Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Informatiksteuerungsorgan des Bundes ISB
Koordinationsstelle NCS

Forschung zu Cyber-Risiken in der Schweiz

Expertenbericht 2017 zur Identifikation der wichtigsten Forschungsthemen

Publikation November 2017

Autoren Isabelle Augsburger-Bucheli, Endre Bangerter, Luca Brunoni, Srdjan Capkun, Eoghan Casey, Jacques De Werra, Myriam Dunn Cavelty, Martin Eling, Sébastian Fanti, Solange Ghernaouti, David-Olivier Jaquet-Chiffelle, Markus Kummer, Vincent Lenders, Gustav Lindstrom, Martin Gwerder, Rolf Oppliger, Evelyne Studer, Manuel Suter

Mandat Staatssekretariat für Bildung, Forschung und Innovation SBFI
Informatiksteuerungsorgan des Bundes ISB

Verantwortlich für die Publikation Eidgenössisches Finanzdepartement EFD

Informatiksteuerungsorgan des Bundes ISB

Schwarztorstrasse 59
CH-3003 Bern

Tel +41 (0)58 462 45 38
E-Mail: info@isb.admin.ch

Inhaltsverzeichnis

1 Einleitung

Cyber-Risiken sind für Staaten, öffentliche Institutionen, Unternehmen und auch für den einzelnen Bürger längst nicht mehr eine mögliche zukünftige Bedrohung. Sie stellt eine Realität dar, welche hohe Kosten verursacht und generell das Vertrauen in die Nutzung neuer Technologien beeinträchtigt. Das Spektrum von Cyber-Risiken reicht heute von der Verunstaltung von Websites über kriminelle Aktivitäten wie Phishing oder Erpressung mittels Denial-of Service Attacken, bis hin zu sehr gezielten Spionageangriffen und Sabotage gegen Staaten, kritische Infrastrukturen und Unternehmen.

Es ist für Hochschulen und andere Forschungseinrichtungen angesichts der raschen Entwicklung von Cyber-Risiken keine einfache Aufgabe, ihre Forschungstätigkeit so auszurichten, dass sie zu einem besseren Verständnis der Problematik beitragen. Zwar haben viele Hochschulen die Wichtigkeit des Themas erkannt und ihre Forschung in diesem Bereich ausgebaut, aber es muss dennoch festgestellt werden, dass das notwendige spezialisierte Wissen in vielen Bereichen noch nicht ausreichend produziert wird. Dies ist nicht nur auf die hohe Dynamik im Bereich Cyber-Risiken zurückzuführen, sondern auch auf die Schwierigkeit, einem stark interdisziplinären Thema wie den Cyber-Risiken gerecht zu werden. Traditionell wurden Fragen mit Bezug zu Cyber-Risiken in erster Linie in den Computerwissenschaften untersucht. Diese technische Forschung ist nach wie vor wichtig für das Verständnis der Problematik. Technische Erkenntnisse zu Cyber-Risiken alleine sind aber nicht ausreichend, um dem Thema in der Gesamtheit gerecht zu werden. Es ist ebenso wichtig, zu verstehen, welche wirtschaftliche und politische Anreize zur starken Verbreitung von Cyber-Risiken führen, wie die Gesellschaft im Umgang mit Cyber-Risiken geschult werden kann und welche rechtlichen Schritte unternommen werden können, um das Problem einzudämmen.

Für die stark disziplinär gegliederte Forschung an Hochschulen ist der Umgang mit neuen, disziplinübergreifenden Themen eine Herausforderung. Zum einen mangelt es oft an einem gemeinsamen Verständnis des Themas, zum anderen setzt die Forschungspolitik noch wenig Anreize für interdisziplinäre Forschung. Für die Gesellschaft, die Wirtschaft und den Staat ist es aber von grosser Bedeutung, dass in allen verschiedenen Fachrichtungen die vorhandenen Kompetenzen weiter ausgebaut und gemeinsam mit dem Wissen aus anderen Disziplinen genutzt werden, so dass die Forschung zu einem besseren Verständnis von Cyber-Risiken beitragen kann.

Der vorliegende Bericht möchte dazu einen Beitrag leisten. Er zeigt jene möglichen Forschungsthemen auf, die einer interdisziplinär zusammengesetzten Expertengruppe aus der Schweizer Hochschullandschaft als besonders relevant erschienen sind. Die Experten haben das jeweilige Thema kurz beschrieben und anschliessend wichtige Forschungsfelder und mögliche Forschungsfragen identifiziert. Damit soll nicht nur den Forschern in den verschiedenen Disziplinen aufgezeigt werden, wo mögliche interessante Forschungsfragen im Bereich Cyber-Risiken liegen, sondern auch das gemeinsame Verständnis für relevante interdisziplinäre Forschung gefördert werden. Nicht zuletzt soll der Bericht der Forschungspolitik Antrieb geben, interdisziplinäre Forschungsprojekte im Bereich Cyber-Risiken künftig gezielt zu fördern.

2 Auftrag, Ziele und Vorgehen

Vor der Präsentation der identifizierten Forschungsthemen und -fragen, soll in diesem Kapitel dargelegt werden, in welchem Kontext der vorliegende Expertenbericht entstanden ist, welche Ziele er verfolgt, wie er erarbeitet wurde und worin bei der Identifikation der wichtigsten Forschungsthemen im Bereich Cyber-Risiken besondere Herausforderungen bestanden.

2.1 Kontext

2.1.1 Nationaler Kontext: Strategien und politische Vorgaben

Das Projekt zur Erstellung des vorliegenden Berichts ist im Rahmen der Umsetzung der **«Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)»** entstanden. Diese Strategie misst der Kompetenzbildung eine grosse Bedeutung bei. Im Handlungsfeld 1 definiert die Strategie folgende Massnahme:

> *«Neue Risiken im Zusammenhang mit der Cyber-Problematik sollen erforscht werden, damit Entscheide in Politik, Wirtschaft und Forschung frühzeitig und informiert getroffen werden können. Die Forschung fokussiert auf technologische, gesellschaftliche, politische und wirtschaftliche Tendenzen, die sich auf Cyber-Risiken auswirken können.»*

Dem Staatssekretariat für Forschung Bildung und Innovation (SBFI) wurde zusammen mit der Koordinationsstelle für die Umsetzung der NCS die Aufgabe übertragen, diese Massnahme auszuführen. Gemeinsam mit weiteren an Forschung im Bereich Cyber-Risiken interessierten Bundesstellen wurde erkannt, dass es zunächst wichtig ist, mit Hilfe von Experten die wichtigsten Forschungsthemen zu identifizieren. Der vorliegende Bericht ist das Resultat dieser Arbeiten.

Neben der NCS sind aber weitere Strategien und Programme des Bundes relevant für die Forschung im Bereich Cyber-Risiken.

- **Strategie des Bundesrates für eine digitale Schweiz:** Die Strategie des Bundesrates hat unter anderem zum Ziel, die Forschung und Bildung im Bereich der Digitalisierung zu fördern. In der Strategie steht: «*Um den Bedürfnissen unserer digitalen Gesellschaft und Wirtschaft gerecht zu werden […] sollen, unter Beachtung der Kompetenzverteilung sowie der Hochschulautonomie, neue Aus- und Weiterbildungsangebote, Lehrstühle an Hochschulen und Forschungszentren gezielt gefördert werden. Ziel ist es, spezifische Kompetenzen in den Bereichen «Data Analytics», «Data Driven Innovation», künstliche Intelligenz, Robotik und «Internet of Things» aufzubauen. Auch der Erforschung der Folgen und gesellschaftlichen Auswirkungen dieser Technologien ist im Sinne einer Technologiefolgenabschätzung Beachtung zu schenken.»*

- **Nationale Strategie zum Schutz kritischer Infrastrukturen:** Eines der Ziele der Strategie ist es, wissenschaftlich fundierte Grundlagen für den integralen Schutz kritischer Infrastrukturen zu schaffen. Im Rahmen der Strategie sollen deshalb «Technologieentwicklungen oder Umwelt- und Umfeldentwicklungen verfolgt werden, die zu neuen Risiken führen können».

2.1.2 Internationaler Kontext: Forschungsagenden anderer Staaten und internationaler Organisationen

Verschiedene Länder haben bereits Forschungsstrategien, -programme oder -agenden zum Thema Cyber-Risiken publiziert. Folgende neuere Beispiele zeigen auf, welche Themen andere Länder im Bereich Cyber-Risiken als besonders relevant betrachten:

- Deutschland: «Selbstbestimmt und sicher in der digitalen Welt 2015-2020», Forschungsrahmenprogramm der Bundesregierung, veröffentlicht Januar 2016.
- Niederlande: «National Cyber Security Research Agenda II», Bericht einer akademischen Expertengruppe im Auftrag der Regierung, veröffentlicht 2014.
- USA: «Federal Cybersecurity Research and Development Strategic Plan», National Science and Technology Council, veröffentlicht 2016.

Auf der Ebene der EU gibt es ebenfalls verschiedene Projekte, welche Forschung zu Cyber-Risiken fördern sollen. Besonders relevant für die Identifikation von Forschungsthemen sind folgende zwei Projekte:

- Europäische Agentur für Netz- und Informationssicherheit (ENISA): «Cybersecurity Strategic Research Agenda», veröffentlicht 2015.
- Cyber-Road-Projekt der Europäischen Kommission: ein Projekt zur Auflistung aller relevanten Forschung im Bereich Cyber-Kriminalität, laufend.

2.2 Ziele

Ausgehend vom Auftrag aus der NCS und dem beschriebenen Kontext dient der vorliegende Bericht drei Zielen:

1) **Identifikation der Forschung in den Fachdisziplinen:** Indem relevante Forschungsthemen und -fragen zusammengestellt werden, sollen Forscher aus den betreffenden Fachdisziplinen ermuntert werden, entsprechende Forschungsprojekte in Angriff zu nehmen. Der Forschungsbericht soll für Professoren, Forschende und Studenten Inspiration und Motivation sein, sich mit einem der vielfältigen Aspekte von Cyber-Risiken auseinanderzusetzen.
2) **Motivation für interdisziplinäre Forschung:** Die Auflistung von Forschungsfragen aus verschiedenen Disziplinen soll dazu beitragen, ein gemeinsames Verständnis für das Thema Cyber-Risiken zu schaffen und damit interdisziplinäre Forschung befördern. Weil der Bericht das Thema aus verschiedenen Perspektiven aufgreift, hilft er den Fachspezialisten zu verstehen, in welchen anderen Disziplinen ähnliche Fragestellungen untersucht werden und wo eine interdisziplinäre Zusammenarbeit möglich und sinnvoll ist.
3) **Sensibilisierung der Forschungspolitik für das Thema Cyber-Risiken:** Weil das Thema einen ausgeprägten interdisziplinären Charakter hat, muss jede Disziplin für sich erfassen, wo und weshalb Forschung in diesem Bereich relevant ist. Der Bericht versucht, ein Gesamtbild zu vermitteln, um so der Politik zu verdeutlichen, dass zur Erforschung von Cyber-Risiken ein breiter und wenn möglich interdisziplinärer Ansatz nötig ist und die Forschung auch in diesem Sinne gefördert werden sollte.

