragen der Cybersicherheit beschäftigen. Sie ermöglichen es diesen Entscheidungsträgern, robuste und dennoch flexible Strategien für potenzielle Zukunftsszenarien zu entwickeln.

Die Cybersicherheitslandschaft befindet sich in einem raschen Wandel, der sich weiter beschleunigt. Diesen haben wir in zwei getrennten Teilen dieser Studie festgehalten. Während sich der erste Teil des European Cyber Defense Reports 2018 mit dem Status quo der nationalen Cybersicherheitsstrategien befasst, ist dieser zweite Teil der Studie auf die Zukunft fokussiert: Wie wird die Cybersicherheitslandschaft in Europa im Jahr 2030 aussehen? Welche Risiken und Chancen ergeben sich daraus? Um diese Fragen zu beantworten, haben wir vier mögliche Szenarien entwickelt.

Im **Goldener-Käfig-Szenario** ist die europäische Cybersicherheitslandschaft hoch stabil und sicher. Bedrohungen sind bekannt und es gibt kaum Disruptionen. Der Industrie geht es gut, auch wenn sie ihren Teil zu den hohen Kosten für Sicherheit beitragen muss. Allerdings gibt es nur sehr wenig Innovationen und eine hohe Verwundbarkeit unvorhergesehenen Bedrohungen gegenüber. Nichtstaatliche Akteure außerhalb der funktionierenden Ordnung bedrohen die Cybersicherheit. Um sichere Regionen wie die EU sind „Goldene Schutzwälle" entstanden, und Protektionismus ist die Norm. Die Gesellschaft ist selbstzufrieden und träge geworden, aber Bedrohungen lauern in den Schatten.

Im **Szenario-Selbstschutz** leben wir in einer zutiefst verunsicherten und technologisch fragmentierten Welt, die durch eine Kultur des Misstrauens und ein hohes Maß an Bürokratie gekennzeichnet ist. Durch die Privatisierung von Sicherheit sowie Cyberselbstregulierung sind kleine, thematische Inseln der Sicherheit entstanden. Um dem Mangel an Effektivität in der Cybersicherheit entgegenzuwirken, herrscht ein hoher Innovationsdruck. Diplomatische Verhandlungen haben deutlich zugenommen. Jedoch werden neue Regeln und Vorschriften nicht durchgesetzt und Cybersöldner sind oft der einzige Schutz vor häufigen Cyberangriffen.

In einer anderen Szenarienwelt hat der **Cyber-Darwinismus** überhandgenommen. Ein Europa der freien Marktkräfte ist zu einem digitalen Dschungel geworden, in dem nichtstaatliche oder quasi-staatliche Akteure aufgestiegen sind. Cyberföderalismus ist die Norm. Auch wenn es kleine, stark geschützte Inseln der (Cyber-)Sicherheit gibt, ist die Außenwelt sehr unsicher. Der anschließende Aufstieg der Zweiklassensicherheit hat zu einem hohen Maß an sozialer Ungerechtigkeit geführt. Cybersicherheit ist zu einem klaren Wettbewerbsvorteil geworden, und Unternehmen migrieren in Bereiche mit klarer Cyberregulierung. Die Individualisierung hat zum Ende der Globalisierung geführt. Auch wenn multilaterale und bilaterale Allianzen weiterhin bestehen, gibt es ein hohes Maß an Aufrüstung. Unter dem Strich besteht Europa aus gescheiterten Cyberstaaten.

Im **Cyber-Oligarchie-Szenario** herrscht eine kleine Cyberelite über die Cybersicherheit. Der hochinnovative freie Markt profitiert stark von der geringen staatlichen Einflussnahme und Kontrolle. Auf der anderen Seite hat die Automatisierung zu hoher Arbeitslosigkeit geführt, während die Zunahme von Cyberangriffen und Gegenangriffen zu einem hohen Risiko von (Cyber-) Konflikten geführt hat. Es gibt einen hohen Bedarf an Abschreckung, was zu einem Cyberwettrüsten und vielen kleinen heißen Kriegen geführt hat. Das Potenzial für neue Staatskonzepte ist groß, und die Privatwirtschaft hat ein aktives Interesse am (Wieder-) Aufbau eines funktionierenden Staates.

Die Cybersicherheitslandschaft von heute verändert sich rasch und signifikant. Diese vier Szenarien zeigen, wie unterschiedlich die Zukunft sein könnte. Jedes Szenario bringt seine eigenen Chancen und Risiken mit sich – was bedeuten sie für uns?

