Bundesministerium
für Wirtschaft
und Energie

MITTELSTAND
GLOBAL
MARKTERSCHLIESSUNGS-
PROGRAMM FÜR KMU

Zivile Sicherheitstechnologien in Norwegen: Digitale Sicherheit und Schutz vor Naturereignissen

Zielmarktanalyse Norwegen 2021
Digitale Geschäftsanbahnungsreise für deutsche KMU

Durchführer:

AHK
Deutsch-Norwegische | Norsk-Tysk
HANDELSKAMMER

Impressum

Herausgeber
Deutsch-Norwegische Handelskammer
Drammensveien 111b
0273 Oslo
Norwegen
Telefon: +47 22 12 82 10
info@handelskammer.no
www.handelskammer.no

Text und Redaktion
Deutsch-Norwegische Handelskammer

redaktionelle Bearbeitung
Carine Gronholz
Rita Hareid
Sybille Köhler
Antje Duca-Ingeberg

Gestaltung und Produktion
Deutsch-Norwegische Handelskammer

Stand
26.10.2021

Die Studie wurde für die digitale Geschäftsanbahnungsreise nach Norwegen für deutsche Unternehmen zum Thema Zivile Sicherheitstechnologien mit Fokus auf digitale Sicherheit und Schutz vor Naturereignissen im Rahmen des BMWi-Markterschließungsprogramms für KMU erstellt.

Inhaltsverzeichnis

Tabellen

Abbildung

Abkürzungsverzeichnis

BIP	Bruttoinlandsprodukt
CAP	*Common Alerting Protocol,* internationaler Standard zum Austausch von Warnmeldungen im XML Format
CEN	*Comité Européen de Normalisation (*Europäisches Komitee für Normung)
CERT	*Computer Emergency Response Team*
DFØ	*Direktoratet for Forvaltning og Økonomistyring* (staatliches Amt für Verwaltung und Finanzen)
DSB	*Direktoratet for samfunnssikkerhet og beredskap,* staatliche Behörde für Sicherheit und Notfallbereitschaft
EFTA	*European Free Trade Association* (Europäische Freihandelsassoziation)
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
F&E	Forschung und Entwicklung
FDI	*Foreign Direct Investments* (Ausländische Direktinvestitionen)
GDPR	*General Data Protection Regulation,* Datenschutzgrundverordnung der EU
GTAI	Germany Trade & Invest
HMS	*Helse, Miljø, Sikkerhet* (Gesundheit, Umwelt, Sicherheit)
IFE	*Institutt for energiteknikk,* Forschungsinstitut für Energietechnik
IKT	Informations- und Kommunikationstechnik
IoT	*Internet of Things* (Internet der Dinge)
ISO	*International Standardisation Organisation* (Internationale Standardisierungsorganisation)
KI	Künstliche Intelligenz
MET	*Meteorologisk Institutt,* norwegisches meteorologisches Institut
Mio	Millionen
Mrd.	Milliarden
NCE	*Norwegian Center of Expertise* (Norwegische Exzellenzcluster)
NCR	*Norwegian Cyber Range*, nationale, sektorenübergreifende Testarena für Cyber- und Informationssicherheit
NEK	*Norsk Elektroteknisk Komitee,* Mitgliederorganisation für die Standardisierung im Bereich Elektrotechnik
NGI	*Norges Geotekniske Institutt,* Norwegisches Geotechnisches Institut
NGU	*Norges geologiske undersøkelse,* Institut für geologische Untersuchungen
NHO	*Næringslivets Hovedorganisasjon* (Norwegischer Arbeitgeberverband)
NKom	nationale Telekommunikationsbehörde
NOK	Norwegische Krone
NOU	*Norges offentlige utredninger,* offizielle Berichte norwegischer Regierungskomitees
NS	*Norsk Standard* (Norwegische Standardisierungsorganisation)
NSM	*Nasjonal Sikkerhetsmyndighet,* nationale Sicherheitsbehörde
NTNU	*Norwegian University of Science and Technology* (Technisch-Naturwissenschaftliche Universität)
NTNU CCIS	*Center for Cyber and Information Security,* Cyber Security-Zentrum der technischen Universität in Trondheim
NTNU IIK	*Institutt for informasjonssikkerhet og kommunikasjonsteknologi,* Institut für IT-Sicherheit und Kommunikationstechnologie der technischen Universität in Trondheim
NUF	*Norskregistrert utenlandsk foretak* (in Norwegen registrierte Niederlassung eines ausländischen Unternehmens)
NVE	*Noregs vassdrags- og energidirektoratet*, staatliche Gewässer- und Energiebehörde
OED	*Olje- og energidepartementet,* Ministerium für Erdöl und Energie
PST	*Politiets sikkerhetstjeneste,* norwegischer Inlandsgeheimdienst
SAAF	*ShapeAccelArrayField*

SD	*Samferdselsdepartementet,* Verkehrsministerium
SSB	*Statistisk Sentralbyrå* (staatliches norwegisches Statistikamt)
TED	*Tenders Electronic Daily*, europäisches Ausschreibungsportal
UiA	*Universitetet i Agder,* Hochschule in Agder
VDI	*Varslingssystem for digital infrastruktur,* Warnsystem für die digitale Infrastruktur

Informationen zur Währungsumrechnung

Alle monetären Beträge, die in dieser Zielmarktanalyse in Norwegischen Kronen (NOK) angegeben werden, wurden mit dem durchschnittlichen Wechselkurs zum Euro (€) im September 2021 umgerechnet (10,186).

Abstract

Naturereignisse tragen in Norwegen einen bedeutenden Anteil am Gesamtrisiko für die zivile Sicherheit. **Überschwemmungen**, Erdrutsche und Waldbrände sind bereits häufige Ereignisse, deren Intensität und Vorkommen auch künftig mit steigender Tendenz erwartet wird. Gleichzeitig tragen die Klimaänderungen zu einer geringeren Vorausschaubarkeit bei. Die offensichtlichste Herausforderung sind häufigere und intensivere Niederschläge mit einer folgenden Gefahr für Hochwasser und Erdrutsche. Die Bevölkerung vieler norwegischer Regionen hat in den vergangenen Jahren starke Schäden durch plötzlich auftretende Überschwemmungen in kleineren Wasserläufen erlitten. Ferner gibt es in Norwegen recht häufige Vorkommen von Quickton, vor allem in den Regionen Østlandet und Trøndelag, aber auch entlang der Küste. Eine Überlastung von Quicktonböden führt zum Zusammenrutschen des Grundes, der Boden fließt wie eine Flüssigkeit davon. **Quickton**-Erdrutsche gehören daher in mehreren Teilen des Landes zum Gefahrenbild.

Für die Prävention von Schäden durch Hochwasser und Erdrutsche ist eine Vielzahl von Akteuren zuständig. Die **Kommunen** sind verantwortlich für die Beobachtung von Naturgefahren bei Flächenplanungs- und Bauvorhaben. Die staatliche Gewässer- und Energiebehörde unterstützt die Kommunen bei der Prävention von Schäden durch Überschwemmungen und Erdrutsche. Sie ist außerdem für die Ausarbeitung von Gefahrenkarten zuständig, kommentiert kommunale Flächenpläne und unterstützt die Kommunen mit Sicherungsmaßnahmen, Überwachung und Warnung. Sie berät die Kommunen und sorgt für die Aufrechterhaltung der Sicherheit bei Ereignissen.