Es ist allen Beteiligten bewusst, dass der Bericht nur ein erster Schritt zur Erreichung der Ziele sein kann. Es ist jedoch wichtig, diesen ersten Schritt zu machen, um damit mehr Kohärenz in Forschung zu Cyber-Risiken in der Schweiz zu erreichen und das Netzwerk der Forschenden aus den verschiedenen Disziplinen zu stärken.

2.3 Vorgehen

Um den Auftrag aus der NCS zur Forschungsförderung zu erfüllen, wurde unter der Leitung des Staatssekretariats für Bildung Forschung und Innovation (SBFI) ein interdepartementales Komitee errichtet, welches die Forschungsförderung im Bereich Cyber-Risiken seitens des Bundes koordiniert. Den Mitgliedern des Komitees wurde schnell klar, dass zur Identifikation der wichtigsten Forschungsthemen Experten aus der Schweizer Hochschullandschaft beigezogen werden müssen. Die grosse Mehrheit der angefragten Experten war bereit, an dem Projekt mitzuarbeiten. Die Expertengruppe besteht aus folgenden 16 Personen:

- Prof. Dr. Isabelle Augsburger-Bucheli, Haute école de gestion Arc, Neuchâtel (HES-SO)
- Prof. Dr. Endre Bangerter, Berner Fachhochschule
- Luca Brunoni (LL.M / MA), Haute école de gestion Arc, Neuchâtel (HES-SO)
- Prof. Dr. Srdjan Capkun, ETH Zürich
- Prof. Eoghan Casey, Université de Lausanne
- Prof. Dr. Jacques De Werra, Université de Genève
- Dr. Myriam Dunn Cavelty, ETH Zürich
- Prof. Dr. Martin Eling, Universität St. Gallen
- Sébastian Fanti (Rechtsanwalt), Canton du Valais
- Prof. Dr. Solange Ghernaouti, Université de Lausanne
- Prof. Martin Gwerder, Fachhochschule Nordwestschweiz
- Prof. Dr. David-Olivier Jaquet-Chiffelle, Université de Lausanne
- Markus Kummer (Diplomat), ICANN Board of Directors
- Dr. Gustav Lindstrom, The Geneva Centre for Security Policy
- Prof. Dr. Rolf Oppliger, Universität Zürich
- Evelyne Studer, Master of Laws, University of Geneva

Bei der Zusammensetzung dieser Expertengruppe wurde darauf geachtet, dass unterschiedliche Disziplinen vertreten sind und sowohl Universitäten als auch Fachhochschulen repräsentiert sind. Weiter wurde auf eine ausgeglichene Vertretung der Sprachgemeinschaften und der Geschlechter geachtet. An vier gemeinsamen Sitzungen im Jahr 2016 haben sich die Experten zunächst auf die wichtigsten Forschungsthemen geeinigt, diese dann ausgearbeitet und einem gegenseitigen Review unterzogen.

3 Forschungsthemen

Die umfassende Digitalisierung der Gesellschaft und Wirtschaft führt dazu, dass Cyber-Risiken ein wichtiges Thema in vielen verschiedenen Bereichen geworden sind. Entsprechend gibt es unzählige mögliche Forschungsthemen in diesem Gebiet. Daraus die wichtigsten Themen auszuwählen und diese nachvollziehbar zu klassifizieren, war die schwierigste Herausforderung für die Expertengruppe. Die hier vorgestellten Themen sind das Ergebnis offener Diskussionen innerhalb der interdisziplinären Gruppe. Die Auflistung erhebt keinerlei Anspruch auf Vollständigkeit und ist nicht als abschliessend zu verstehen. Sie soll aber einen Überblick zu interessanten und relevanten Themen vermitteln und so als Inspiration für Forschende und als Information für Entscheidungsträger aus Politik und Wirtschaft dienen.

Im ersten Abschnitt dieses Kapitels wird die Methode zur Strukturierung der Forschungsthemen vorgestellt. Es ist für das Verständnis des Berichts wichtig zu wissen, warum welche Themen in welchen Unterkapiteln ausgeführt werden. Die nächsten Abschnitte enthalten die Auflistung der Forschungsthemen. Zunächst werden in einem ersten Teil des Inventars generelle Forschungsthemen beschrieben, dann folgt ein zweiter Teil mit Forschungsthemen zu spezifischen Anwendungen und Technologien.

3.1 Klassifizierung der Forschungsthemen

Es gibt viele verschiedene Möglichkeiten, Forschungsthemen im Bereich Cyber-Risiken zu klassifizieren. Die Expertengruppe hat diese erörtert und sich darauf geeinigt, die Auflistung in zwei Teile zu gliedern. Ein erster Teil beinhaltet die generellen Forschungsbereiche, worunter alle generellen und übergreifenden Forschungsbereiche fallen (wie zum Beispiel Forschung zu Risikomanagement oder Forschung zum Schutz von Daten und Privatsphäre). In einem zweiten Teil – den Fokusthemen – werden Themen zu spezifischen Technologien oder Anwendungen aufgeführt, welche von der Expertengruppe als besonders relevant im Hinblick auf Cyber-Risiken identifiziert wurden. Beispiele für solche Fokusthemen sind Forschung zu FinTech oder Cloud Computing.

Folgende drei Gründe führten zur gewählten Systematik:

1) **Forschung zu Cyber-Risiken ist disziplinenübergreifend**
   Typischerweise würde man eine Übersicht zu Forschungsthemen entlang den traditionellen akademischen Disziplinen strukturieren. Im Bereich der Cyber-Risiken würde das jedoch bedeuten, künstliche Abgrenzungen einzuführen. Cyber-Risiken sind ein vielfältiges Phänomen betreffen gleichzeitig verschiedenste Bereiche, so dass disziplinenübergreifenden Ansätzen nötig sind, um sie zu analysieren. Beispielsweise sind viele technologische Forschungsthemen direkt verbunden mit rechtlichen Fragestellungen und umgekehrt ist dies genauso der Fall. Die Expertengruppe entschied deshalb, sich bei der Auflistung der Forschungsthemen nicht in erster Linie an den akademischen Disziplinen zu orientieren.
2) **Unvermeidbare Überschneidungen zwischen den Themen**
   Eine weitere Möglichkeit zur Strukturierung wäre die Klassifizierung nach Anwendungsfeldern und Technologien. Diese Wahl hätte aber zu zahlreichen Wiederholungen geführt, weil ähnliche Themen in vielen Anwendungsfeldern und Technologien von Bedeutung sind. Auch bei einer Strukturierung nach Themenfeldern bleiben Überschneidungen bestehen, sie können jedoch direkt in den Kapiteln transparent gemacht werden, wodurch nachvollziehbar bleibt, wo welche Themen behandelt werden.
3) **Verschiedene Spezifizierungsgrade: Forschungsbereiche vs. Fokusthemen**
   Neue Forschungsthemen im Bereich Cyber-Risiken entstehen üblicherweise dann, wenn neue Technologien entwickelt worden sind, wenn bestehende Technologien in neuen Anwendungsfeldern zum Einsatz kommen oder wenn neue Anwendungen dazu führen, dass bestehende Technologien auf neue Art und Weise genutzt werden. Beispiele für solche Entwicklungen sind Cloud Computing, das Internet der Dinge (Internet of Things) oder Big Data Analytics. Für eine Übersicht zu Forschungsthemen müssen solche Entwicklungen deshalb berücksichtigt werden. Die Expertengruppe entschied, diese wichtigen Entwicklungen und die spezifischen Forschungsfragen, die sich aus ihnen ergeben, in separaten Kapiteln als Fokusthemen aufzunehmen.

3.2 Forschungsbereiche

Die Expertengruppe hat zehn generelle Forschungsbereiche identifiziert:

1) Schutz der Privatsphäre und Personendaten
2) Sicherheit von Rechnernetzen
3) Rechtliche Rahmenbedingungen
4) Prävention und Strafverfolgung von Cyber-Kriminalität
5) Vorfallerkennung, Vorfallbewältigung, digitale Forensik
6) Management von Cyber-Risiken
7) Ökonomie der Cyber-Sicherheit
8) Sicherheit von Cyber-Physischen Systemen
9) Cyber-Sicherheit in internationalen Beziehungen

10) Menschliche und soziale Faktoren der Cyber-Sicherheit

Alle diese Themen werden im Folgenden in je einem separaten Unterkapitel verfasst. Jedes Unterkapitel beginnt mit einer generellen Beschreibung des Forschungsbereiches, gefolgt von einer Beschreibung der Relevanz des Forschungsbereiches und einer Zusammenstellung der wichtigsten Schnittstellen zu anderen Bereichen. Schliesslich werden mögliche Forschungsthemen aus allen möglichen Disziplinen im betreffenden Gebiet aufgeführt und Beispiele für interessante Forschungsfragen gegeben. Weder die Auflistung der Themen noch jene der Fragen ist als abschliessend oder vollständig zu verstehen. Sie sollen jedoch einen Eindruck über mögliche Forschungsprojekte vermitteln.

3.2.1 Schutz der Privatsphäre und Personendaten

Beschreibung des Forschungsbereiches:

Die stark gestiegenen Kapazitäten zur Sammlung, Aufbewahrung und Analyse von Daten stellen neue Herausforderungen an den Schutz der Privatsphäre und der Daten selber. Durch die Verwendung von Diensten im Internet teilen die Nutzer eine grosse Menge von Daten – manchmal bewusst (zum Beispiel über die sozialen Medien), häufig aber auch unbewusst, weil ihre Daten stillschweigend gesammelt, aufbewahrt und für kommerzielle Zwecke ausgewertet werden. Grosse Firmen und teilweise auch Staaten haben die Möglichkeit, das Verhalten von Nutzern weitgehend zu überwachen. Verschärft wird die Situation dadurch, dass Daten nicht mehr verschwinden und das «Recht auf Vergessen» – also die Löschung von Daten und Informationen – dadurch für die Nutzer kaum mehr durchsetzbar ist.