Begeben Sie sich mit uns auf die Reise.

center
for the long view

Kritische Unsicherheiten

Die Treiber der Zukunft für die Cybersicherheitslandschaft

Als Teil der Szenarioanalyse haben wir eine umfassende Liste mit politischen, militärischen, technologischen, sozialen, wirtschaftlichen und umweltbezogenen Faktoren entwickelt, die das Potenzial haben, die Cybersicherheitslandschaft in Europa zu beeinflussen. Diese Liste basiert auf umfangreichen Analysen mit Hilfe von Künstlicher Intelligenz unter Verwendung von natürlicher Sprachverarbeitung, Experteninterviews sowie auf traditioneller Recherche. Ein vielseitiges, interdisziplinäres Expertengremium aus den öffentlichen und privaten Sektoren sowie aus der Zivilgesellschaft hat diese Treiber nach ihrem Einfluss auf die Cybersicherheitslandschaft in Europa bis zum Jahr 2030 und nach dem

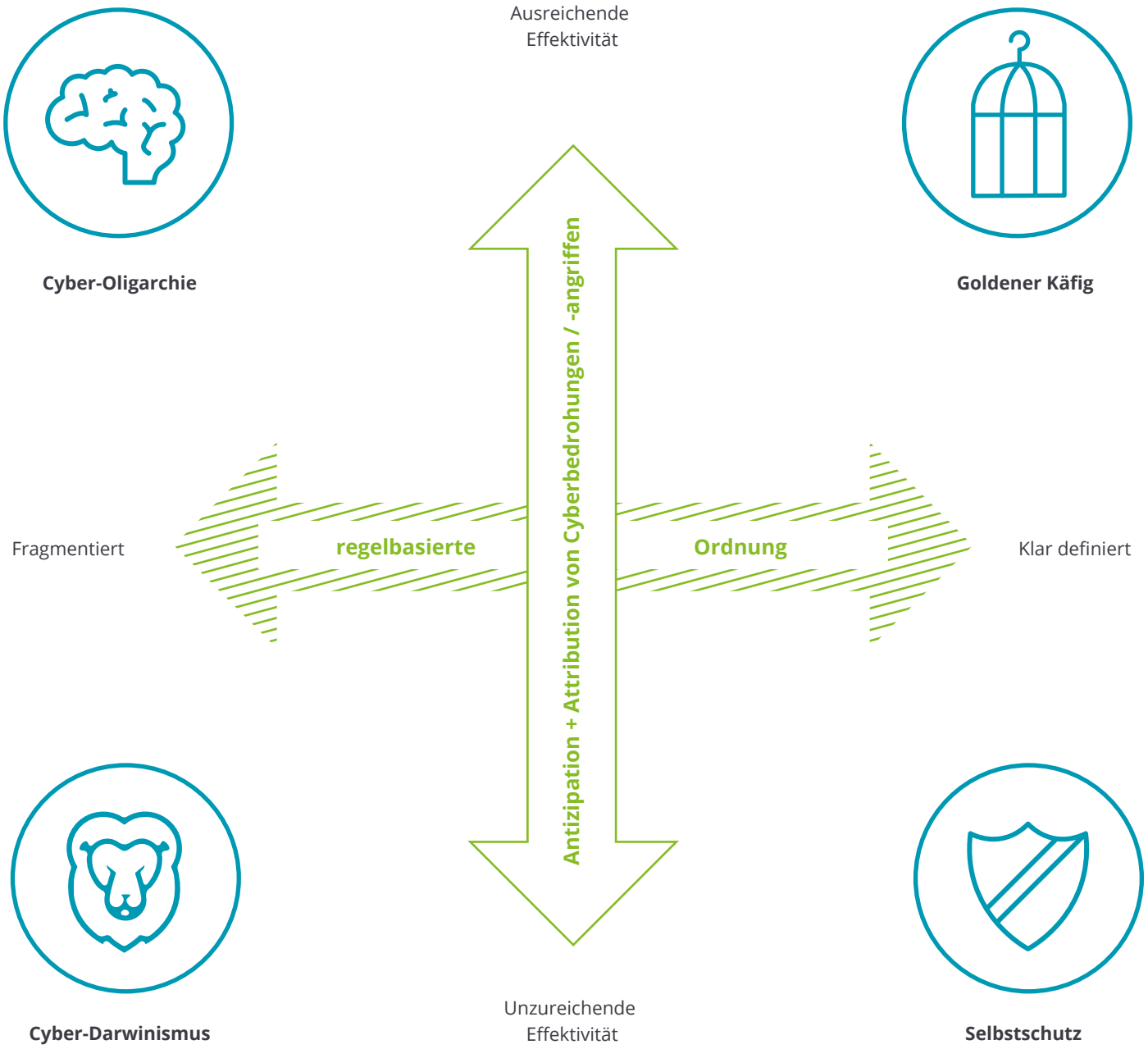
Grad der Unsicherheit ihrer Entwicklung bewertet. Anschließend wurden die einflussreichsten und unsichersten Treiber in Cluster von kritischen Unsicherheiten eingeteilt. Kritische Unsicherheiten sind übergreifende Schlüsselthemen, die die Entwicklung der Cybersicherheitslandschaft in Europa in die eine oder die andere Richtung kippen könnten.