Der norwegische Markt ist offen gegenüber neuen Technologien, Innovationen und Konzepten. Besonders nachgefragte Lösungen auf dem aktuellen Markt sind Hochwasserwarnungssysteme auf detailliertem Niveau und Warnsysteme für Erdrutsche in Quickton-Böden. Es wird auch die kontinuierliche Integration von 5G in immer mehr kritische Gesellschaftsfunktionen erwartet – dies bringt neue Möglichkeiten für die Nutzung moderner Technologien auf mehreren Anwendungsfeldern der Sicherheit im Hinblick auf Naturereignisse mit sich.

Norwegen gehört zu den Ländern, die bisher in der Digitalisierung ihrer Gesellschaftsfunktionen am weitesten vorangeschritten sind. Diese Entwicklung setzt sich weiter fort: Bis Ende 2024 wird der landesweite **Roll-Out des 5G-Netzes** erwartet. Dies schafft viele Möglichkeiten, jedoch auch neue Abhängigkeiten, unübersichtlichere Prozesse und neue Anfälligkeiten. Die Gesellschaft wird immer abhängiger von Elektrizität, Telekommunikation und Logistik – dies steigert die Anfälligkeit für technisches Versagen, Angriffe und Naturereignisse.

Die Gesellschaft ist von der Funktionalität ihrer kritischen Infrastrukturen abhängig – es wird vorausgesetzt, dass diese jederzeit und überall reibungslos laufen. Dazu gehört auch **Energieversorgung.** Strom trägt einen hohen Anteil am Energieverbrauch des Landes, kein anderes Land ist so abhängig von Elektrizität – viel zitierte Beispiele sind die Wärmeversorgung von Gebäuden oder der hohe Anteil der Elektromobilität. Ein Versagen der Stromversorgung führt zu fatalen Folgen für alle Sektoren und digitalen Systeme, von denen die gesamte Gesellschaft abhängig ist.

Digitale Sicherheit ist ein wichtiger Fokusbereich, um digitale Risiken und deren Abhängigkeiten und Folgeereignisse zu reduzieren. Die Anzahl neuer IoT-Anwendungen basierend auf 4G und 5G wächst, allmählich werden die neuen IoT-Lösungen zu einem integrierten Teil der Wertschöpfungsketten von immer mehr kritischen Funktionen. Daher steigt der **Bedarf an zuverlässigen Sicherheitslösungen**, welche spezifisch zum Schutz der neuen, komplexeren Netzwerktechnologie entwickelt wurden. Künstliche Intelligenz und maschinelles Lernen können eine entscheidende Rolle beim schnellen Aufdecken verdächtiger Aktivitäten spielen.

Nie zuvor gab es eine stärkere Nachfrage nach IT-Sicherheit. Unternehmen, welche Sicherheitsdienstleistungen, -beratungen, -infrastruktur und -software verkaufen, vermelden ein starkes Wachstum. Durch mobiles Arbeiten in Kombination mit Digitalisierungsvorhaben, beschleunigt durch die Corona-Pandemie, wurden öffentliche und private Unternehmen und Organisationen vor neue Sicherheitsherausforderungen gestellt. Die Anzahl digitaler Angriffe hat sich im vergangenen Jahr vervielfacht und sorgte für einen wachsenden Bedarf an IT-Sicherheitslösungen.

1 Zielmarkt Allgemein

1.1 Länderprofil und allgemeine Informationen

Norwegen ist mit einer Gesamtfläche von 323.802 km² und einer Einwohnerzahl von ca. 5,4 Mio. (Januar 2021)[1] verglichen mit den meisten anderen europäischen Staaten sehr dünn besiedelt. Hauptstadt und Regierungssitz des Landes ist Oslo. Oslo ist neben der industriegeprägten Westküste auch das wirtschaftliche und politische Zentrum des Landes. Insgesamt gibt es ein starkes Gefälle, wenn man die Bevölkerung in den Großstädten und auf dem Land vergleicht. Rund 26 % der Einwohner leben in den fünf größten Städten.[2]

Tabelle 1: Die wichtigsten Fakten zu Norwegen auf einen Blick

Hauptstadt	Oslo
Fläche	323.802 km[23]
Einwohner	5.398.804 (erstes Quartal 2021)[4]
Landeswährung	Norwegische Krone (NOK) Wechselkurs zum Euro: 10,7207 (Durchschnitt 2020)[5]
Staatsform	Konstitutionelle Monarchie mit Parlamentarismus
Staatsoberhaupt	König Harald V.
Regierungschef	Jonas Gahr Støre, *Arbeiderpartiet* (sozialdemokratische Arbeiterpartei)
Sprache	Norwegisch (*Bokmål, Nynorsk*)
Verwaltung	11 Verwaltungsbezirke (*fylkeskommuner*) 356 Kommunen
Größte Städte bzw. Kommunen des Landes (mit Einwohnerzahlen)	Oslo (697.549) Bergen (285.070) Trondheim (207.015) Stavanger (143.981) Bærum (128.113)[6]
Zugehörigkeit zu politischen Bündnissen	Mitglied des Europäischen Wirtschaftsraumes (EWR), kein Mitglied der EU
Wirtschaftliche Kennziffern	
BIP pro Kopf (2020)	634.532 NOK (ca. 59.187 €).[7]
BIP (2020)	3 413 450 Mio. NOK (ca. 318,4 Mrd. €)[8]
BIP-Prognose	2022 + 4,3 %, 2023: +2,7 %[9]
Leitzins	0,06 % (September 2021)[10]

[1] SSB, 23.02.2021, *Befolkning*, https://www.ssb.no/folkemengde, 09.03.2021.
[2] SSB, 18.12.2018, *Befolkning*, https://www.ssb.no/befolkning/statistikker/folkemengde/aar-berekna, 09.03.2021.
[3] CIA WorldFactbook., 2019, *NORWAY*, S. 1, https://www.cia.gov/the-world-factbook/static/0ae463d06343fbf4c546ca0393f2ef19/NO-summary.pdf, 09.03.2021.
[4] SSB, 19.05.2021, *Befolkning*, https://www.ssb.no/befolkning/folketall/statistikk/befolkning, 22.07.2021.
[5] Norges Bank, 09.03.2021, *Valutakurser*, https://www.norges-bank.no/tema/Statistikk/Valutakurser/?tab=currency&id=EUR, 09.03.2021.
[6] SSB, 09.03.2021, *Befolkning*, tabell 01222, https://www.ssb.no/statbank/table/01222, 09.03.2021.
[7] SSB, 07.07.2021, *Nasjonalregnskap*, https://www.ssb.no/nasjonalregnskap-og-konjunkturer/nasjonalregnskap/statistikk/nasjonalregnskap, 22.07.2021
[8] SSB, 07.07.2021, *Nasjonalregnskap*, https://www.ssb.no/nasjonalregnskap-og-konjunkturer/nasjonalregnskap/statistikk/nasjonalregnskap, 22.07.2021
[9] SSB, 04.06.2021, *Konjunkturtendensene,* https://www.ssb.no/nasjonalregnskap-og-konjunkturer/konjunkturer/statistikk/konjunkturtendensene, 22.07.2021
[10] Norges Bank, o. J., *Styringsrenten månedsgjennomsnitt,* https://www.norges-bank.no/tema/Statistikk/Rentestatistikk/Styringsrente-manedlig/, 17.10.2021.