Forschung zu den Themen Datenschutz und Privatsphäre ist für verschiedenste Disziplinen relevant. Hier beschrieben sind Forschungsthemen der Computerwissenschaften und der Kryptografie. In diesen Disziplinen besteht die zentrale Herausforderung darin, dass Daten immer stärker dezentral erfasst und verwaltet werden. Der physische Schutz von Systemen reicht damit nicht aus, um einen angemessenen Schutz der Privatsphäre zu gewährleisten. Er muss durch einen logischen Schutz mit kryptologischen Verfahren zur Authentifizierung, Zugriffskontrolle und Verwendungskontrolle abgelöst werden.

Relevanz:

Der Schutz der Privatsphäre und der Daten kommt durch die fortschreitende Digitalisierung zunehmend unter Druck. Die oft persönlichen Daten können leicht missbräuchlich genutzt werden und die herrschende Intransparenz bei der dezentralen Erfassung und der Verwaltung der Daten beeinträchtigt das Sicherheitsgefühl der Nutzenden. Forschung auf den verschiedenen Ebenen ist daher zwingend nötig, um Lösungen zur Verbesserung der aktuellen Situation aufzuzeigen.

Verwandte Forschungsbereiche

Vorfallbewältigung, Vorfallerkennung, digitale Forensik; Rechtliche Rahmenbedingungen; Strafverfolgung und Prävention von Cyber-Kriminalität; Management von Cyber-Risiken; Sicherheit von Cyber-Physischen Systemen.

Mögliche Forschungsthemen

- **Kryptologische Forschung:** Die Entwicklung von kryptologischen Verfahren zur Sicherung der Anonymität oder der Pseudonymität bleiben ein wichtiges Forschungsgebiet. Sie bilden die Grundlage dafür, dass den Nutzern Alternativen zur Verfügung stehen, um ihre Daten zu schützen. Die Entwicklung von Tor (Netzwerk zur Anonymisierung von Verbindungsdaten) und Anwendungen im E-Voting stützen sich auf diese Technologien.
- **Datenminimierendes Identitätsmanagement:** Bei den heute verwendeten Systemen zur Identifikation der Nutzer werden Zertifikate übermittelt, die viele Informationen über die Nutzenden enthalten (z. B. über PKI-Zertifikate). Um den Datenschutz zu verbessern, sollten neue Methoden der Identifizierung entwickelt werden, welche möglichst wenige Daten über die Nutzenden enthalten.

- **«Privacy by design»:** Bei der Entwicklung neuer Technologien und Anwendungen muss der Schutz der Privatsphäre und der Daten bereits bei der Entwicklung berücksichtigt werden. Die Forschung soll entsprechende Grundlagen erarbeiten und technologischer Möglichkeiten aufzeigen.

Beispiele für Forschungsfragen:

- Welche neuen Technologien können dazu beitragen, dass die Nutzenden die Kontrolle über ihre Daten zurückgewinnen?
- Wie kann die Nachvollziehbarkeit über die Nutzung der Daten sichergestellt werden?
- Welche Bedeutung hat Quantum-Computing für die bestehenden Verschlüsselungstechniken?
- Wie kann der Schutz der Privatsphäre und der Daten beim Design von Systemen besser berücksichtigt werden?
- Welche technischen Standards können im Bereich zum Schutz von Daten entwickelt und angewendet werden?

3.2.2 Sicherheit von Rechnernetzen

Beschreibung des Fokusthemas:

Das Internet hat unsere Gesellschaft in den letzten 30 Jahren revolutioniert. Industrie, Privatpersonen und Regierungen sind dadurch immer abhängiger von einer stets funktionierenden und sicheren Kommunikationsinfrastruktur geworden. Heutige Kommunikationsprotokolle und die Hardware/Software, welche auf den angeschlossenen Rechnersystemen läuft, sind aber sehr fragil und können von bösartigen Akteuren mit einfachen Mitteln missbraucht werden. In der Folge sind Denial-of-Service Angriffe, Datendiebstähle oder Erpressungen gegen Organisationen und Personen tagtäglich zu verzeichnen.
Die Verwundbarkeit der Netze ist in Kombination unserer hohen Abhängigkeit von diesen Infrastrukturen eine zentrale Herausforderung der Cyber-Sicherheit. Die Forschung hat die Aufgabe aufzuzeigen, wie die Resilienz und Robustheit von Rechnernetzen so gestärkt werden kann. Es gilt zu überlegen, welche Bestandteile der Netzewerke mit welchen Methoden sicherer gemacht werden können und welche Komponenten komplett neu entworfen und konzipiert werden müssen.

Relevanz:

Forschung kann einen wichtigen Beitrag zur Entwicklung von resilienten und resistenten Rechnernetzen leisten. Es gilt sowohl neue Netzwerktechnologien zu entwickeln, welche Sicherheit bereits in ihrem Design integriert haben, aber auch Methoden zu finden, um die bestehenden Rechnernetze zu schützen, da die installierten Infrastrukturen nicht von einem Tag auf den anderen ersetzt werden können.

Mögliche Forschungsthemen:

- **Architekturen für sichere Netzwerke:** Die Architektur von Netzwerken muss so organisiert und betrieben werden, dass ein Monitoring des Datenverkehrs gewährleistet ist und ungewollte Aktivität rasch erkannt werden kann. Mit der wachsenden Komplexität von Netzwerken steigen auch die Anforderungen an die Architektur. Forschung soll aufzeigen, welche Lösungen sich für welche Netzwerke eignen und soll innovative Architekturen entwickeln.
- **Absicherung existierender Netzwerkprotokolle:** Viele der heute häufig verwendeten Protokolle verschlüsseln die übertragenen Daten nicht. Dadurch besteht das Risiko, dass Daten von Unbefugten mitgelesen oder gar manipuliert werden. Die Ablösung dieser Protokolle wird aber auf Grund ihrer weiten Verbreitung noch lange dauern. Es braucht deshalb Forschung zu technischen Lösungen zur Absicherung dieser Protokolle.
- **Neue sichere Netzwerkprotokolle:** Die Entwicklung neuer, sicherer Netzwerkprotokolle ist ein wichtiger Beitrag der Forschung zur Verbesserung der Sicherheit, der Datenübertragung innerhalb sowie zwischen Netzwerken.
- **Minimierung der Hardware-Unterstützung:** durch Abstraktion und Virtualisierung der Hardware kann das Problem der Sicherheit der Endgeräte teilweise entschärft

werden. Die Minimierung der Hardware-Abhängigkeit kann deshalb ein möglicher Weg zu einer Stärkung der Netzwerksicherheit sein. Es gilt, die Möglichkeiten und Grenzen dieses Ansatzes weiter zu analysieren.

- **Sichere Integration von Applikationen:** Zur Netzwerksicherheit gehört auch die Frage, wie die verschiedenen Applikationen sicher integriert werden können. Dabei kann Forschung neue Methoden entwickeln zur Validierung und zum Monitoring der durch Applikationen übertragenen Daten sowie zur Beschränkung der Nutzung und zur Einschränkung der Nutzergruppen..

Beispiele für Forschungsfragen:

- Wie können unsere Kommunikationsinfrastrukturen robuster gegen Denial-of-Service Angriffe gemacht werden?
- Wie lassen sich Software/Hardware für Anwendungen und Systeme auf Schwachstellen prüfen, bzw. verifizieren?
- Wie kann man Software für Anwendungen und Kommunikationsinfrastruktur sicher entwickeln?
- Wie lassen sich Computernetze gegen Malware und Datendiebstahl besser schützen?
- Wie lassen sich Hackerangriffe schneller detektieren?

3.2.3 Rechtliche Rahmenbedingungen

Beschreibung des Foschungsbereichs:

Rechtliche Fragen zur Regulierung der digitalen Welt gewinnen zunehmend an Bedeutung und stellen die Gesetzgeber vor schwierige Herausforderungen. Die Komplexität und Vielschichtigkeit der Themen im Bereich Cyber-Sicherheit machen es schwierig, aus Sicht Gesetztgebung Entwicklungen zu antizipieren und neu aufkommende Themen rechtzeitig zu erkennen und umfassend abzudecken.

Forschung kann dazu jedoch einen wichtigen Beitrag leisten, indem grundlegende Daten erfasst und analysiert werden. Sie ermöglicht ein tieferes Verständnis der bestehenden Herausforderungen und der künftigen Entwicklungen. Daraus abgeleitet kann festgestellt werden, wie bestehende Gesetze verbessert werden können, wo es nötig ist, neue Gesetze zu erlassen und welche Wirkung von Änderungen der Rechtsgrundlagen zu erwarten ist. Ziel der Forschungsbemühungen sollte die Entwicklung von geeigneten gesetzlichen Rahmenbedingungen im Bereich der Cyber-Risiken sein.

Relevanz:

Die rechtlichen Rahmenbedingungen beeinflussen den Umgang mit Cyber-Risiken direkt. Fehlende oder mangelhafte Rechtsgrundlagen und Schwierigkeiten bei der Anwendung bestehender Gesetze auf Fragen im Bereich der Cyber-Risiken führen zu Rechtsunsicherheit. Forschung zu den Möglichkeiten der Gesetzgebung ist deshalb wichtig. Eine Analyse des Handlungsbedarfs im Bereich der Gesetzgebung ist zudem von grosser praktischer Relevanz.

Verwandte Forschungsbereiche:

Privatsphäre und Datenschutz (1); Prävention und Strafverfolgung von Cyber-Kriminalität (3); Management von Cyber-Risiken (5); Cyber-Sicherheit in internationalen Beziehungen.

Mögliche Forschungsthemen:

- **Rechtliche Aspekte zum Schutz der Privatsphäre und zum Datenschutz:** Das automatische Sammeln von Daten ist zu einem Kerngeschäft vieler Business-Modelle geworden. Die rechtlichen Rahmenbedingungen dafür sind jedoch unzureichend entwickelt. Es muss analysiert werden, wie die Gesetzesgrundlagen ausgestaltet werden müssen, um Transparenz und Rechenschaftspflichten zu stärken.
- **Rechtsgrundlagen für staatliches Handeln:** Möglichkeiten und Grenzen staatlicher Reaktionen auf Cyber-Angriffe sind ein vieldiskutiertes Thema. Im Fokus stehen Fragen nach den rechtlichen Voraussetzungen und Konsequenzen staatlicher Überwachungstätigkeiten oder aktiver staatlicher Gegenmassnahmen im Fall von Cyber-Spionage. Im Schweizerischen Kontext sind das neue Nachrichtendienstgesetz (NDG)

und das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) zu analysieren.