Unser Expertengremium hat zwei kritische Unsicherheitscluster als wesentliche Einflussfaktoren für die Zukunft der europäischen Cybersicherheit identifiziert. Erstens die Existenz und das Ausmaß einer regelbasierten Ordnung. Dies bezeichnet eine Ordnung, die auf rechtlichen Rahmenbedingungen und Standards auf lokaler, nationaler oder internationaler Ebene oder einer Kombination hieraus basiert. Zweitens die Fähigkeit, Cyberbedrohungen zu verhindern und Cyberangriffe zu attribuieren. Die Antizipation von Cyberbedrohungen beinhaltet die Identifizierung von und die Vorbereitung auf Cyberangriffe innerhalb des bekannten Spektrums von Angriffsmechanismen und -methoden. Die Attribution von Cyberangriffen bezieht sich auf den Prozess der Zuschreibung von Straftaten an Täter durch die erfolgreiche Zurückverfolgung, Identifizierung und rechtliche Strafverfolgung von Cyberkriminellen.

Die regelbasierte Ordnung kann entweder klar definiert und funktionsfähig oder fragmentiert und auf der Herrschaft des Stärkeren basiert sein. Bei Ersterer ist Europa durch das Vorhandensein operativ getriebener Regeln und Vorschriften zu Cyberfragen, bilateraler und multilateraler Zusammenarbeit sowieso allgemeiner menschlicher Interaktion im Cyberspace gekennzeichnet. Im zweiten Fall hingegen ist Europa vom Fehlen allgemein akzeptierter und durchgesetzter Vorschriften geprägt. Dabei wird Cybersicherheit von einer dominanten Minderheit getrieben und kontrolliert. Zu den zugrundeliegenden Treibern dieser kritischen Unsicherheit gehören internationale Cyberkooperation, internationale unilaterale Cyberregulierung, Datenschutz und Regulierung der Privatsphäre, die Bedeutung der EU für die Cybersicherheit und die Beziehungen zwischen der EU und anderen Akteuren wie der NATO, den Vereinten Nationen und einzelnen Staaten wie Russland, China oder Nordkorea.

Das Antizipieren von Cyberbedrohungen und die Attribution von Cyberangriffen können in Zukunft entweder ausreichend oder unzureichend wirksam sein. Einerseits könnte diese kritische Unsicherheit die Form von Vorbeugung, Früherkennung und Aufklärung von Cyberbedrohungen annehmen, wobei die Behörden in der Lage sind, Angriffe zuzuordnen und Täter effizient zu verfolgen. Andererseits könnte die Zukunft geprägt sein von einer hohen (Cyber-) Unsicherheit aufgrund der Unfähigkeit des Staates, Cyberangriffe zu verhindern oder zu verfolgen. Dieser Entwicklungen liegen die Treiber Entwicklung der Computerrechenleistung, Quantencomputing, die Höhe von Cyberrisiken, die Effizienz und Genauigkeit von Attribution, die Effizienz der Strafverfolgung bei der Bekämpfung von Cyberkriminalität und ICT-Terrorismus, Threat Intelligence sowie Malware- und Ransomwareangriffe zugrunde. Die Kombination der zwei kritischen Unsicherheiten führt zu vier Zukunftsvisionen, wie in Abbildung 1 dargestellt. Alle vier hieraus resultierenden Szenarien entsprechen fünf Kriterien: Sie müssen plausibel, relevant, divergent, herausfordernd und ausgewogen sein. Jedes dieser vier Szenarien erzählt also von einer anderen Zukunft, von vier alternativen Welten, die im Jahre 2030 existieren könnten.

Abb. 1 – Szenario-Matrix zur Beschreibung der Zukunft der europäischen Cybersicherheitslandschaft



Vier mögliche Szenarien für die Zukunft

Die Cybersicherheitslandschaft in Europa im Jahr 2030

Goldener Käfig

Klar definierte und funktionierende regelbasierte Ordnung und ausreichende Effektivität bei der Antizipation von Cyberbedrohungen und der Attribution von Cyberangriffen

In diesem Szenario ist Europa sehr sicher und stabil und sieht sich mit wenig Disruption konfrontiert. Die Cyberbedrohungslage ist bekannt und Sicherheitsorganisationen berichten ehrlich über aktuelle Bedrohungen und Entwicklungen. Obwohl eine starke Cyberüberwachungskultur existiert, um ein hohes Maß an Sicherheit zu gewährleisten, ist diese klar und transparent geregelt. Starke Innovation in den frühen 2020er Jahren hat zu einer Schaffung der technologischen Fähigkeiten geführt, um Cyberbedrohungen effektiv entgegenzutreten. Regelmäßiges Training und Testen der Cyberfähigkeiten garantieren ständige Wachsamkeit gegenüber Cyberbedrohungen. Dies wird durch zivile Cyberübungen ergänzt, zum Beispiel in Schulen und Privatunternehmen. Um Europa herum wurde ein „goldener Schutzwall" errichtet und Protektionismus bestimmt die europäische Politik.