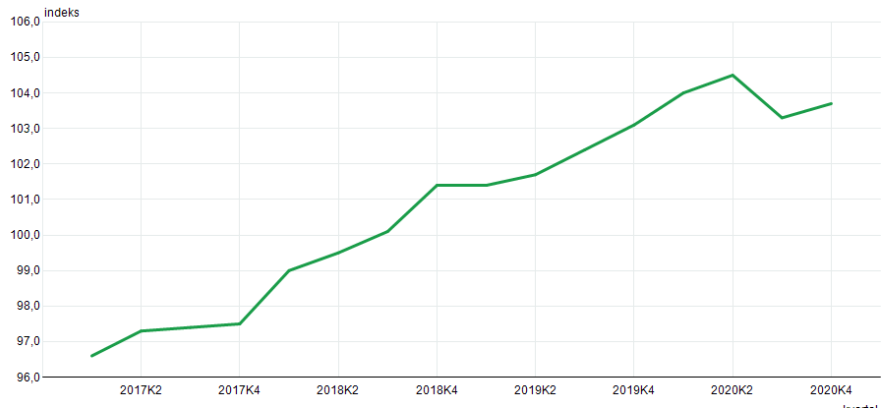
1.2 Wirtschaft, Struktur und Entwicklung

Die **Öl- und Gasindustrie** ist der größte Wirtschaftszweig des Landes und außerdem ein starker Treiber der Gesamtwirtschaft.[11] Weltweit ist Norwegen der drittgrößte Nettoexporteur von Erdgas.[12] **Bergbau** spielt in Norwegen ebenfalls eine entscheidende Rolle, v.a. im Hinblick auf den Abbau von Industriemineralien, Naturstein und metallischen Erzen. Weitere **wichtige Industriezweige** sind die Metallerzeugung und -verarbeitung (v.a. Aluminium), die Elektro-/elektrotechnische Industrie, die maritime Industrie sowie die Baubranche. Darüber hinaus hat auch **Informations- und Kommunikationstechnologie** aus Norwegen nationale und internationale Anerkennung erlangt.

Wirtschaftspolitisch spielt in Norwegen der Staat eine große Rolle. Viele große Wirtschaftsakteure befinden sich in öffentlicher Hand. Hierzu gehören Equinor, der Energieerzeuger Statkraft, die Netzgesellschaft Statnett und der Telekommunikationskonzern Telenor. Dennoch nimmt die staatliche Beteiligung an der Industrie nach und nach ab.[13]

Das norwegische **Bruttoinlandsprodukt** verzeichnete in den vier Jahren vor der Corona-Krise konstante Wachstumsraten. Die Gesamtwirtschaft hatte sich kontinuierlich von der Ölpreiskrise 2015/2016 erholt. Anfang 2020 erfolgte ein erneuter starker Einbruch, verursacht durch die weltweite Corona-Pandemie.

Abbildung 1: Entwicklung des norwegischen Bruttoinlandsproduktes (Festland), saisonbereinigter Volumenindex. 2018 = 100, 2. Quartal 2017 – 4. Quartal 2020



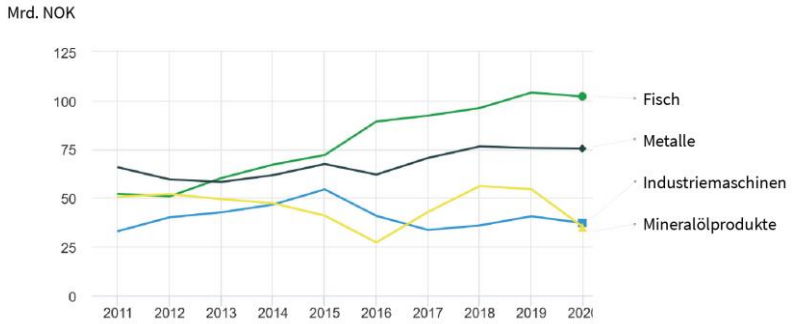
Quelle: SSB, o.D., *Nasjonalregnskap*, tabell 09190, https://www.ssb.no/statbank/table/09190, 09.03.2021.

[11] Norsk Petroleum, 25.03.2021, *Eksport av olje og gas*, http://www.norskpetroleum.no/produksjon-og-eksport/eksport-av-olje-og-gass/, 07.04.2019.
[12] Regjeringen, 04.05.2018, *Gas exports from the Norwegian shelf*, https://www.regjeringen.no/en/topics/energy/oil-and-gas/Gas-exports-from-the-Norwegian-shelf/id766092/, 07.04.2019.
[13] Auswärtiges Amt, *Norwegen: Wirtschaft*, 03.06.2019, https://www.auswaertiges-amt.de/de/aussenpolitik/laender/norwegen-node/-/205866, 12.04.2019.

1.3 Außenhandelsbeziehungen

2020 umfasste der **Warenexport** insgesamt 773,2 Mrd. NOK (ca. 72,1 Mrd. €) – dies entspricht einem Rückgang von -15,5 % im Vergleich zum Vorjahr. Dieser ist u.a. auf die kontinuierlich geschwächte Norwegische Krone (NOK) und den abgestürzten Rohölpreis im ersten Quartal 2021 zurückzuführen. Der Festland-Export lag bei 442,3 Mrd. NOK (ca. 41,3 Mrd. €) und nahm um 6,5 % im Vergleich zu 2019 ab.[14] Hier war der Rückgang bei raffinierten Mineralölprodukten am stärksten, ebenfalls eine Konsequenz des Ölpreisverfalls. **Der Export von Industriemaschinen und -ausrüstungen** ging um 8,8 % zurück und umfasste ein Gesamtvolumen von 37,1 Mrd. NOK (ca. 3,5 Mrd. €).[15] Abbildung 2 gibt die Exportentwicklung der Festlandindustrie seit 2011 wieder.

Abbildung 2: Export von Fisch, Metallen, Maschinen und Raffinerie-Endprodukten, 2011-2020, in Mrd. NOK



Quelle: SSB, 15.01.2021, *Handelsoverskuddet nesten utradert i 2020,* https://www.ssb.no/utenriksokonomi/artikler-og-publikasjoner/handelsoverskuddet-nesten-utradert-i-2020, 10.03.2021.

Der **Import** stieg 2020 leicht um 0,6 % an, insgesamt wurden 2020 Waren und Dienstleistungen im Wert von 762,8 Mrd. NOK (ca. 71,15 Mrd. €) nach Norwegen importiert.[16] Insgesamt erzielte die norwegische Volkswirtschaft somit einen Handelsbilanzüberschuss im Wert von 10,4 Mrd. NOK (ca. 907 Mio. €), dies ist der historisch niedrigste Überschuss seit den 1980er Jahren.[17] Betrachtet man lediglich die norwegische Festlandwirtschaft (exkl. Öl- und Gasindustrie), so erzielte das Land 2020 sogar ein Handelsbilanzdefizit in Höhe von 312 Mrd. NOK (ca. 29,1 Mrd. €).[18]

Zu den Importgütern mit dem stärksten Wachstum im Jahr 2020 gehörten u.a. medizinische Ausrüstungen, Pharmazeutika und Nickelerz. Mit einem Gesamteinfuhrwert von 89,5 Mrd. NOK (ca. 8,35 Mrd. €) **trugen Industriemaschinen und -ausrüstungen** ebenfalls einen wichtigen Anteil am Import. Diese sind u.a. zum Einsatz in zentralen Infrastrukturprojekten und als Produktionsmittel in der Industrie bestimmt. Weitere wichtige Einfuhrgüter sind Fahrzeuge (86 Mrd. NOK bzw. 8 Mrd. €) sowie Metalle und Metallwaren (63,1 Mrd. NOK bzw. 5,9 Mrd. €).[19]

Die **wichtigsten Importpartner** im Jahr 2020 waren die Volksrepublik China (Warenimport im Wert von 92 Mrd. NOK bzw. 8,6 Mrd. €) und Deutschland (Waren- und Dienstleistungsimporte im Wert von 87,5 Mrd. NOK bzw. 8,16 Mrd. €).[20]

Die Abbildungen 3 und 4 stellen die wichtigsten Handelspartner Norwegens dar.