- **Haftungsverteilung**: In Bezug auf Cyber-Sicherheit stellen sich viele komplexe Fragen hinsichtlich der Haftungsverteilung. Es muss untersucht werden, wer für welche Bereiche in der Cyber-Sicherheit haften soll (was im Zivil- oder im Strafrecht festgehalten werden kann). Dies setzt politische Entscheide über die gewünschten wirtschaftlichen und rechtlichen Anreize für die verschiedenen Akteure voraus. Beispielsweise ist zu klären, inwiefern die Opfer eines Angriffs verantwortlich gemacht werden sollen (insbesondere im Fall von Datendiebstahl), was wiederum zur Frage führt, welche Mindeststandards für die Vorbeugung gelten sollten.
- **(Alternative) Streitbeilegungsmethoden:** Die Schweiz hat eine lange Tradition in der Streitschlichtung. Sie könnte für Streitbeilegungsverfahren in Bezug auf Fragen des Daten- und Persönlichkeitsschutzes eine wichtige Rolle übernehmen. Die Forschung kann dazu Ideen und Vorschläge für globale Streitbeilegungsmethoden liefern.

Beispiele für Forschungsfragen:

- Was sind die rechtlichen Voraussetzungen fürdie Einführung einer Meldepflicht von Cyber-Vorfällen? Welches wären die Konsequenzen einer solchen Meldepflicht?
- Welche gesetzlichen Grundlagen bestehen für Vorgaben im Bereich der Verschlüsselungstechnologien?
- Welche rechtlichen Anreize sind möglich, damit die Sicherheit in der Softwareentwicklung künftig besser berücksichtigt wird?
- Wie sollten Haftungsfragen zwischen Nutzern, Produzenten und Drittparteien verteilt sein?
- Sollten Produzenten von Software zu Transparenz über mögliche Sicherheitslücken verpflichtet werden?
- Welche Mittel sind bei der Abwehr von Cyber-Angriffen legal? Wo sind die Grenzen?

3.2.4 Prävention und Strafverfolgung von Cyber-Kriminalität

Beschreibung des Foschungsbereichs:

Wir leben in einer Ära, in der das Präfix «cyber» in der Kriminalität omnipräsent geworden ist. Computer und Netzwerke führen zu neuen Vorgehensweisen von Kriminellen und verändern demensprechend auch die Prozesse der Strafverfolgung. Neue Technologien eröffnen ständig neue Möglichkeiten für Cyber-Kriminelle. Es bleibt aus rechtlicher Sicht und insbesondere zur Wahrung der Rechtssicherheit entscheidend, dass kriminelle Taten auch in diesem neuen Umfeld untersucht, verfolgt und bestraft werden.

Solide rechtliche Rahmenbedingungen sind eine erste Voraussetzung für die Reduktion von Cyber-Kriminalität. Es braucht aber ebenso eine gute Präventionsstrategie. Forschung aus den Disziplinen der Psychologie, Anthropologie, Kriminologie oder Soziologie kann dazu beitragen, massgeschneiderte Präventionskampagnen für verschiedene Bevölkerungsgruppen zu entwickeln.

Schliesslich ist in der Strafverfolgung die Zusammenarbeit entscheidend. Diese umfasst den Informationsaustausch zwischen Opfern und Behörden, aber auch die Kooperation auf internationaler Ebene.

Relevanz:

Für eine effiziente Prävention und Verfolgung von Cyber-Kriminalität braucht es konstante Anstrengungen von allen Seiten. Dazu braucht es auch wertvolle Einsichten aus der Forschung.

Verwandte Forschungsbereiche:

Privatsphäre und Datenschutz; Rechtliche Rahmenbedingungen; Vorfallbewältigung und Forensik; Management von Cyber-Risiken; Cyber-Sicherheit in internationalen Beziehungen, menschliche Faktoren der Cyber-Sicherheit.

Mögliche Forschungsthemen:

- **Aktualisierung des Strafrechts:** Viele Straftaten im Cyber-Raum fallen unter bereits existierende Artikel des Strafrechts. Einige finden jedoch in einem Graubereich statt oder nutzen bewusst Gesetzeslücken aus. Oft kann es genügen, die Interpretation bestehenden Rechts auf diese Fälle auszuweiten. Ein Beispiel ist der Identitätsdiebstahl, welcher nicht direkt im Strafrecht adressiert wird, aber dennoch durch bestehende Artikel strafbar ist. In anderen Fällen wird ein solches Vorgehen nicht genügen. Es bleibt darum zu klären, wann und unter welcher Bedingung neue Gesetzesartikel nötig sind.
- **Anpassungen der Strafverfolgung:** Behörden müssen über Mittel verfügen, um Straftaten von Cyber-Kriminellen effizient und zeitnah zu untersuchen und zu verfolgen. Zugleich muss eine Balance gefunden werden zwischen dieser Anforderung und den individuellen Freiheiten der Bürger. Diese Herausforderung stellt sich besonders bei der Beweisaufnahme und -sicherung in der digitalen Welt. Entsprechend muss untersucht werden, welche Anpassungen in den Prozessen der Strafverfolgung nötig sind.
- **Internationale Kooperation:** Cyber-Kriminalität kennt keine Grenzen. Aus diesem Grund ist internationale Zusammenarbeit bei der Strafverfolgung essentiell. Es gilt zu untersuchen, wie diese Zusammenarbeit möglichst effizient gestaltet werden kann. So Ein wichtiges Beispiel für einen Untersuchungsgegenstand ist die Europäische Konvention zu Cyber-Kriminalität, welche vor 10 Jahren unterzeichnet worden ist. Aufgrund dieses Beispiels kann untersucht werden, welche wie die internationale Zusammenarbeit funktioniert und wie sie künftig gestaltet werden sollte. Ebenfalls interessant ist der Vergleich der Massnahmen anderer Länder im Bereich Cyber-Kriminalität, um so eine breite Übersicht über mögliche Aktivitäten gegen Cyber-Kriminalität zu gewinnen.
- **Darknets:** Die isolierten Netzwerke, welche durch Peer-to-Peer-Verbindungen aufgebaut werden, bieten einen attraktiven Markt für kriminelle Aktivitäten, da sie für Behörden der Strafverfolgung schlecht zugänglich sind und die Anonymität der Akteure in hohem Masse geschützt bleibt. Als Forschungsthema ist zu untersuchen, welchen Einfluss die Darknets auf kriminelle Aktivitäten haben und wie es für Strafverfolger möglich sein kann, kriminelle Aktivitäten in diesen Netzwerken zu verfolgen.

Beispiele für Forschungsfragen:

- Sollten neue Formen der Kriminalität, wie beispielsweise Identitätsdiebstahl mittels neuen Tatbeständen, geregelt werden oder genügen die bestehenden Grundlagen?
- Sind die bestehenden Prozesse der Strafverfolgung geeignet für die Aufklärung von Cyber-Kriminalität?
- Wie effektiv ist die heutige internationale Zusammenarbeit im Kampf gegen Cyber-Kriminalität?
- Welche Möglichkeiten werden neue Technologien für Kriminelle schaffen?
- Welche Mittel verwenden andere Staaten gegen Cyber-Krimielle?

3.2.5 Vorfallerkennung, Vorfallbewältigung, digitale Forensik

Beschreibung des Foschungsbereichs:

Die wachsende Spezialisierung und Komplexität von Cyber-Angriffen machen die Erkennung und Analyse von Vorfällen zunehmend schwierig. Moderne Angriffsmethoden und Malware sind so gestaltet, dass sie Sicherheitsmechanismen umgehen, inklusive Antiviren-Programme und Vorfallerkennungssysteme. Sogar Organisationen mit einer hohen Sensibilität für die Sicherheit, wie Banken oder staatliche Institutionen, müssen immer wieder erfolgreiche Angriffe verzeichnen.
Vorfälle zu entdecken und rechtzeitig und effektiv zu bewältigen ist deshalb von entscheidender Bedeutung für die Minderung von Cyber-Risiken. Entsprechend hat sich die Cyber-Sicherheitsforschung auch von ihrem ursprünglichen Fokus auf Abwehr- und Schutzmassnahmen gelöst und entwickelt Methoden der Vorfallerkennung, -bewältigung und –

analyse. Diese Methoden leisten auch einen wichtigen Beitrag zur Prävention, da Informationen über die Identität und das Vorgehen von Tätern entscheidend dafür sind, die richtigen Schutzmassnahmen zu ergreifen.
Digitale Forensik und Vorfallanalyse sind sehr ähnliche Disziplinen. Traditionell beschäftigt sich digitale Forensik mit Fällen, in welchen der Angreifer kriminelle Taten in der physischen Welt begonnen hat. Der Fokus solcher Untersuchungen richtet sich auf die Auswertung von Datenträgern. Die Vorfallanalyse hingegen beschäftigt sich mit Angriffen auf IT-Infrastrukturen. Der Tatort ist die IT-Infrastruktur und entsprechend sind die auszuwertenden Daten technischer Natur, zum Beispiel Log-Daten, Netzwerkverkehr, bösartiger Code, Systemmodifizierungen usw.
Gemeinsam ist beiden Disziplinen, dass sie ein tiefes Verständnis der Technologien verlangen. Die wichtigste Forschungsherausforderung besteht in beiden Disziplinen darin, grosse Mengen an Daten aus oft verschiedenen Quellen zu analysieren und zu kontextualisieren. Besonders wichtig ist Forschung zu digitaler Forensik und Vorfallanalyse in Spezialgebieten wie bei mobilen Geräten, Netzwerken, Datenspeichern und Gesundheitssystemen.
Viele illegale Märkte und Aktivitäten haben jetzt ein digitales Äquivalent: gefälschte Dokumente, Medikamente oder Uhren und ähnliches werden im Darknet angeboten. Sie haben direkte negative Auswirkungen auf den Grenzschutz, die Gesundheitsversorgung oder schwächen die Wettbewerbsfähigkeit der Schweizer Wirtschaft. Aus diesem Grund braucht es Techniken, um diesen Phänomenen zu begegnen indem Methoden der digitalen Forensik mit Methoden der Open Source Intelligence (OSINT), die von Sozial- und Humanwissenschaften stark gestützt sind, kombiniert werden.