Nach dem ersten Innovationsschub gibt es jetzt, im Jahr 2030, jedoch nur noch sehr wenig Raum für Innovationen, und das geringe Innovationspotenzial ist auf das Ingenieurswesen beschränkt. Der Privatsektor ist zwar gesund, aber muss sich an den hohen Kosten des Cybersicherheitssystems beteiligen. Die Gesellschaft ist bequem geworden und verlässt sich auf bestehende Lösungen. Während sich die Staaten in hoher Alarmbereitschaft befinden, wenn Gegner und Bedrohungen vorhanden sind, werden sie träge, wenn dies nicht der Fall ist. Folglich ist Europa zwar auf bekannte Bedrohungen vorbereitet, aber sehr anfällig für unvorhergesehene Entwicklungen. Deshalb stellen nichtstaatliche Akteure, die außerhalb der bestehenden Ordnung agieren, die größte Bedrohung für die Cybersicherheitslandschaft in Europa dar.

Selbstschutz

Klar definierte und funktionierende regelbasierte Ordnung und unzureichende Effektivität bei der Antizipation von Cyberbedrohungen und der Attribution von Cyberangriffen

In dieser Welt ist Europa sehr bürokratisch, extrem unsicher und technologisch fragmentiert. Obwohl es kleine thematische Inseln der Sicherheit gibt, zum Beispiel rund um das vernetzte Gesundheitssystem, ist Cybersicherheit außerhalb dieser Bereiche lückenhaft. Da der öffentliche Sektor keine effiziente Cybersicherheit garantieren konnte, wurde Sicherheit privatisiert. Cyberselbstregulierung und der Einsatz von Cybersöldnern sind die Norm. Dies hat zu einer neuen Cybersicherheitswirtschaft und zu einem Wettbewerb zwischen privaten und öffentlichen Sicherheitsanbietern geführt. Der öffentliche Sektor kämpft hart um Respekt im Sicherheitsbereich. Es gibt umfangreiche Cyberspähtruppen und Cybersondereinheiten. Wachsende Bedrohungslagen haben jedoch zur Notwendigkeit von privat-öffentlichen Partnerschaften geführt. Das daraus resultierende Sicherheitskorsett ist dabei, die Gesellschaft zu ersticken, und es herrscht eine Kultur des Misstrauens.

Um dem Mangel an Effektivität in der Cybersicherheit entgegenzuwirken, besteht in Europa ein enormer Innovationsdruck, wobei sowohl der öffentliche als auch der private Sektor die technologische Entwicklung vorantreiben. Das Innovationspotenzial befindet in der Privatwirtschaft, aber der Schwerpunkt liegt auf nationaler Cybersicherheitsinnovation. Wenn nötig verstaatlichen Regierungen private Unternehmen im Drang nach effizienter Cybersicherheit. In diesem Umfeld herrschen Skaleneffekte, und kleine und mittlere Unternehmen leiden darunter.

Um die regelbasierte Ordnung aufrechtzuerhalten und zu erweitern, haben Verhandlungen und Diplomatie stark an Bedeutung gewonnen. Zusammenarbeit und Regulierung wurden auf bilateraler und multilateraler Ebene verstärkt, und weiterhin werden neue Allianzen gebildet. Es mangelt jedoch an Effizienz bei der Umsetzung dieser klar definierten und operativen Regeln.

Cyber-Darwinismus

Fragmentierte regelbasierte Ordnung, getrieben von der Herrschaft der Stärksten und unzureichende Effektivität bei der Antizipation von Cyberbedrohungen und der Attribution von Cyberangriffen.

In dieser alternativen Zukunft ist Europa zu einem Dschungel geworden, der auf der Basis einer Laissez-faire-Mentalität arbeitet. Während kleine Inseln mit einem hohen Maß an (Cyber-)Sicherheit innerhalb von „gated communities" existieren, ist die Außenwelt sehr unsicher. Daraus resultiert ein Zwei-Klassen-Sicherheitssystem, das niedrige Sicherheitsklassen stark diskriminiert und ausschließt. Eine Flut höchst ineffizienter Cyberregulierungen auf regionaler oder mindestens nationaler Ebene hat zum Cyberföderalismus geführt: Um den Mangel an effektiver nationaler und internationaler Regulierung zu kompensieren, haben Bundesländer und Teilregionen eine eigene Cyberpolitik entwickelt. Das daraus resultierende regulatorische Chaos und die Existenz von Sicherheitsknotenpunkten hat zu regionalen Cybersicherheitshäfen geführt, die von ihrem Sicherheitsstatus profitieren und einen hohen Lebensstandard bieten. Cyberwarlords herrschen über einzelne Territorien, und nichtstaatliche und quasi-staatliche Akteure haben an Macht gewonnen. Die Globalisierung ist beendet und wurde durch Individualisierung ersetzt. Cybersicherheit ist zu einem klaren Wettbewerbsvorteil geworden. Industrien wandern in Gebiete mit hoher Cyberregulierungsklarheit, wie zum Beispiel China, ab. Allianzen dauern an bestehenden bilateralen und multilateralen Abkommen fort, aber das Fehlen internationaler Regulierung hat zu einer starken Aufrüstung einzelner Länder und Teilregionen geführt. Insgesamt besteht Europa aus gescheiterten Cyberstaaten, die vom Prinzip des Überlebens der Stärksten beherrscht werden.