[14] SSB, 27.01.2021, *Utenrikshandel med varer*, https://www.ssb.no/utenriksokonomi/statistikker/muh/aar, 10.03.2021.
[15] SSB, 15.01.2021, *Handelsoverskuddet nesten utradert i 2020,* https://www.ssb.no/utenriksokonomi/artikler-og-publikasjoner/handelsoverskuddet-nesten-utradert-i-2020, 10.03.2021.
[16] SSB, 27.01.2021, *Utenrikshandel med varer*.
[17] SSB, 15.01.2021, *Handelsoverskuddet nesten utradert i 2020.*
[18] SSB, 27.01.2021, *Utenrikshandel med varer*.
[19] SSB, 15.01.2021, *Handelsoverskuddet nesten utradert i 2020.*
[20] Ebd.

Abbildung 4: Wichtigste Handelspartner Norwegens Import, 2020, in %

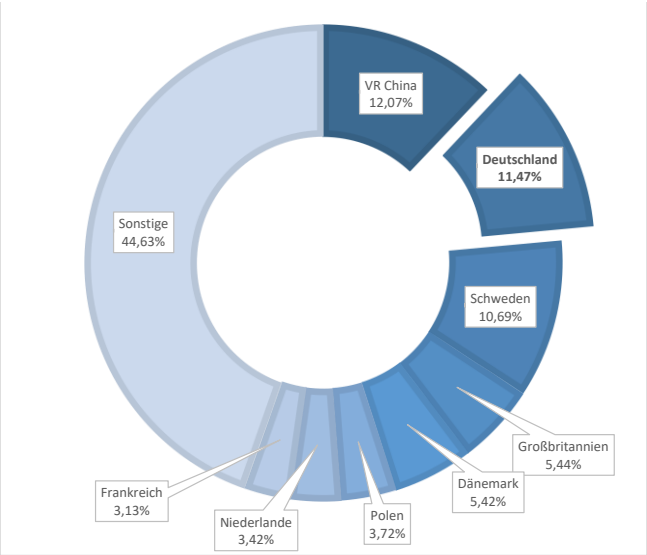
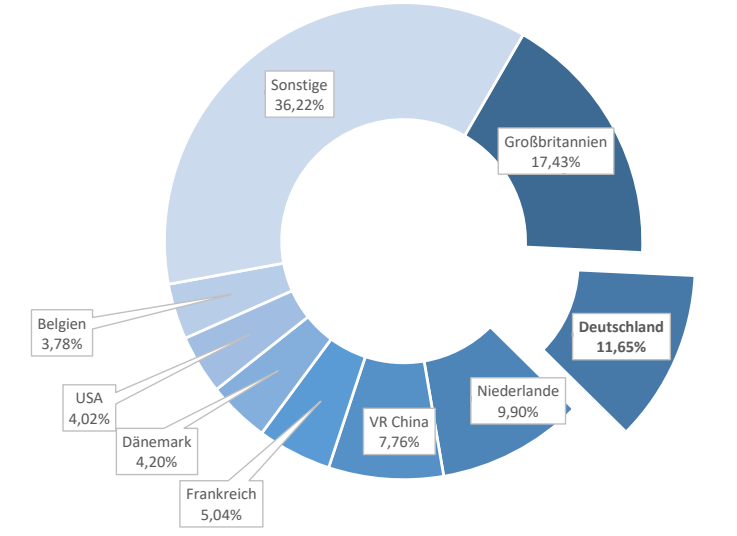


Abbildung 3: Wichtigste Handelspartner Norwegens, Export, 2020, in %



Quelle: SSB, 27.01.2021, *Utenrikshandel med varer*, https://www.ssb.no/utenriksokonomi/statistikker/muh/aar, 11.03.2021. Darstellung: AHK Norwegen

1.3.1 Brexit

Es wird damit gerechnet, dass sich vor allem die Bedeutung Großbritanniens in den Handelsbeziehungen nach Abschluss des Brexits ändern wird. Der norwegische Industrieverband *Norsk Industri* rechnet damit, dass der Brexit **zur Stärkung in den Beziehungen mit den weiteren EWR-Mitgliedsstaaten führen wird**. Dies liegt v.a. an der hier vorhandenen Rechtssicherheit und Vorausschaubarkeit.[21] Im Juli 2021 unterzeichnete Norwegen ein **Freihandelsabkommen mit Großbritannien**. Dabei handelt es sich um das umfangreichste Abkommen dieser Art, welches Norwegen jemals mit einem anderen Staat abgeschlossen hat (ausgenommen dem EWR-Vertrag). Dieses sichert norwegischen Unternehmen einen gleichwertigen Zugang zum britischen Markt verglichen mit den EU-Staaten. Norwegische Industrieunternehmen können somit weiterhin von der Zollfreiheit, die seit über 60 Jahren nach Großbritannien besteht, profitieren. Gleichzeitig ersetzt das Abkommen nicht vollständig die Verbindung, welche Norwegen durch den EWR-Vertrag mit Großbritannien hatte. Die dynamische Entwicklung eines gemeinsamen Regelwerks, welche ein wichtiges Merkmal des EWR-Abkommens ist, fällt mit dem neuen Vertrag weg. Entstehen künftig neue Handelsbarrieren, müssen diese im laufenden Dialog mit Großbritannien geklärt werden.[22]

1.3.2 Wirtschaftsbeziehungen zu Deutschland

Deutschland gehört zu den **bedeutendsten Handelspartnern** Norwegens. Die BRD ist prozentual gesehen hinter Großbritannien der zweitwichtigste Exportpartner und hinter der Volksrepublik China der **zweitwichtigste Importpartner** Norwegens. Nach Deutschland exportiert Norwegen v.a. Gas, Erdöl, Elektrizität, Nichteisen-Metalle und chemische Erzeugnisse. Aus Deutschland wurden 2020 vor

[21] Norsk Industri, 02.01.2021, *Brexit-avtale på plass – hva betyr dette for Norge og Norsk Industri?*, 11.03.2021.
[22] Regjeringen, 08.07.2021, *Undertegnet historisk frihandelsavtale med Storbritannia*, https://www.regjeringen.no/no/aktuelt/undertegnet-historisk-frihandelsavtale-med-storbritannia/id2866032/, 11.10.2021.

allem Maschinen und Transportmittel (ca. 50 Mrd. NOK bzw. 4,7 Mrd. €) sowie chemische Produkte (13 Mrd. NOK bzw. 1,2 Mrd. €) bezogen.[23]