Relevanz:

Die Relevanz ergibt sich aus der zunehmenden Digitalisierung der Gesellschaft. Cyber-Angriffe sind zu einem ernsthaften Problem geworden und werden immer ausgefeilter in den Methoden. Gleichzeitig ist die Forschung und Lehre im Bereich der Vorfallbewältigung und -analyse in der Schweiz noch nicht gut entwickelt, obwohl die Schweiz ein attraktives Ziel für Cyber-Kriminelle darstellt.

Verwandte Forschungsbereiche:

Schutz der Privatsphäre und Datenschutz; Big Data; Cloud Computing; rechtliche Grundlagen; Management von Cyber-Risiken.

Mögliche Forschungsthemen:

- **Automatisierung:** Eine (Teil-)Automatisierung der Aktivitäten zur Vorfallerkennung und -analyse kann die Prozesse entscheidend beschleunigen. Sie kann auch zu unmittelbarer Erkennung von Angriffen und zu neuen Sicherheitssystemen führen, die eine anpassungsfähige Abwehr von neuen Attacken oder Varianten von Malware ermöglichen.
- **Konsolidierung, Korrelation und Präsentation von Daten:** Wie können Vorfälle in einer geeigneten Weise erfasst und beschrieben werden, die über die reine Sammlung von herkömmlichen Indikatoren wie den Indicators of Compromise hinausgehen? Beispiele für Lösungen können analytische Methoden und Systeme sein, die Attacken auf Grund von Verhaltensmustern detektieren, nicht nur auf der Basis von einzelnen Indikatoren. Ebenso von Interesse können Systeme sein, die nicht offensichtliche Verbindungen zwischen Angriffen analysieren.
- **Vorhandenes Wissen teilen und nutzen:** Die rasche Entwicklung der Technologien und der Angriffsmethoden machen es schwierig, alle neuen forensischen Möglichkeiten zu kennen oder die schon bekannten wieder zu finden. Forschung kann dazu beitragen, eine Systematik zur Erfassung von neuem und zur Aufbewahrung von bestehendem Wissen zu entwickeln.
- **Integration von digitaler Forensik in die Prozesse der Strafverfolgung und in nachrichtendienstliche Analysen:** Die Anwendung von hochentwickelten analytischen Methoden, um Erkenntnisse über Angreifer zu gewinnen muss weiter ausgebaut werden. Mittels digitaler Forensik kann es gelingen, Angreifer auf Grund ihrer digitalen Spuren und mit Hilfe von Verhaltensprofilen zu identifizieren.

- **Forensik und Vorfallanalyse bei neuen Technologien:** Es braucht neue Methoden, um digitale Forensik bei neuen Technologien - wie dem Internet der Dinge - anzuwenden.
- **Monitoring**: Viele Technologien und Aktivitäten von kriminellen können besser verstanden werden, wenn der Austausch der betreffenden Gruppen über Webforen, sozialen Netzwerken oder im Darknet genau verfolgt wird. Das Ausmass der Informationen, die auf verschiedenen Plattformen zur Verfügung stehen, nimmt stetig zu. Entsprechend wichtig ist es, ein systematisches Vorgehen bei der Analyse dieser Informationen zu entwickeln.
- **Identifizierung**: Auf Grund der Verhaltensmuster können Charakteristiken der Angreifer identifiziert werden. Kombiniert mit Methoden der herkömmlichen Forensik kann es so gelingen, die Personen hinter Angriffen zu identifizieren.
- **Visualisierung:** Die Visualisierung grosser Mengen von Informationen ist eine wichtige Herausforderung in der Vorfallanalyse. Sie hilft den Analysten, Muster und Anomalien zu erkennen.

Beispiele für Forschungsfragen:

- Wie können die Taktiken, Vorgehensweisen und Prozesse von Angreifern identifiziert werden?
- Wie können Verhaltensmuster und andere Charakteristiken von Angreifern genutzt werden, um die Täter zu identifizieren?
- Wie können die Analysen von Vorfällen beschleunigt werden? Welche Prozesse können automatisiert werden?
- Wie können wir die Methoden der Vorfallbewältigung und der Forensik nutzen, um das Risiko-Management zu unterstützten?
- Wie kann das Wissen, das aus der Vorfallanalyse gewonnen wird, besser für die Prävention genutzt werden?
- Wie können systematisch und gezielt Informationen aus Online-Foren, sozialen Netzwerken und dem Darknet zu Akteuren und ihren Taktiken gesammelt werden?

3.2.6 Management von Cyber-Risiken

Beschreibung des Forschungsbereichs:

Cyber-Risiken entwickeln sich sehr dynamisch und sind zugleich äusserst komplex. Die Dynamik ergibt sich aus der raschen technologischen Entwicklung, aufgrund derer bestimmte Risiken sehr schnell an Bedeutung gewinnen (oder auch verlieren) können. Die Komplexität ist eine Folge der Vielzahl von Interdependenzen in modernen Systemen, welche es schwierig, wenn nicht gar unmöglich machen, die Konsequenzen von erfolgreichen Angriffen abzuschätzen.

Diese Charakteristiken sind die zentralen Herausforderungen für das Management der Cyber-Risiken. Forschung in diesem Bereich muss sich zunächst mit der Theorie und den Methoden des Risikomanagements im Bereich der Cyber-Risiken auseinandersetzen. Es muss untersucht werden, ob und wie die bestehenden Methoden der Risikoanalyse angepasst werden sollten, um der Dynamik und der Komplexität von Cyber-Risiken gerecht zu werden.

Auf der operativen Ebene braucht es Forschung zu den Instrumenten der Risikoanalyse und des –managements, wie zum Beispiel zu möglichen Bedrohungskarten, Risikomatrizen oder Szenarien basierten Planungen. Solche Forschung soll auch dazu beitragen, Indikatoren zu entwickeln, um sowohl die Risiken selber, als auch die Effektivität von Gegenmassnahmen messbar zu machen.

Schliesslich gehört auch eine strategisch-politische Ebene zum Bereich Management von Cyber-Risiken. Auf dieser Ebene geht es um die Frage, wie Cyber-Risiken im Kollektiv angegangen werden können. Wichtige Themen sind dabei das Potential von Public-Private Partnerships, Grenzen und Möglichkeiten im Informationsaustausch und regulatorische Fragen, wie beispielsweise die Option, eine Meldepflicht bei Vorfällen einzuführen.

Relevanz:

Cyber-Angriffe können nicht vollständig verhindert werden. Es braucht darum ein Risikomanagement, welches hilft, die Lage realistisch einzuschätzen und die richtigen Prioritäten zu setzen. Im Bereich Cyber-Risiken stellen sich an die bewährten Methoden des Risikomanagements neue Herausforderungen. Weil das Risikomanagement den Rahmen für alle Aktionen zum Schutz vor Cyber-Risiken vorgeben soll, ist Forschung in diesem Bereich von grosser Bedeutung.

Verwandte Forschungsbereiche:

Schutz der Privatsphäre und Datenschutz; Rechtliche Rahmenbedingungen; Ökonomie der Cyber-Sicherheit; Menschliche Faktoren der Cyber-Sicherheit.

Mögliche Forschungsthemen:

- **Theorie und Methodik des Risikomanagements:** Weil sich Cyber-Risiken sehr dynamisch entwickeln und äusserst komplex sind, ist es sehr schwierig, ihre Wahrscheinlichkeit und ihr Schadenspotential abzuschätzen. Es braucht daher Forschung zu den Möglichkeiten und Grenzen der bestehenden Ansätze der Risikoanalyse. Es ist zu untersuchen, wie Cyber-Risiken mit anderen Risiken verglichen und in bestehende Risikokataloge integriert werden können.
- **Instrumente des Risikomanagements:** Forschung sollte auch dazu beitragen, Instrumente für das Management von Cyber-Risiken zu entwickeln, wie zum Beispiel Risikokarten, Szenarien oder Simulationen. Die Messbarkeit von Risiken und Gegenmassnahmen ist dabei ein wichtiges Thema. Eine bessere Messbarkeit könnte Praktikern dabei helfen, das richtige Schutzniveau für ihre Organisation zu bestimmen.
- **Informationsaustausch:** Eine grosse Herausforderung für das Management von Cyber-Risiken ist der Mangel an Informationen über die Risiken und über mögliche Gegenmassnahmen. Um diesem Mangel zu begegnen, haben sich Organisationen und Plattformen für den Informationsaustausch etabliert. Für die Forschung gilt es zu untersuchen, wie solche Plattformen und Organisationen effektiv und effizient betrieben werden können. Ein spezieller Fokus soll dabei auf den Informationsaustausch zwischen öffentlichen und privaten Akteuren in den so genannten Public-Private Partnerships gelegt werden.
- **Regulation:** In der Praxis ist das Risikomanagement stark beeinflusst vom regulatorischen Kontext. Regierungen können die Praktiken und Standards des Risikomanagements über Gesetze und Verordnungen vorgeben. Ein wichtiges Beispiel für einen solchen regulatorischen Eingriff ist die Meldepflicht bei Vorfällen. Forscher sollten untersuchen, wann und unter welchen Bedingungen eine Meldepflicht effektiv zur Verbesserung des Cyber-Risikomanagements beiträgt.

Beispiele für Forschungsfragen:

- Welche Auswirkungen haben die hohe Dynamik und die grosse Komplexität von Cyber-Risiken auf die Anwendbarkeit der bestehenden Praktiken und Methoden des Risikomanagements?
- Wie kann die Eintrittswahrscheinlichkeit und das Schadensausmass bei Cyber-Risiken abgeschätzt werden?
- Mit welchen Methoden kann festgestellt werden, welches das optimale Ausmass von Investitionen in die Cyber-Sicherheit ist?
- Welche Anreize führen zu einem stärkeren Informationsaustausch zu Cyber-Risiken?
- Wie kann die Zusammenarbeit zwischen privaten und staatlichen Akteuren gestärkt werden?
- Welche Regulierungen sind sinnvoll? Was wären potenzielle Konsequenzen von Audits durch den Staat oder einer Meldepflicht zu Cyber-Vorfällen?