Cyber-Oligarchie

Fragmentierte regelbasierte Ordnung, getrieben von der Herrschaft der Stärksten und ausreichende Effektivität bei der Antizipation von Cyberbedrohungen und der Attribution von Cyberangriffen

In diesem Szenario beherrscht eine kleine Elite von Cyberexperten die Cybersicherheitslandschaft in Europa. Cybersicherheit wird nicht mehr vom Staat gesteuert. Stattdessen wird Cybersicherheit privat nach den „Gesetzen des Stärkeren" durchgesetzt. Folglich gibt es ein hohes Potenzial für neue Staatskonzepte. Der Privatsektor hat ein aktives Interesse am Vorhandensein eines funktionierenden Cybersicherheitsstaates und steuert sowohl Finanzen als auch Wissen zur (Wieder)Herstellung von Ordnung im öffentlichen Sektor bei. In dieser fragmentierten Ordnung, die von den Stärksten beherrscht wird, besteht ein großer Bedarf an Abschreckung, auch nuklearer Natur. Infolgedessen hat ein Cyberwettrüsten stattgefunden, dessen Spannungen sich in vielen kleinen heißen Konflikten entluden. Cyberangriff haben zugenommen, und das Risiko von (Cyber-)Konflikten, einschließlich des Einsatzes von Internet-Waffen der Massenvernichtung (IWMDs), ist hoch.

Die Abwesenheit von staatlicher Einflussnahme und Kontrolle hat dem Privatsektor große Chancen eröffnet. Der freie Markt profitiert von einem großen Spielraum für Innovation und Kreativität. Start-ups florieren und streben im Allgemeinen nicht nach Unabhängigkeit, sondern nach der Eingliederung in einen der Technologieriesen. Auch zwischen traditionellen Industrien wie der Automobilindustrie und diesen Technologieriesen haben sich starke Allianzen gebildet, wobei führende traditionelle Unternehmen unter dem Dach innovativer Technologie-Imperien agieren. Nichtsdestotrotz hat die Automatisierung zu hoher Arbeitslosigkeit geführt, und es kommt zu häufigen sozialen Protesten. Traditionelle bilaterale und multilaterale Allianzen bleiben bestehen, und es gibt ein hohes Maß an Positionsklarheit bei den Akteuren im Bereich der Cybersicherheit.