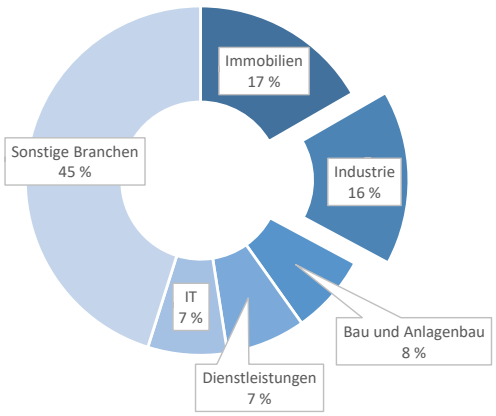
Die norwegische Regierung hat die Bedeutung der wirtschaftlichen und politischen Zusammenarbeit mit Deutschland in ihrer „**Deutschland-Strategie**" verankert. Diese wurde 2019 zuletzt aktualisiert und sieht u.a. vor, dass die Zusammenarbeit zwischen norwegischen und deutschen Universitäten, Hochschulen, Forschungseinrichtungen, Wirtschaftsakteuren und Forschungsgruppen intensiviert werden soll.[24]

Zentrale Projekte der Wirtschaftszusammenarbeit zwischen beiden Ländern sind derzeit u.a. die Unterseekabelverbindung *NordLink* zum Stromaustausch zwischen Deutschland und Norwegen sowie eine strategische Partnerschaft beim Bau von sechs U-Booten. In den Bereichen Anlagenbau und Infrastruktur sind zahlreiche deutsche Unternehmen in Norwegen vertreten, u.a. in der Abfallwirtschaft, der Lebensmittelindustrie in der Holzverarbeitungsindustrie sowie unterschiedlichen Anwendungsfeldern der Transportinfrastruktur.

1.4 Investitionsklima

Die **ausländischen Direktinvestitionen (FDI)** in Norwegen betrugen 2018 1.440 Mrd. NOK (ca. 134 Mrd. €). Dies entspricht einer Steigerung von 91 Mrd. NOK (ca. 8,5 Mrd. €) verglichen zum Vorjahr. Abbildung 5 zeigt, dass 2019 Immobilien (ca. 15 Mrd. NOK bzw. 1,4 Mrd. €) und die Industrie (14,5 Mrd. NOK bzw. 1,35 Mrd. €) zu den beliebtesten und am stärksten wachsenden Investitionsbranchen in Norwegen gehörten.[25]

Abbildung 5: Ausländische Direktinvestitionen in Norwegen, Transaktionen gesamt, 2020, in %.



Quelle: SSB, 20.01.2021, *Størst økning i utenlandske investeringer i eiendom og industri*, https://www.ssb.no/utenriksokonomi/artikler-og-publikasjoner/storst-okning-i-utenlandske-investeringer-i-eiendom-og-industri, 11.03.2021. Darstellung: AHK Norwegen.

Trotz des verhältnismäßig geringen Rückgangs des BIP im Jahr 2020 besteht eine gewisse Zurückhaltung im Hinblick auf Investitionen in der norwegischen Wirtschaft. Für die Industrie wird ein Investitionsrückgang im Umfang von 12 % im Vergleich zu

[23] SSB, o. J., *Utenrikshandel med varer*, tabell 08809, https://www.ssb.no/statbank/table/08809/, 11.03.2021.
[24] Regjeringen, 13.06.2019, *Die Deutschland-Strategie der norwegischen Regierung 2019,* https://www.regjeringen.no/en/dokumenter/deutschland_strategi/id2654427/, 11.03.2021.
[25] SSB, 20.01.2021, *Størst økning i utenlandske investeringer i eiendom og industri,* https://www.ssb.no/utenriksokonomi/artikler-og-publikasjoner/storst-okning-i-utenlandske-investeringer-i-eiendom-og-industri, 11.03.2021.

2020 prognostiziert, die verarbeitende Industrie rechnet sogar mit einem Rückgang der Investitionen von über 20 %. Steigende Investitionen werden u.a. in der Herstellung von Metall, Elektronik und Elektrogeräten erwartet.[26]

[26] Germany Trade & Invest, 18.01.2021, *Unsicherheit drückt Investitionslust*, https://www.gtai.de/gtai-de/trade/specials/special/norwegen/unsicherheit-drueckt-investitionslust-236502, 11.03.2021.

2 Zivile Sicherheit in Norwegen

Auch in der norwegischen Gesellschaft ändern sich die Risiken für die zivile Sicherheit kontinuierlich durch permanente gesellschaftliche Entwicklungen und veränderte äußere Umstände. Durch die gegenseitige Abhängigkeit der kritischen Gesellschaftsfunktionen entstehen komplexere und interdisziplinäre Herausforderungen. Daher sind eine höhere und schnellere Anpassungsfähigkeit sowie Kompetenzen zu Zusammenhängen, Anfälligkeit, Maßnahmen und Effekten gefragt.[27]

Naturereignisse stellen in Norwegen einen wesentlichen Teil des Risikos für die zivile Sicherheit dar. Überschwemmungen, Erdrutsche und Lawinen sowie Waldbrände sind bereits häufige Ereignisse, für die eine steigende Tendenz und Intensität in der Zukunft vorhergesagt wird. Klimatische Änderungen tragen auch zu einer geringeren Vorausschaubarkeit bei. Es wird schwieriger, zu prognostizieren, wo Ereignisse eintreten – hieraus entstehen wiederum Konsequenzen in anderen Lebensbereichen wie Versorgungssicherheit oder Migration. Ferner gehört Norwegen zu den Ländern, die im Bereich der Digitalisierung der wesentlichen Gesellschaftsfunktionen am weitesten vorangeschritten ist – es ist abzusehen, dass sich diese Entwicklung weiter fortsetzt. Dies führt zu neuen Anfälligkeiten und Abhängigkeiten über verschiedene Verantwortungsbereiche und Sektoren hinweg. **Digitale Sicherheit** ist damit ein wichtiger Fokusbereich, um diese Risiken zu minimieren. [28]

2.1 Naturereignisse mit hoher Relevanz für Norwegen

Klimaänderungen und die Folgen von Extremwetterlagen stellen die zivile Sicherheit in vielen Bereichen vor Herausforderungen. Extreme Wetterereignisse treten häufiger und mit höherer Intensität auf – es wird prognostiziert, dass sich diese Entwicklung fortsetzt.[29] Dies trifft auch für Norwegen zu – hier sind vor allem steigende Niederschlagsmengen und -vorkommen mit der Gefahr für Überschwemmungen und Erdrutsche zentrale Problemstellungen. Das norwegische meteorologische Institut (*Meteorologisk Institutt,* MET*)* erwartet steigende Temperaturen und Niederschläge über das gesamte Landesareal in allen Jahreszeiten.[30]

Überschwemmungen

In den letzten 200 Jahren gab es 40-60 größere **Überschwemmungen** in Norwegen – diese treten also relativ häufig mit größeren Konsequenzen auf. Es wird erwartet, dass durch die klimatischen Änderungen bis 2100 weniger Überschwemmungen in Verbindung mit der Schneeschmelze (in Anzahl und Umfang), dafür mehr und häufigere Überschwemmungen durch Regenfälle auftreten. Starke Niederschläge in kurzer Zeit (weniger als zwölf Stunden) sind in den letzten Jahren häufiger und intensiver geworden. Somit werden auch künftig **mehr intensive, lokale Niederschlagsepisoden** erwartet. Dies kann zu einer Überlastung der Leitungssysteme in dicht besiedelten Gebieten führen, was wiederum in Überschwemmungen resultieren kann. Treten solche Perioden mit hoher Niederschlagsintensität häufiger auf, steigt auch die Wahrscheinlichkeit für Erdrutsche und Murgänge (Schlammlawinen). Dies kann auch in Gebieten auftreten, in denen diese Ereignisse bisher noch nicht vorgekommen sind. Die Bewohner vieler Ortschaften erfuhren in den vergangenen Jahren starke Schäden durch plötzlich auftretende Überschwemmungen in kleineren Gewässern oder Wasserläufen.[31]

---

[27] DSB (2021), *DSB årsrapport 2020*, S. 21, https://www.dsb.no/globalassets/dokumenter/rapporter/dsbs-arsrapport-2020.pdf, 19.08.2021.