3.2.7 Ökonomie der Cyber-Sicherheit

Beschreibung des Forschungsbereichs:

Die ökonomische Perspektive zur Cyber-Sicherheit analysiert das Verhältnis zwischen den finanziellen Verlusten auf Grund von Cyber-Vorfällen und den Kosten für die Schutz-

massnahmen. Der Mangel an Cyber-Sicherheit wird auf eine fundamentale Anreiz-Problematik und der ungenügenden Informationslage zu den Kosten von Cyber-Risiken zurückgeführt.
Die falschen Anreize sind eine direkte Konsequenz der Natur des Cyber-Raumes als ein sehr dichtes und komplexes Netzwerk von Informationssystemen und Nutzern. Für individuelle Nutzer und Firmen bedeutet die Einbindung ihrer Systeme in Netzwerke, dass diese - unabhängig von ihren eigenen Investitionen in die Sicherheit - immer bis zu einem gewissen Grad verwundbar bleiben. Die Cyber-Sicherheit weist in verschiedener Hinsicht den Charakter von öffentlichen Gütern auf und entsprechend führen Investitionen in die Cyber-Sicherheit zu hohen positiven Externalitäten. Daraus entsteht ein Koordinationsproblem, das darin besteht, dass der Nutzen von Investitionen eines Akteurs in die Cyber-Sicherheit von den Investitionen aller anderen Akteure abhängt.
Zusätzlich erschwert der Mangel von Daten über die Kosten von Cyber-Risiken, das richtige Ausmass der nötigen Investitionen in Schutzmassnahmen zu bestimmen. Bisher gibt es noch kaum Modelle zur Berechnung von Cyber-Risiken. Solche Modelle würden nicht nur den Praktikern helfen, ein Risikomanagement zu betreiben, sondern auch das Entstehen eines Marktes für Versicherungen zu Cyber-Risiken begünstigen. Bisher ist die Datenlage zu den Verlusten auf Grund von Cyber-Angriffen für Versicherungen nicht ausreichend, um Prämien, Kapital und Reserven zu berechnen. Entsprechend ist der Markt noch unterentwickelt. Es ist jedoch zu erwarten, dass sich Versicherungen zu Cyber-Risiken in den kommenden Jahren etablieren werden.

Relevanz:

Es ist heute unbestritten, dass Cyber-Risiken zu einem wirtschaftlich relevanten Problem geworden sind. Dennoch gibt es noch relativ wenig Forschung aus ökonomischer Perspektive darüber, wie die durch Cyber-Risiken entstehenden Kosten gesenkt werden könnten. Vertiefte Erkenntnisse zu den Kosten von Cyber-Risiken sind auch Voraussetzung dafür, dass ein funktionierender Markt für Versicherungen zu Cyber-Risiken entstehen kann.

Verwandte Forschungsbereiche:

Rechtliche Rahmenbedingungen; Strafverfolgung und Prävention von Cyber-Kriminalität; Management von Cyber-Risiken.

Mögliche Forschungsthemen:

- **Kosten von Cyber-Risiken**: Schätzungen über die Kosten von Cyber-Risiken gehen weit auseinander und sind oft nicht unabhängig, da sie von Anbietern von Gegenmassnahmen veröffentlicht werden. Forscher können dazu beitragen, eine bessere Systematik zur Schätzung der Kosten zu entwickeln und damit die Basis für Risiko-Modelle im Bereich der Cyber-Risiken zu schaffen.
- **Analyse der Cyber-Sicherheit als öffentliches Gut:** Es gilt zu untersuchen, in welcher Hinsicht Cyber-Sicherheit als öffentliches Gut beschrieben werden kann und welche Konsequenzen sich daraus für das Management von Cyber-Risiken ergeben.
- **Versicherbarkeit von Cyber-Risiken:** Ebenfalls zu untersuchen ist, auf welche Art Cyber-Risiken versicherbar sind und welche Voraussetzungen dafür geschaffen werden müssen. Ein wichtiges Instrument zur Entwicklung von Cyber-Versicherungen sind Datenbanken zu Vorfällen. Forscher können mithelfen, solche Datenbanken zu schaffen.
- **Regulation:** Aus wirtschaftswissenschaftlicher Sicht sollen die Effekte bestehender oder möglicher regulativer Eingriffe zur Förderung der Cyber-Sicherheit aus einer Kosten-Nutzen-Perspektive untersucht werden.

Beispiele für Forschungsfragen:
- Könnte die Verfügbarkeit von Versicherungen gegen Cyber-Risiken zu verstärkten Investitionen in das Cyber-Risikomanagement führen?
- Wie können die Modellierung und die Kostenberechnung von Cyber-Risiken verbessert werden angesichts der fehlenden Daten, der dynamischen Entwicklungen und der hohen Komplexität?
- Inwiefern können Instrumente wie die «Alternative Risk Transfer» oder «Insurance Linked Strategies» genutzt werden, um die Tragbarkeit von Cyber-Risiken durch Versicherungen zu erhöhen?
- Welches sind die ökonomischen Kosten und Nutzen von regulatorischen Eingriffen?
- Wie kann im Cyber-Risikomanagement mit extremen Risiken umgegangen werden?

3.2.8 Sicherheit von Cyber-physischen Systemen

Beschreibung des Forschungsbereichs:
Cyber-physische Systeme breiten sich sehr schnell über die verschiedensten Anwendungsfelder hinweg aus. Im Bereich der Gebäudesteuerung sind solche Systeme schon weit verbreitet, sie finden aber auch vermehrt Anwendung im Medizinbereich oder als prominentes Beispiel bei selbstfahrenden Fahrzeugen.
Alle diese Systeme bieten unzweifelhaft grosse Vorteile, führen aber auf Grund ihrer Verbreitung oder ihren Fähigkeiten auch zu neuen Sicherheitslücken. Massgebend ist, dass alle diese Systeme für ihr Funktionieren von einer Vielzahl von Sensoren abhängen, die kontinuierlich Daten erfassen. Gleichzeitig sind die Systeme oft nicht oder nur schwach gesichert, was sie zu einem sehr attraktiven Ziel für Angriffe macht. Es braucht verbesserte Sicherheitsmassnahmen und ein gesteigertes Bewusstsein der Anwender, damit diese Systeme künftig gegen Angreifer besser geschützt sind.
Cyber-physische Systeme führen zugleich zu neuen Herausforderungen im Umgang mit dem Datenschutz. Über eine Auswertung, der durch solche Systeme erfassten Daten, können sehr viele Informationen über Nutzende gewonnen werden. Es muss analysiert werden, welche Auswirkungen diese Entwicklungen auf den Datenschutz haben.

Relevanz:
Die rasche Verbreitung von Cyber-physischen Systemen in allen Anwendungsbereichen (von der Industrie über das Gesundheitswesen bis hin zur Unterhaltungselektronik) macht die Forschung zur Sicherheit dieser Systeme sehr wichtig, da es künftig immer schwieriger werden wird, klare Grenzen zwischen der physischen Welt und dem Cyber-Raum zu ziehen.

Verwandte Forschungsbereiche:
Schutz der Privatsphäre und Datenschutz; Vorfallbewältigung, Vorfallerkennung, digitale Forensik; Rechtliche Rahmenbedingungen; Strafverfolgung und Prävention von Cyber-Kriminalität; Management von Cyber-Risken.

Mögliche Forschungsthemen:
- **Sicherheit im Internet der Dinge**: Es gilt, die wichtigsten Herausforderungen bei der Sicherheit des Internets der Dinge systematisch zu analysieren und Vorschläge zu erarbeiten, wie die Situation verbessert werden kann. Zu berücksichtigen sind neben möglichen technologischen Lösungen auch Massnahmen zur Aufklärung der Nutzerinnen und Nutzer.
- **Sicherheit in speziellen Anwendungsfeldern:** Cyber-physische Systeme kommen in verschiedenen Anwendungsfeldern zum Einsatz. Es stellen sich jeweils aus dem Kontext dieser Anwendungen verschiedene Forschungsfragen.
- **Sicherheit von kritischen Infrastrukturen und deren Dienstleistungen:** In kritischen Infrastrukturen ist die Sicherheit von gesamtgesellschaftlicher Relevanz. Die Auswirkungen der zunehmenden Vernetzung dieser Systeme auf die Sicherheit muss überprüft werden. Dabei sind insbesondere auch die gegenseitigen Abhängigkeiten verschiedener Infrastrukturen zu berücksichtigen.

Beispiele für Forschungsfragen:
- Welche neuen Technologien können helfen, die Sicherheit von Cyber-physischen Systemen zu verbessern?
- Wie können dezentrale Systeme von Missbrauch geschützt werde,n ohne dazu zentrale Infrastrukturen einzuführen?
- Auf Grund welcher Kriterien kann die Sicherheit von Cyber-physischen Systemen gemessen werden und wie könnten Zertifizierungsverfahren auf solche Systeme angewendet werden?
- Wie können Updates auf Cyber-physische Systeme gespielt werden und wie kann dieser Prozess automatisiert werden?

3.2.9 Cybersecurity in International Relations

Beschreibung des Forschungsbereichs:
Cyber-Sicherheit ist zunehmend auf der Agenda der Politik. Bei den Bemühungen, die Cyber-Sicherheit zu erhöhen, ist sie Rolle der Nationalstaaten bei der Sicherung des Cyber-Raumes besonders im Fokus. Mehrere Möglichkeiten werden aktuell diskutiert, von der Einführung von Verhaltenskodizes bis zu Übereinkommen über Normen und Regeln im Cyber-Raum. Ergänzend zu diesen Bemühungen werden vertrauensbildende Massnahmen ergriffen, um die internationale Kooperation zu stärken und Mechanismen zu identifizieren, wie den Cyber-Bedrohungen gemeinsam begegnet werden kann.

Relevanz
Im strategischen Diskurs wird der Cyber-Raum sowohl als Ziel von Angriffen (risk to cyberspace) als auch als Angriffsmittel (risk through cyberspace) wahrgenommen. Diese Kombination und die Flut von Vorfällen haben dazu geführt, dass die Cyber-Sicherheit zu einem Hauptthema der nationalen und internationalen Sicherheitsdebatten wurde. Cyber-Sicherheit kann dabei nicht nur als technisches oder rechtliches Problem betrachtet werden, sondern auch als Thema der Diplomatie und der Aussen- und Militärpolitik.
Entsprechend gibt es heute viele internationale Initiativen zur Cyber-Sicherheit. Die meisten fokussieren darauf, den Cyber-Raum so zu regulieren, dass er zu einem stabilen und verlässlichen Platz wird.
Für die Forschung sind diese Entwicklungen eine sehr gute Gelegenheit, formelle und informelle internationale Initiativen zu untersuchen und bestehenden Konfliktlinien nachzugehen. Ein Verständnis dieser Faktoren ist Voraussetzung dafür, gute internationale Lösungen für das Problem der Cyber-Sicherheit zu finden.

Verwandte Forschungsbereiche:
Rechtliche Grundlagen, Prävention und Strafverfolgung von Cyber-Kriminalität; menschliche Faktoren in der Cyber-Sicherheit.