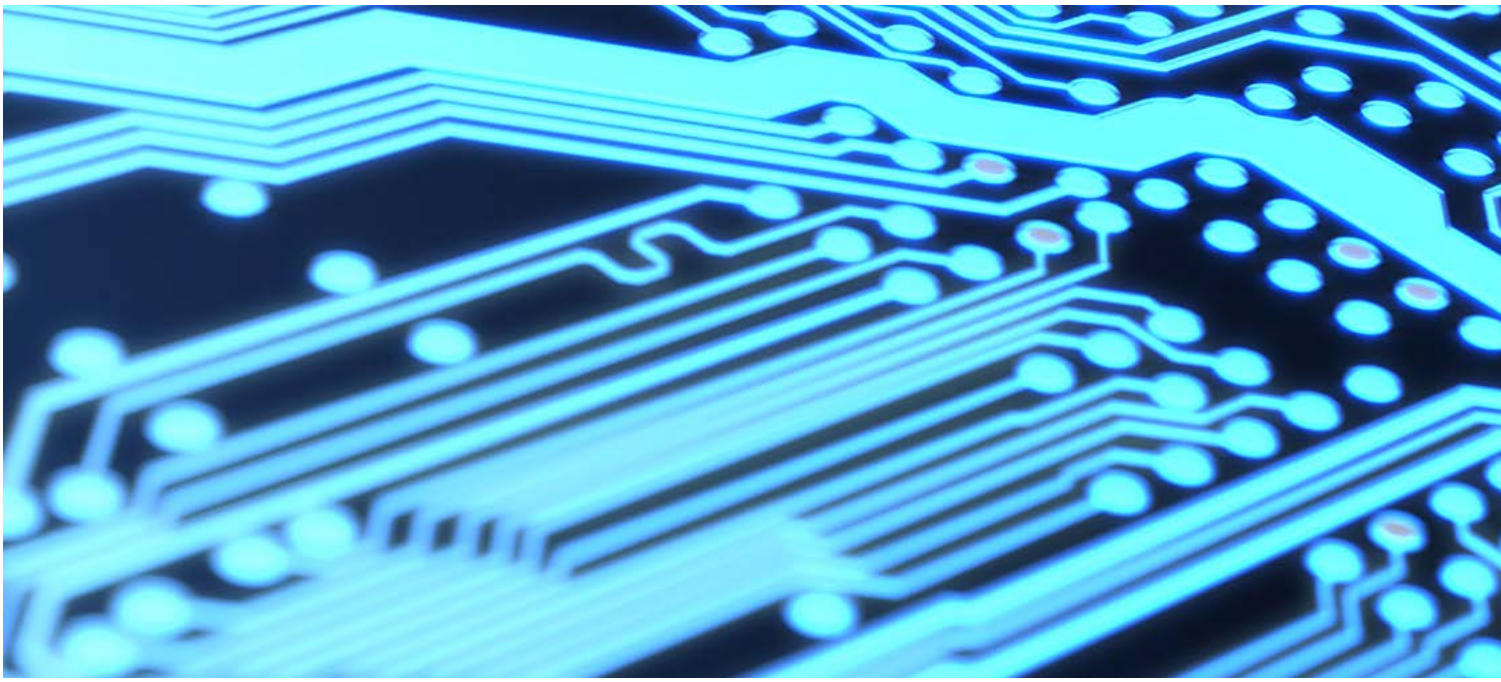
Fazit und Ausblick

Die Zukunft der Cybersicherheitslandschaft in Europa wird weitreichende Folgen für die privaten und öffentlichen Sektoren sowie für die Zivilgesellschaft haben.

Bei der Betrachtung dieser vier Szenarien fällt am meisten ihr zeitlicher Horizont auf. Im dynamischen und extrem schnelllebigen Bereich der Cybersicherheit erscheint bereits das Erfassen von einigen wenigen Jahren oft als eine unmögliche Aufgabe. Nichtsdestotrotz – und genau deswegen – blicken unsere Szenarien weiter in die Zukunft und zeigen, wie die Cybersicherheits- landschaft im Jahr 2030, aussehen könnte.

Auch wenn die Zukunft der Cybersicherheitslandschaft äußerst ungewiss ist, müssen ihre Auswirkungen auf die öffentlichen und privaten Sektoren und die Zivilgesellschaft in Europa und darüber hinaus unbedingt bedacht werden. Unsere vier Szenarien machen genau das möglich. Wir gehen nicht davon aus, dass ein einzelnes Szenario vollständig und eindeutig wie hier beschrieben eintrifft – vielmehr wird die Zukunft der Cybersicherheitslandschaft zwischen den verschiedenen Zukunftsalternativen liegen. Indem Akteure und Entscheider über diese vier extremen Szenarien nachdenken und sich darauf vorbereiten, können sie robuste, aber flexible Strategien für jede Zukunft zwischen diesen Alternativen formulieren. In Anbetracht der Erkenntnisse über den derzeitigen Stand der nationalen Cybersicherheitsstrategien in Europa, wie sie im ersten Teil des European Cyber Defense Report 2018 skizziert werden, ist dies besonders essenziell. Mit vielen veralteten Cybersicherheitsstrategien und keiner einzigen zukunftsfokussierten Cyberstrategie ist die Vorbereitung auf die Zukunft von außerordentlicher Wichtigkeit.

Während sich aus diesen Szenarien eine Vielzahl von gemeinsamen Schlussfolgerungen für die verschiedenen Akteure ergibt, ist die vielleicht wichtigste hierbei die Notwendigkeit der übergreifenden Kooperation. Zusammenarbeit und Abstimmung innerhalb und zwischen Staaten und regionalen und internationalen Organisationen wird unerlässlich sein. Der Privatsektor, einschließlich Militär und Nachrichtendienste, der öffentliche Sektor und die Zivilgesellschaft in jedem Land müssen zusammenarbeiten, um sich auf zukünftige Risiken vorzubereiten und Chancen in der Zukunft zu nutzen. Ebenso müssen die Staaten gemeinsam daran arbeiten, Cybergovernance regional und global voranzutreiben. Regionale und internationale Organisationen und Allianzen, insbesondere die EU, die NATO und die Vereinten Nationen, müssen