[28] DSB (2021), *DSB årsrapport 2020*, S. 97, https://www.dsb.no/globalassets/dokumenter/rapporter/dsbs-arsrapport-2020.pdf, 19.08.2021.

[29] DSB (2021), *Analyser av krisescenarioer 2019*, S. 9, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

[30] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 24, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000ddpdfs.pdf, 19.08.2021.

[31] DSB (2019), *Analyser av krisescenarioer 2019*, S. 9, 35, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

Gleichzeitig zeigte der norwegische Sommer im Jahr 2018, geprägt von starker Trockenheit im Süden des Landes und darauf folgenden Waldbränden und Ernteausfällen, die anderen Konsequenzen des Klimawandels. Da die meisten Flächenbrände jedoch immer noch relativ gering ausfallen, wird das Thema Trockenheit in dieser Analyse nicht weiter berücksichtigt.[32]

Erdrutsche und Lawinen

Erdrutsche und Murgänge gehören zu den Naturereignissen mit den meisten Todesopfern in Norwegen. Seit 1900 wurden über 500 solcher Ereignisse mit insgesamt ca. 1.100 Todesopfern registriert. Die meisten dieser waren bei Schneelawinen zu beklagen, gefolgt von Felsstürzen und Erdrutschen bedingt durch Quickton. Schneelawinen finden in dieser Analyse keine weitere Erwähnung.[33]

Durch das staatliche Programm zum Mapping für **Felsstürze** werden instabile Felspartien ermittelt. Ein detailliertes Mapping instabiler Felsgebiete wird für die Regionen Troms, Møre og Romsdal, Sogn og Fjordane sowie teilweise in den Regionen Telemark und Rogaland vorgenommen. Dieses soll dazu dienen, Gefahren bei Flächenplanungsvorhaben in Betracht zu ziehen und Maßnahmen zur Risikominimierung zu eruieren. Die Überwachung großer, instabiler Felspartien wird durch die staatliche Gewässer- und Energiebehörde durchgeführt (*Noregs vassdrags- og energidirektoratet,* nachfolgend NVE). In diesem Rahmen wurden sieben Gebiete als „Hochrisikoobjekte» identifiziert, diese unterliegen somit einer ununterbrochenen Überwachung mit zugehörigen Bereitschaftsleistungen. Dies sind die Felspartien Åknes, Hegguraksla und Mannen im Verwaltungsbezirk Møre og Romsdal, Joasetbergi in Sogn og Fjordane sowie Jettan, Indre Nordnes und Gámanjunni in der Region Troms. Ein Felssturz in diesen Gebieten würde mehrere tausend Menschen treffen. In vier der sieben Hochrisikogebieten besteht auch eine **Gefahr für Flutwellen,** da ein Felssturz im Fjord enden würde. Daher wurden auch Unterspülungsgebiete untersucht, basierend auf das Volumen der instabilen Felsen und der berechneten Höhe der Flutwellen.[34]

Felsstürze gehören zu den bedrohlichsten Naturkatastrophen, welche in Norwegen eintreffen können. Größere Felsstürze sind selten, aber der Schadensumfang kann umso höher sein. In der Vergangenheit gab es zwei bis vier Felsstürze pro Jahrhundert mit Todesopfern. Die letzten größeren Felssturz-Unglücke gab es in den 1930er Jahren in Tafjord und Loen in Westnorwegen, bei denen 40 bzw. 73 Personen ums Leben gekommen sind. Hierbei sind größere Felspartien kollabiert und in den Fjord gestürzt – dies führte zu enormen Flutwellen mit einer hohen Reichweite und katastrophalen Konsequenzen für Menschen, Gebäude, Tiere und bewirtschaftete Felder.[35] In den vergangenen Jahren erhielt die Felspartie „Mannen“ hohe mediale Aufmerksamkeit. Dabei handelt es sich um einen 1294 m hohen Felsen in der Region Romsdalen. Diese Felspartie gehört zu den am strengsten überwachten Gebieten in Norwegen und wird sehr genau von Geologen des NVE überwacht. Nach vielen Jahren geprägt von Evakuierungen und sich ständig ändernden Gefahrenlagen rutschten 2019 nach hohen Niederschlagsmengen Teile des Felsens ab. Nach diesem Ereignis wurde die Lage offiziell als weniger gefährlich eingeschätzt und die Bewohner konnten wieder ihre Häuser beziehen.[36]

In Schweden und Norwegen gibt es eine besondere Gefahr für **Erdrutsche bedingt durch Quickton**. Eine Überbelastung des Quicktonbodens kann dazu führen, dass der Ton seine Substanz verliert und wie eine Flüssigkeit davonfließt.[37] In Norwegen befinden sich die größten Vorkommen an Quickton im östlichen Teil des Landes und in der Region Trøndelag. Es gibt jedoch auch geringere Vorkommen in marinen Ablagerungen entlang der gesamten norwegischen Küste. Hierdurch entsteht eine Gefahr in weiten Landesteilen. Bisher wurden über 2.000 Quickton-Zonen mit potenzieller Gefahr für größere Erdrutsche in Norwegen identifiziert. Aktuell werden diese Zonen von ca. 140.000 Personen bewohnt, darüber hinaus befinden sich dort andere Bebauungen wie Schulen,

[32] DSB (2019), *Analyser av krisescenarioer 2019*, S. 9, 81, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

[33] DSB (2019), *Analyser av krisescenarioer 2019*, S. 54, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

[34] DSB (2019), *Analyser av krisescenarioer 2019*, S. 54, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

[35] DSB (2019), *Analyser av krisescenarioer 2019*, S. 53, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

[36] Forskning.no, 10.09.2019, *Hva skjer med resten av Mannen nå?*, https://forskning.no/geologi/hva-skjer-med-resten-av-mannen-na/1560028, 20.08.2021.

[37] NGI, o. J., *Kvikkleireskred i Norge*, https://www.ngi.no/Tjenester/Fagekspertise/Kvikkleireskred/Kvikkleireskred-i-Norge, 20.08.2021.