Mögliche Forschungsthemen:
- **Cyberpower:** Es gilt theoretische Ansätze zu entwickeln, um das Konzept der Macht im Cyber-Raum zu definieren und die entsprechenden Dynamiken zu verstehen. Dazu gehört es, die potentielle Wirkung von offensiven Fähigkeiten zu analysieren (auch als Mittel gegen Cyber-Kriminalität und Cyber-Terror) und die rechtlichen und ethischen Fragen dazu zu erörtern.
- **Cyber-Abschreckung:** Es ist zu prüfen, ob und wie die Theorie der gegenseitigen Abschreckung auch auf die Machtpolitik im Cyber-Raum angewendet werden kann. Dabei muss zusätzlich die wichtige Rolle von nichtstaatlichen Akteuren bei der Nutzung von Cyber-Fähigkeiten berücksichtigt werden.
- **Eskalation von Konflikten:** Die besondere Dynamik von Konflikten im Cyber-Raum muss besser verstanden werden.
- **Normen, Abkommen, Institutionen und Strukturen:** Obwohl die internationale Zusammenarbeit in vielen Bereichen am Anfang steht, gibt es dennoch verschiedene Normen, Abkommen, Institutionen und Strukturen. Ihre Effekte, ihr modus operandi und ihre Schwachstellen sind ein wichtiges Forschungsgebiet. Die Forschung soll

dazu beitragen, mögliche Formen von institutionellen Rahmen im Bereich Cyber-Sicherheit zu identifizieren.

- **Internet Gouvernanz:** Die verschiedenen Modelle der Internet Gouvernanz sind zu vergleichen und ihre Vor- und Nachteile zu beschreiben. Dabei ist die wichtige Rolle von privaten Akteuren besonders zu beachten.

Beispiele für Forschungsfragen:

- Was bedeutet «Cyberpower» und wie kann sie gemessen werden?
- Was ist sind die spezifischen Eigenschaften von Konflikten im Cyber-Raum? Und welches sind typische Dynamiken für solche Konflikte? Welche Entwicklungen sind zu erwarten?
- Welchen Einfluss haben die verschiedenen Cyber-Vorfälle auf die Entwicklung der internationalen Beziehungen?
- Wie entwickeln sich die Regeln, Entscheidungsprozesse und Machtpositionen in bestehenden Modellen der Internet Gouvernanz? Sind diese Modelle effektiv und effizient?
- Was können vertrauensbildenden Massnahmen sein und wie können sie zur Stabilität beitragen?
- Was ist die Rolle von privaten Akteuren in der Internet Governanz und in den Institutionen zur Förderung der Cyber-Sicherheit?
- Was sind «offensive Cyber-Fähigkeiten»? Wie könnte eine Rüstungskontrolle im Cyber-Bereich aussehen? Welche Technologien wären dazu nötig?
- Wie könnte die Attribution bei Cyber-Attacken verbessert werden?

3.2.10 Menschliche und soziale Faktoren in der Cyber-Sicherheit

Beschreibung des Forschungsbereichs:

Viele, wenn nicht sogar die Mehrheit der Cyber-Vorfälle sind direkt oder indirekt auf ein Fehlverhalten der Nutzer zurückzuführen. Beispiele dafür sind schwache Passwörter, das Öffnen von E-Mails mit Schadcode oder die Herausgabe von Daten und Informationen auf Grund von gefälschten Anfragen.

Forschung zu Cyber-Risiken sollte deshalb auch den menschlichen Faktor der Cyber-Sicherheit berücksichtigen. Solche Forschung schliesst psychologische, soziologische, anthropologische und kulturelle Studien ein. Gegenstand der Forschung sind sowohl das Verhalten der Opfer als auch der Angreifer. Es ist wichtig, die Verhaltensweisen beider Gruppen zu verstehen, damit die richtigen Massnahmen getroffen werden können, um das Ausnutzen von Schwachstellen bei den Nutzern schwieriger zu machen.

Relevanz:

Forschung zum Verhalten von potentiellen Opfern und Tätern im Cyber-Raum ist wichtig, weil am Ursprung von Attacken immer menschliche Absichten oder menschliche Fehler stehen. Cyber-Risiken können nur dann gemindert werden, wenn neben den technischen, wirtschaftlichen und rechtlichen Fragen auch der menschliche Faktor angemessen berücksichtigt wird. Es ist zudem wichtig zu untersuchen, welchen Einfluss Cyber-Risiken und die Debatte über Sicherheit und Überwachung im Internet einen Einfluss auf das Verhalten von Nutzern hat.

Verwandte Forschungsbereiche:

Schutz der Privatsphäre und Datenschutz; Strafverfolgung und Prävention von Cyber-Kriminalität; Management von Cyber-Risiken.

Mögliche Forschungsthemen:

- **Wahrnehmung von Cyber-Risiken:** Es ist zu untersuchen, wie Cyber-Risiken in der Gesellschaft wahrgenommen werden und ob es relevante Unterschiede zwischen verschiedenen Nutzergruppen gibt.
- **Verhalten der Nutzer:** Forschung sollte versuchen, das Verhalten von Nutzern in Bezug auf Cyber-Risiken zu erklären. Es ist zu analysieren, wie bewusst den Nutzern die Cyber-Risiken sind, welchen Einfluss diese auf ihr Nutzungsverhalten haben und wie eine selbstbestimmte Nutzung sichergestellt werden kann.

- **Motivation der Angreifer:** Die Motivation der Angreifer ist häufig nicht ausschliesslich ökonomisch. Der psychologische, anthropologische und kulturelle Kontext dieser Täter muss untersucht werden, damit ein besseres Verständnis über die nicht-ökonomischen Faktoren gewonnen werden kann.
- **Ethik im Cyber-Raum:** Es ist zu untersuchen, welche Ethik im mehrheitlich anonymen Umfeld des Cyber-Raums gilt, welche Standards mehrheitlich praktiziert werden und welche Grenzen überschritten werden.

Beispiele für Forschungsfragen:

- Wie können verschiedene Nutzergruppen besser über Cyber-Risiken aufgeklärt werden?
- Wie können verhaltenspsychologische Faktoren in das Risikomanagement integriert werden?
- Wie müssten Systeme gestaltet sein, damit Nutzer die Sicherheitsanforderungen besser verstehen und beachten?
- Welche psychologischen Effekte haben Cyber-Angriffe auf die Opfer?
- Wie beeinflussen sich Angreifer gegenseitig? Gibt es Rollenmodelle?
- Wie werden Cyber-Risiken in der Popkultur (in Kino, Literatur, Video, Musik, Malerei) thematisiert? Inwiefern trägt dies zum Bewusstsein für Cyber-Risiken bei? Und wie werden die Angreifer davon beeinflusst?
- Wie können universelle ethische Verhaltenskodizes im globalisierten Cyber-Raum entwickelt und angewendet werden?
- Wie kann verhindert werden, dass das Internet zur Radikalisierung verschiedener Gruppen beiträgt?

3.3 Fokusthemen: Besonders relevante Bereiche, Technologien und Anwendungen

In diesem Kapitel werden Fokusthemen aufgeführt. Dies sind Bereiche und Anwendungen, welche in der Diskussion um Cyber-Risiken viel Aufmerksamkeit gewonnen haben. Alle dieser Themen beeinflussen die Debatten auf ihre Weise und eine Übersicht zu Forschungsthemen wäre nicht komplett, ohne diese Fokusthemen behandelt zu haben. Gleichzeitig konnten diese Themen nicht direkt einem der oben beschriebenen Bereiche zugeordnet werden, weil sie mehrere dieser Bereiche betreffen. Die Expertengruppe hat sich darum entschieden, folgende drei Themen separat als Fokusthemen zu beschreiben:

1) Big Data
2) Cyber-Risiken und Cloud Computing
3) Sicherheit in der FinTech

3.3.1 Big Data

Beschreibung des Fokusthemas:

Die umfassende Sammlung und Analyse von sehr grossen Datenmengen ist unter dem Begriff Big Data bekannt geworden. Der Begriff bezieht sich dabei einerseits auf die neuen Technologien, welche solche Auswertungen in kurzer Zeit ermöglichen, andererseits auf das Phänomen, dass Datenauswertungen eine immer stärkere Rolle spielen bei der Transformation zur digitalen Gesellschaft.

Über das Internet werden laufend Daten erhoben, gesammelt, ausgetauscht, ausgewertet und (kommerziell) verwertet. Dies führt zu wichtigen Fragen in Bezug auf Cyber-Risiken hinsichtlich des Schutzes dieser Daten, ihres Lebenszyklus und ihrer Aufbewahrung. Die Technologien der Datenanalyse können aber gleichzeitig auch wertvolle Instrumente bei der Aufklärung von Straftaten sein und spielen oft eine wichtige Rolle, wenn es darum geht, Cyber-Angriffe einer Täterschaft zuzuordnen.

Relevanz

Die neuen Möglichkeiten zur Analyse grosser Datenmengen in kurzer Zeit und sie mit anderen Datensätzen abzugleichen und zu korrelieren, ist für alle Forschungsgebiete im Bereich Cyber-Risiken relevant. Das Thema wird die Zukunft der digitalen Gesellschaft massgeblich mitprägen und nimmt daher in der Forschung zu Cyber-Risiken einen wichtigen Platz ein.

Mögliche Forschungsthemen:

- **Big Data und die Rolle von Datenmonopolen:** Es ist zu analysieren, welche Auswirkung die Entstehung von Daten-Monopolen auf die Wirtschaft und die Gesellschaft haben. Zu untersuchen ist insbesondere, inwiefern heute Staaten von Konzernen mit Datenmonopol in einem bestimmten Bereich abhängig sind.
- **Big Data als Instrument für Cyber-Sicherheit:** Das Potential von Big Data bei der Prävention und Aufklärung von Cyber-Angriffen ist gross. Die Forschung sollte dieses Potential ausloten und aufzeigen, wie Möglichkeiten künftig genutzt werden könnten.
- **Rechtliche Herausforderung Big Data:** Die Möglichkeiten zur umfassenden Sammlung und Analyse von riesigen Datenvolumen ist in den rechtlichen Grundlagen kaum oder wenig berücksichtigt. Die dezentralen Infrastrukturen von Big Data stellen eine zusätzliche Herausforderung. Es ist zu untersuchen, wie mit dieser Problematik umgegangen werden kann.
- **Politischer, gesellschaftlicher und ökonomischer Kontext von Big Data:** Das Phänomen Big Data kann nur verstanden werden, wenn der politische, gesellschaftliche und ökonomische Kontext in die Untersuchung einbezogen wird. Es ist zu analysieren, wer die Technologien von Big Data wie und aus welchen Gründen nutzt.