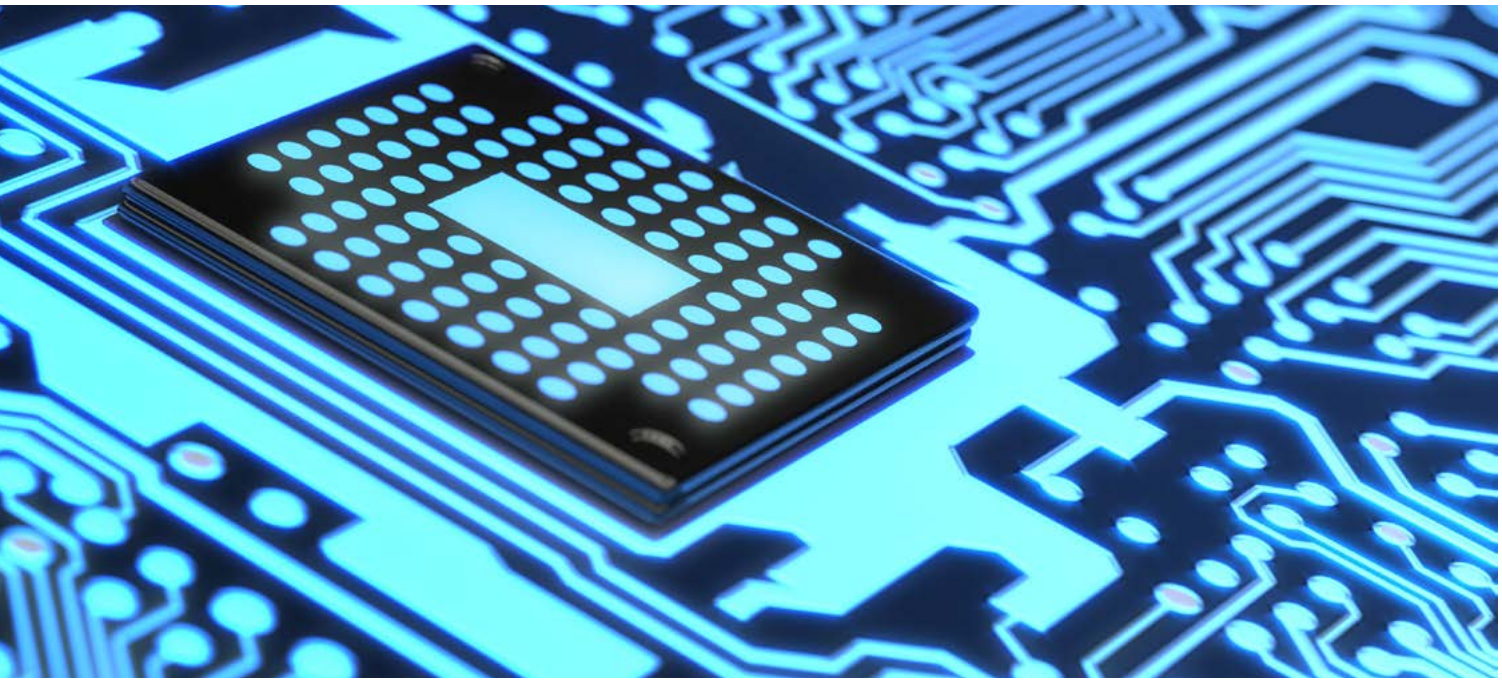


mit den Staaten und untereinander zusammenarbeiten, um Cybersicherheit auf allen Ebenen zu ermöglichen.

Viele andere allgemeine Folgerungen ergeben sich aus den vier Szenarien. Der Bedarf an digitaler Bildung und Ausbildung, die Notwendigkeit, sich mit der Verschiebung in Richtung Hybrid- oder Cyberkriegsführung auseinanderzusetzen, einschließlich des möglichen offensiven Einsatzes von Cyberwaffen durch Staaten, und die Notwendigkeit, unverzichtbare Infrastrukturen zu schützen, sind nur einige Beispiele dafür. Gleichzeitig bringt jedes Szenario eine Reihe von spezifischen Folgerungen mit sich, sowohl hinsichtlich der Risiken als auch der Chancen.

Das Entwickeln spezifischer Strategien für jedes der vier Szenarien ermöglicht es Entscheidungsträgern, flexibel auf das dynamische Umfeld der Cybersicherheit innerhalb und außerhalb Europas zu reagieren. So können Entscheidungsträger den Wandel in der Cybersicherheitslandschaft proaktiv vorantreiben und sich auf die Risiken vorbereiten, die in den Schatten am Wegrand lauern. In diesem Sinne zielen diese Geschichten über die Zukunft darauf ab, aktuelle Denkweisen herauszufordern, Wahrnehmungen in Frage zu stellen und Komplexitäten zu erfassen, die ansonsten verloren gehen würden.

Die vier Szenarien mögen radikal unterschiedlich sein, aber sie haben einen gemeinsamen Nenner: Vordenken, Weitsicht und eine enge Zusammenarbeit zwischen Entscheidungsträgern der privaten und öffentlichen Sektoren und der Zivilgesellschaft werden vonnöten sein, um die sich ständig verändernde Landkarte der europäischen Cybersicherheitslandschaft erfolgreich zu handhaben. Die Szenarioanalyse kann dabei als Kompass dienen – und Sie den Weg weisen lassen.



Methodik

Eine kurze Einführung in das Szenariodesign und seine Methodik
Diese Studie über die Zukunft der europäischen Cybersicherheitslandschaft basiert auf der siebenstufigen Szenariomethodik des Center for the Long View (CLV). Diese wendet die wissenschaftlichen Leitprinzipien der Objektivität, Zuverlässigkeit und Validität an. Diese Studie ist das Ergebnis umfangreicher Recherchen, Experteninterviews und eines Szenario-Workshops mit politischen, militärischen, wirtschaftlichen und sozialen Cybersicherheitsexperten aus den privaten und öffentlichen Sektoren und der Zivilgesellschaft sowie dem Deloitte-Netzwerk und erfahrenen Szenarioanalysten des CLV.