Kindergärten, Industrie und Gewerbe. Zehn Quicktonzonen liegen in dicht besiedelten und bebauten Gebieten. Es gibt weiterhin Gebiete mit Potenzial für größere Quickton-Erdrutsche, welche noch nicht identifiziert worden sind.[38]

Risikoanalyse zu Quickton-Erdrutschen in norwegischen Städten

Die Risikoanalyse zu Quickton-Erdrutschen in Städten der norwegischen Sicherheitsbehörde DSB (*Direktoratet for samfunnssikkerhet og beredskap;* im folgenden DSB) zeigt in aller Deutlichkeit, wie katastrophal ein solches Ereignis in dicht besiedelten Gebieten enden kann. In dieser Analyse wird ein Szenario eines Erdrutsches im Gebiet Øvre Bakklandet in Trondheim im Umfang von 10x100 m dargestellt. Es folgt eine Evakuierung am folgenden Tag und in der darauffolgenden Nacht wird ein größerer Erdrutsch im Umfang von 3 Mio. m^3 ausgelöst. Dieser führt unmittelbar zu einer Flutwelle (flussauf- und flussabwärts) im Fluss Nidelva, von welchem die Bebauung entlang des Flusses betroffen ist. Durch den Erdrutsch entsteht ein vollständiger Aufstau des Flusses und der Pegel des Flusses steigt um 12 m. Auf dem ca. 0,5 km^2 großen Gebiet mit durch den Erdrutsch gelockerten Grund leben ca. 2.000 Einwohner. Ein Areal von ca. 1,5 km^2 mit ca. 1.000 Einwohnern im Stadtzentrum von Trondheim wird überschwemmt. Die Konsequenzen dieses Szenarios werden als sehr schwerwiegend bewertet – es werden ca. 200 Todesopfer und 500 Schwerverletzte angenommen. Mehrere geschützte Kulturdenkmäler werden irreparabel beschädigt und die direkten ökonomischen Verluste werden auf ca. 30 Mrd. NOK (ca. 2,9 Mrd. €) geschätzt. Kritische Infrastrukturen wie das Strom- und Kommunikationsnetz sowie Straßen und Schienen sind komplett beschädigt und ein Wiederaufbau der wichtigsten Funktionen dauert mindestens einen Monat.

DSB (2019), *Analyser av krisescenarioer 2019*, S. 60-63, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

Erdrutsche durch Quicktonmassen sind aufgrund des verheerenden Erdrutsches am 30.12.2021 in Ask, nördlich von Oslo, in Norwegen ein sehr aktuelles Thema. Hierbei sind zehn Menschen ums Leben gekommen, durch den Erdrutsch wurden insgesamt neun Wohngebäude mit über 30 Wohnungen komplett zerstört. Laut NVE war dies einer der größten Quickton-Erdrutsche in Norwegen. Viele Bewohner in diesem Gebiet, die inzwischen wieder ihre Häuser bezogen haben, fühlen sich in diesen immer noch nicht sicher. NVE bestätigt hingegen, dass die Gebäude sicher sind. Daher hat der norwegische Staat eine finanzielle Unterstützung für die Bewohner genehmigt, falls diese bis Ende 2021 an einem anderen Ort leben möchten.[39]

Stürme und Orkane

Heftiger Wind in Sturm- oder Orkanstärke mit zugehörigen Windböen sind jene Extremwetterlagen, welche in die größten Schäden verursachen – insbesondere in Kombination mit Sturmfluten, die aufgrund eines Anstiegs des Grundwasserpegels durch starken Wind und niedrigen Luftdruck entstehen. Verschiedene Klimamodelle zeigen nur wenig oder gar keine Änderungen der durchschnittlichen Windverhältnisse in Norwegen bis 2100. Gleichzeitig wird es in den kommenden Jahren eine Tendenz zu einer etwas höheren Wahrscheinlichkeit für starke Stürme und Orkane geben. Dies trifft auch für Regionen zu, die bisher nicht von diesen Extremwetterereignissen betroffen waren, wie z.B. die Region um den Oslofjord. Es kann künftig z.B. auch starker Wind aus unerwarteten oder vorher nicht dagewesenen Windrichtungen vorkommen. Dies kann zu Schäden an Gebäuden und Gefahr für Leib und Leben führen. Dies kann sich auch auf die Energieinfrastruktur auswirken (z.B. Beschädigung der Stromleitungen). Da viele gesellschaftliche Grundfunktionen von einer kontinuierlichen Stromzufuhr abhängig sind, können länger andauernde **Stromausfälle** starke Herausforderungen mit sich bringen. Treten Stürme oder Orkane gemeinsam mit hohen Niederschlagsmengen auf, kann dies auch Konsequenzen für das **Wasser- und Abwassersystem** haben.[40]

[38] DSB (2019), *Analyser av krisescenarioer 2019*, S. 11, 54, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

[39] NRK, o. J., *Leirskredet i Gjerdrum*, https://www.nrk.no/nyheter/leirskredet-i-gjerdrum-1.15307406, 20.08.2021.

[40] DSB (2019), *Analyser av krisescenarioer 2019*, S. 35, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

2.2 Risikobewertung verschiedener Naturereignisse

Die staatliche Sicherheitsbehörde DSB gibt jährlich eine Analyse verschiedener Krisenszenarien heraus. In diesen werden Risiken in Verbindung mit katastrophalen Ereignissen, auf welche die norwegische Gesellschaft vorbereitet sein sollte, beleuchtet. Das Dokument umfasst Naturereignisse, größere Unglücke und beabsichtigte Handlungen. Die Analyse betrachtet mehrere Sektoren und Verwaltungsniveaus, um Kenntnisse und Bewusstsein für mögliche Szenarien und deren Konsequenzen zu fördern.[41] Die Risikobewertungen für die verschiedenen Ereignissen werden in Anhang 1 dargestellt. Die dunkelblau hervorgehobenen Säulen kennzeichnen die Erkenntnisse aus neuesten Analysen. Aus der Graphik geht hervor, dass Brände in unterirdischen Tunnels sowie Überflutungen durch Regenfälle die wahrscheinlichsten Ereignisse sind.

2.3 Digitale Sicherheit in kritischen Gesellschaftsfunktionen

Norwegen ist eines der digitalisiertesten Länder der Welt und sehr weit vorangeschritten im Hinblick auf das Angebot digitaler Dienstleistungen. Steuererklärungen werden elektronisch eingereicht, Pensionen werden online beantragt und Lebensmittel mit dem Mobiltelefon gezahlt. Der Alltag der Norweger ist digital – v.a. zum Vorteil von Privatpersonen, Unternehmen und der Verwaltung. Gleichzeitig entstehen mit dieser Entwicklung auch Risiken. Immer mehr Geräte, Prozesse und Dienstleistungen sind von einer funktionierenden IT-Infrastruktur und Internetverbindung abhängig; gleichzeitig steigen die Datenmengen, die generiert und gespeichert werden müssen. Laut der nationalen Sicherheitsbehörde (*Nasjonal Sikkerhetsmyndighet,* nachfolgend NSM) ist die steigende Komplexität der digitalen Systeme und Wertschöpfungsketten eine wichtige Ursache dafür, dass auch die Anfälligkeit für digitale Risiken steigt.[42] Die Gesellschaft ist davon abhängig, dass kritische Funktionen funktionell bleiben und es wird vorausgesetzt, dass die digitalen Infrastrukturen, welche diese unterstützen, jederzeit und überall funktionieren. Ein Risikoereignis kann in einer bestimmten Infrastruktur auftreten und Konsequenzen für ein anderes digitales Ökosystem mit sich führen. Solche gegenseitigen, sektorübergreifenden Abhängigkeiten stellen somit eine besondere Herausforderung für die Sicherheit verschiedener digitaler Infrastrukturen dar.[43]