Beispiele für Forschungsfragen:

- Welches sind generell die Konsequenzen von Big Data für die Cyber-Sicherheit? Verbessern diese Technologien die Situation oder verstärken sie die Risiken sogar zusätzlich?
- Welche Rolle sollte der Staat in Bezug auf Big Data einnehmen? Braucht es eine stärkere Regulierung?
- Funktioniert der freie Markt oder sind die Monopole von Grossfirmen zu stark?
- Welche rechtlichen Grundlagen braucht es für Big Data?
- Welches ist das Potential von Big Data bei der Verhinderung und Aufklärung von Cyber-Attacken?
- Wie kann Big Data das Risikomanagement von Cyber-Risiken beeinflussen?

3.3.2 Cyber-Risiken und Cloud Computing

Beschreibung des Fokusthemas:

In den letzten Jahren sind die Cloud Services sehr populär geworden. Viele dieser Services nutzen einen zentralen Speicher, um Daten zu sammeln und ermöglichen es dem Nutzer, die Informationen - unabhängig von seinem Standort – abzurufen. Andere nutzen tatsächlich eine dezentrale Datenspeicherung, was der ursprünglichen Idee des Cloud

Computing eher entspricht. DUnter den in Clouds angebotenen Services finden sich in Anwendungen verschiedenster Gebiete, von der Steuerung von Cyber-physischen Systemen, über Büroapplikationen bis hin zu Systemen für das E-Voting.
Die Speicherung von Daten in einer Cloud ist jedoch nicht ohne Risiken. Fehlfunktionen oder Manipulationen können dazu führen, dass die Daten Dritten zur Verfügung stehen, was zu Unannehmlichkeiten, aber auch ernsthaften Problemen mit dem Datenschutz oder gar zu finanziellen Verlusten führen kann.
Cloud Services haben die Eigenschaft, dass die Daten auf Grund ihrer Funktion mobil sind und daher nicht an ein einzelnes Rechtssystem gebunden sind. Die Daten und Funktionen können über verschiedene Länder hinweg verteilt sein. Eine rechtliche Kontrolle von Cloud Services ist daher nicht einfach. Dies zeigt sich beispielsweise bei der durch Cloud Computing ermöglichten digitalen Währungen (wie Bitcoin, Ethereum, Dodgecoin, Litecoin oder anderen) oder auch bei Informationsplattformen ohne zentrale Infrastrukturen.

Relevanz

Cloud Computing ist eine sehr wichtige Technologie geworden, deren Auswirkungen einen direkten Einfluss auf Cyber-Risiken und mögliche Gegenmassnahmen haben. Für die Forschung im Bereich Cyber-Risiken ist es wichtig zu verstehen, wie sich Cloud Computing weiterentwickelt und welches die konkreten Auswirkungen auf die Cyber-Sicherheit sind.

Mögliche Forschungsthemen:

- **Schutz der Privatsphäre und Datenschutz in der Cloud:** Es ist zu analysieren, welche Konsequenzen die Verbreitung von Cloud Services auf den Schutz der Privatsphäre und der persönlichen Daten hat. Es braucht technische Sicherheitsmassnahmen bei der Speicherung der Daten, bei der Kontrolle des Zugangs und bei der Übermittlung. Auch in Bezug auf die Rechte und Pflichten der Nutzer und der Anbieter von Cloud-Diensten bleiben viele wichtige Fragen zu klären.
- **Forensik und Cloud Computing:** Cloud Computing kann zu Herausforderungen bei der forensischen Analyse werden, weil grosse Datenmengen an verschiedenen Orten gespeichert sind, welche kaum mehr physisch zugänglich sind. Es müssen die entsprechenden technischen Instrumente entwickelt und rechtliche Fragen geklärt werden.
- **Bewusstsein der Nutzer:** Viele Nutzende sind sich kaum bewusst, wie und wo ihre Daten gespeichert werden. Es gilt Möglichkeiten zu identifizieren, wie den Nutzern ein besseres Verständnis der Cloud-Technologie vermittelt werden kann.

Beispiele für Forschungsfragen:

- Welche rechtlichen Fragen stellen sich bei der Nutzung der Cloud?
- Wie können illegale Aktivitäten in der Cloud entdeckt und zugeordnet werden?
- Welche Herausforderungen stellen sich in Bezug auf den Datenschutz?
- Wie kann die Authentizität und Integrität von Daten in der Cloud sichergestellt werden?

3.3.3 Sicherheit in der FinTech

Beschreibung des Fokusthemas:

Die Finanzindustrie hat die digitale Transformation der Gesellschaft und Wirtschaft immer früh übernommen und vorangetrieben. Die Einführung von digitalen Technologien und komplexen Finanzprodukten veränderten beispielsweise in den 70er und 80er Jahren die Branche massiv. Heute gehören digitale Technologien zu ökonometrischen Auswertungen, Modellierungen, Aufzeichnungen und Ausführungen von Transaktionen längst zum Standard.
Der nächste grosse Schritt in dieser Entwicklung geschieht aktuell durch das Aufkommen der FinTech-Industrie (der Kombination von Finance und Technologie). Die wichtigsten Applikationen sind aktuell «Social Trading» (Anlageberatung auf sozialen Plattformen); «Robo-Advisory» (automatisierte Anlageberatung) oder «Peer-to-peer lending» (direkte Kreditvergabe von Privatperson an Privatperson).

Das Marktpotential dieser Applikationen ist oft noch unklar, ebenso sind die Risiken dieser neuen Anwendungen bisher kaum erforscht. Es braucht in diesem Bereich noch viel Grundlageforschung, um zu klären, welche Auswirkungen FinTech auf die Finanzindustrie und auf die Cyber-Risiken hat.

Relevanz:

FinTech stösst weltweit in den Medien und bei Praktikern auf viel Interesse. Die Schweiz ist gewillt, in der FinTech eine wichtige Rolle zu spielen. Obwohl die Bedeutung von FinTech bei Praktikern und in der Politik unbestritten ist, gibt es noch kaum einen akademischen Diskurs über die Bedeutung und den Einfluss dieser Technologie. Es besteht daher klaren Bedarf für Forschung in diesem Bereich.

Mögliche Forschungsthemen:

- **Auswirkung der FinTech auf die Finanzindustrie:** Es ist noch unklar, wie stark und in welcher Hinsicht die neuen Technologien die Finanzindustrie verändern werden. Die Forschung sollte dazu beitragen, das Phänomen der FinTech besser einzuschätzen und mögliche Konsequenzen aufzuzeigen.
- **Verstärkte Abhängigkeit:** Die noch stärkere Digitalisierung der Finanzindustrie verstärkt auch deren Abhängigkeit von IT-Dienstleistern. Bei einem breitflächigen Ausfall der IT droht auch das Finanzsystem zu kollabieren. Es gilt zu untersuchen, wie sich die systemischen Risiken mit der Verbreitung von FinTech steigen.
- **Neue Risiken:** Die neuen Technologien bringen auch neue Risiken mit sich. Auch in dieser Hinsicht gibt es erst wenige Erkenntnisse. Je früher potentielle Risiken aber erkannt werden, desto besser kann sich die Finanzindustrie darauf vorbereiten.

Beispiele für Forschungsfragen:

- Werden Finanzintermediäre wie Banken oder Versicherungen durch die FinTech verdrängt? Welches Potential haben in dieser Hinsicht die Blockchain-Technologie oder das Peer-to-peer lending?
- Wie verändern die FinTech die systemischen Risiken im Finanzsektor? Steigern sie diese auf Grund der grossen Abhängigkeit von IT-Dienstleistungen oder senken sie die Risiken durch ihre dezentrale Struktur?
- Braucht es künftig noch menschliche Beratung in der Finanzindustrie? Wie ist die Kundenakzeptanz von Robo-Advisors?
- Welchen Einfluss haben Big Data-Analysen auf den Handel? Sind Algorithmen angesichts der Verfügbaren Datenmenge effektiver im Handel als Menschen?

4 Schlusswort

Der Expertenbericht wollte drei Ziele erreichen: eine Übersicht der wichtigsten Forschungsthemen in den verschiedenen Fachrichtungen, die Förderung eines gemeinsamen Verständnisses für die Forschung in den unterschiedlichen Disziplinen und schliesslich die Sensibilisierung der Forschungspolitik für das Thema Cyber-Risiken. Mit der Fülle und Vielfältigkeit der aufgeführten Themen ist es sicher gelungen, einen Beitrag zu den ersten beiden Ziele zu leisten. Es konnte dargestellt werden, wie breit die Thematik ist und wie viele anspruchsvolle Forschungsfragen in den verschiedenen Disziplinen zu bewältigen sind. Es ist zu hoffen, dass sich viele Forschende motiviert fühlen, die komplexen aber wichtigen und interessanten Themen in ihrer Arbeit anzugehen. Es sei aber hier nochmals betont, dass der Bericht keinen Anspruch auf Vollständigkeit erhebt. Es gibt noch weitere, im Bericht nicht enthaltene Forschungsfragen, welche genauso relevant sein können. Zudem führt die rasch voranschreitende technologische Entwicklung dazu, dass ständig neue Herausforderungen dazukommen.

Als Instrument für die Sensibilisierung der Forschungspolitik hilft dieser Bericht, indem er die gesamte Palette an Themen aufführt. Forschung zu Cyber-Sicherheit darf nicht auf technische Fragestellungen reduziert werden und wird vor allem dann zu relevanten Resultaten führen, wenn ein möglichst interdisziplinärer Ansatz gewählt wird. Der Bericht soll als Grundlage dienen für die Ausgestaltung von künftiger Forschungsförderung im Bereich Cyber-Risiken.

Es bleibt zum Schluss der Appell an alle – Forschende und Forschungsfördernde – die Forschung zu den erwähnten Themen voranzutreiben. Wenn wir als Gesellschaft die digitalen Technologien nutzen, sind wir auf deren Sicherheit angewiesen. Sicherheit wiederum entsteht nur dann, wenn die vorhandenen Probleme gründlich analysiert und innovative Lösungen erarbeitet werden. Die Schweiz verfügt über hervorragende Hochschulen, welche bereits heute zu vielen der aufgeführten Themen forschen. Es gilt, dieses Potential zu nutzen und weiterzuentwickeln, damit die Schweiz eine wichtige Rolle bei der Entwicklung und Anwendung von Technologien und Methoden zur Cyber-Sicherheit übernehmen kann und zugleich die Fähigkeit hat, die eigenen Infrastrukturen vor Cyber-Risiken zu schützen.