Unsere Szenariomethodik beginnt mit der Formulierung einer Fokusfrage, um den Umfang und die strategische Ausrichtung des Projekts zu bestimmen. Die Schwerpunktfrage für diese Studie war die folgende: Wie wird die Cybersicherheitslandschaft in Europa im Jahr 2030 aussehen?

Da Szenarien eine Möglichkeit bieten, die Dynamik der Zukunft zu verstehen, ist der zweite Schritt unseres methodischen Ansatzes die Identifikation von Zukunftstreibern, die das Potenzial haben, die Antwort auf die Fokusfrage zu beeinflussen. Diese Treiber lassen sich in fünf Kategorien einteilen, die als STEEP-Forces bezeichnet werden und sich aus sozialen, technologischen, wirtschaftlichen, umwelttechnischen und politischen Faktoren zusammensetzen (aus dem Englischen: social, technological, economic, environmental, political).

Um die lange Liste der Treiber für diese Studie zu ermitteln, haben wir vor allem auf unser KI-basiertes Analyse-Tool CLV Deep View und auf Interviews mit ausgewählten Deloitte-Experten zurückgegriffen. Deep View verwendet natürliche Sprachverarbeitung, um Millionen von Datensätzen zu lesen und zu bewerten. Besondere Analyseansichten können über Schlüsselwörter, Phrasen, Personen, Unternehmen oder Institutionen erstellt werden. So können wir hochkomplexe Sachverhalte und Zusammenhänge ganzheitlich verstehen und aktuelle und zukünftige Trends erkennen. So hilft Szenarioplanung, die Voreingenommenheit traditioneller Analyseansätze zu vermeiden. Diese sind oft stark beeinflusst von dem Charakter, der Einstellung oder den persönlichen Vorlieben der Szenarioanalysten.

In einem dritten Schritt priorisieren und bündeln wir die identifizierten Treiber in kritische Unsicherheiten. Das ist notwendig, weil nicht alle Treiber gleich unsicher sind. Oft ist die Entwicklung einzelner Treiber sehr klar und vorhersehbar und bleibt somit über alle vier Szenarien relativ gleich. Kritische Unsicherheiten müssen also zwei Kriterien erfüllen: Erstens müssen sie einen maßgeblichen Einfluss auf die Antwort der Fokusfrage haben. Zweitens müssen sie sehr unsicher oder volatil sein. Zunächst erscheinen alle kritischen Unsicherheiten einzigartig, doch durch eine Analyse möglicher Korrelationen zwischen einzelnen kritischen Unsicherheit können verwandte Unsicherheiten vermieden und die konkreten Bausteine für unser Szenario-Framework festgelegt werden.

Das Szenario-Framework wird im vierten Schritt unseres Szenario-Design-Ansatzes entwickelt. Die ermittelten kritischen Unsicherheiten dienen dabei als Achsen einer Szenariomatrix, die vier sehr unterschiedliche, aber plausible Szenarien aufzeigt. In der vorliegenden Studie sind diese zwei kritischen Unsicherheiten die Beschaffenheit der regelbasierten Ordnung und die Möglichkeit, Cyberbedrohungen zuvorzukommen und Cyberangriffe zu attribuieren.

Ist die Szenariomatrix einmal erstellt, entwickeln wir in einem fünften Schritt die vier Szenarionarrative. Szenarionarrative definieren die Rahmenbedingungen und den einzigartigen Charakter eines jeden Szenarios im Kontext einer Geschichte. Die zuvor identifizierten Treiber dienen hier als Bausteine. Diese werden als Schlüsselelemente von unserem Zukunftszeitpunkt aus zurückentwickelt, um Meilensteine für jedes Szenario zu definieren und die Geschichte flüssig zu erzählen.

In einem sechsten Schritt nutzen wir dann diese Szenarionarrative, um daraus Konsequenzen für die beteiligten Akteure, wie die privaten und öffentlichen Sektoren sowie die Zivilgesellschaft, abzuleiten.

In einem siebten und letzten Schritt definieren wir für jedes der vier Szenarien Schlüsselindikatoren, um die Trendentwicklung verfolgen zu können. Ziel dieses Schrittes ist es, zu jedem Zeitpunkt einschätzen zu können, welches Szenario am wahrscheinlichsten eintreten wird, und Verlagerungen von einem Szenario zu einem anderen identifizieren zu können. Dies dient als solide Grundlage für ein langfristiges Monitoring.

Abb. 2 – Siebenstufiger Szenarioprozess

Ansprechpartner

Katrin Rohmann
Public Sector Leader
Deloitte Risk Advisory
Tel: +49 (0)30 25468 127
krohmann@deloitte.de

Dr. Florian Klein
Head of the Center for the Long View
Monitor Deloitte
Tel: +49 (0)69 9713 7386
fklein@deloitte.de

Annina Lux
Center for the Long View
Deloitte Risk Advisory
Tel: +49 (0)30 25468 5131
anlux@deloitte.de

Besonderer Dank gilt Knut Schönfelder und André Roosen für ihren Beitrag.

Deloitte.

Stand 09/2018