Laut der NSM sind E-Mails die dominierende Methode für Cyber-Angriffe.[44] Die Corona-Pandemie hat gezeigt, wie abhängig moderne Gesellschaften von digitalen Lösungen sind. Die steigende Anzahl an **Phishing-Versuchen** und das strategische Ausnutzen der pandemischen Situation digitaler Angreifer wurde in mehreren Ländern beobachtet. Sicherheitsmaßnahmen, die in anderen Ländern umgesetzt worden sind, treffen auch auf Norwegen zu. Dazu gehört z.B. das verstärkte Teilen von Informationen und Maßnahmen zu einem besseren Verständnis der Situation. Im Zuge der Pandemie gab es einen besonderen Bedarf für Ratschläge und Warnungen, die an die Situation angepasst wurden. In Norwegen wurde dies durch eine enge Zusammenarbeit zwischen NSM und dem Gesundheitssektor zu Maßnahmen, darunter die Platzierung mehrerer VDI-Sensoren, umgesetzt.[45]

Die digitale Welt bietet Cyberkriminellen Möglichkeiten für Hacking, Spionage, digitale Angriffe und Beeinflussungskampagnen. In norwegischen Behörden und Unternehmen wurde in den vergangenen Jahren eine steigende Anzahl zielgerichteter Datenschutzverletzungen beobachtet. Besonders anfällige Ziele sind die Organe der norwegischen Staatsverwaltung, Technologieunternehmen mit einer weltmarktführenden Position in ihrem Segment sowie Unternehmen, welche eng mit den

---

[41] DSB (2019), *Analyser av krisescenarioer 2019*, S. 5, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 11.10.2021.

[42] DSB (2019), *Analyser av krisescenarioer 2019*, S. 197, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021; JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 27-28, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 19.08.2021.

[43] Departementene (2019), *Nasjonal strategi for digital sikkerhet*, S. 15, https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf, 23.08.2021.

[44] DSB (2019), *Analyser av krisescenarioer 2019*, S. 197, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 30.08.2021

[45] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 79, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 30.08.2021.

kritischen Infrastrukturen verwoben sind.[46] Cyberangriffe gegenüber **kritischen Gesellschaftsfunktionen** können schwerwiegende Konsequenzen für einen großen Teil der Gesellschaft mit sich bringen. Dies gilt insbesondere für die Energieversorgung oder die Telekommunikation.[47]

2.3.1 Infrastruktur

Energieinfrastruktur

Die **Energieversorgung ist der Grundstein der modernen norwegischen Gesellschaft** und gleichzeitig die wichtigste und kritischste Infrastruktur des Landes.[48] Da ein hoher Teil des Energieverbrauchs auf Strom zurückgeht, ist kein anderes Land so abhängig von Elektrizität. Das Land ist ein wichtiger Standort für energieintensive Industrien, ferner wird Strom in hohem Maße für die Beheizung von Gebäuden und Warmwasser verwendet.[49] Norwegen ist außerdem das Land mit den weltweit meisten Elektroautos pro Einwohner.[50] Ein Versagen der Stromversorgung bringt Konsequenzen für alle gesellschaftlichen Sektoren und digitalen Systeme, von denen die gesamte Gesellschaft abhängig ist, mit sich.

Die Aufmerksamkeit des DSB im Bereich der Sicherheit der Stromversorgung wächst im Gleichschritt mit der zunehmenden Abhängigkeit der Gesellschaft von Elektrizität in verschiedensten Lebensbereichen. Dies ist eine gesteuerte und gewünschte Entwicklung im Hinblick auf den Übergang zu erneuerbaren Energien durch Klimaänderungen und neue Technologien, Effizienzsteigerung und eine bessere Verfügbarkeit durch Digitalisierung. Für die Sicherheit in der Elektrizitätsversorgung bedeutet dies neue Herausforderungen, da die Aktivitäten und die Komplexität in den verwandten Branchen zunehmen: Neue Technologie soll im norwegischen Stromnetz funktionieren und die Gesellschaft wird verwundbarer, je mehr neue Anwendungsfelder für Elektrizität entstehen.[51]

Auch wenn die norwegische Stromversorgung sehr sicher ist, kann eine vollständige Versorgungssicherheit zu keinem Zeitpunkt garantiert werden. Ein wichtiger Meilenstein war die Einführung digitaler Zähler- und Abrechnungssysteme. Im Zuge dieses Roll-Outs wurden bis Anfang 2019 bei allen norwegischen Stromkunden ein digitaler Stromzähler, der mit dem jeweiligen Netzbetreiber kommunizieren kann, installiert. Damit hat sich auch in der Energiebranche die Nutzung von IT-Systemen und -infrastrukturen deutlich erhöht. Die digitalen Zähler versorgen die Netzbetreiber mit genaueren Informationen zum Status und Zustand im Übertragungsnetz. Gleichzeitig verstärkt der Roll-out der Zählersysteme die Abhängigkeit zwischen der Energieversorgung und Telekommunikationssektor. Die Energieversorger und Netzbetreiber nutzen in hohem Maße die Dienste der kommerziellen Kommunikationsanbieter, um die Signale der Zähler an die Netzgesellschaften zu kommunizieren. Diese Entwicklung hat dazu geführt, dass eine hohe Betriebssicherheit in der Energieversorgung, darunter auch die IT-Sicherheit, noch zentraler in der Gesellschaft und in der Branche geworden ist.[52]

---

[46] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 28, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 19.08.2021.

[47] DSB (2019), *Analyser av krisescenarioer 2019*, S. 197-199, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

[48] DSB (2021), *DSB årsrapport 2020*, S. 48, https://www.dsb.no/globalassets/dokumenter/rapporter/dsbs-arsrapport-2020.pdf, 23.08.2021.

[49] Energifakta Norge, 20.08.2021, *Energibruken i ulike sektorer*, https://energifaktanorge.no/norsk-energibruk/energibruken-i-ulike-sektorer/. 23.08.2021.

[50] Regjeringen, 10.06.2021, *Norge er elektrisk*, https://www.regjeringen.no/no/tema/transport-og-kommunikasjon/veg_og_vegtrafikk/faktaartikler-vei-og-ts/norge-er-elektrisk/id2677481/, 23.08.2021.

[51] DSB (2021), *DSB årsrapport 2020*, S. 48, https://www.dsb.no/globalassets/dokumenter/rapporter/dsbs-arsrapport-2020.pdf, 23.08.2021.

[52] Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning (2015), *NOU Digital sårbarhet – sikkert samfunn*, S. 129, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf, 23.08.2021.

Elektronische Kommunikationsinfrastruktur (Telekommunikation)

Die Wertschöpfungskette der elektronischen Kommunikation erstreckt sich über die verschiedenen Ebenen des Telekommunikationsnetzes. An der Spitze aller Telekommunikationsdienstleistungen stehen die sogenannten *over the top*-Dienstleistungen, welche häufig von Akteuren angeboten werden, die traditionell nicht der Kommunikationsbranche zugeordnet werden und die daher oft keiner regulatorischen Kontrolle unterliegen. Einige Akteure bieten Dienste entlang der gesamten Wertschöpfungskette. Zentralster Dienstleister ist Telenor, der ursprünglich nationale norwegische Telekommunikationsbetreiber. GlobalConnect betreibt ein beinahe landesweites Netz, welches im Wesentlichen den Eisenbahnlinien folgt. Altibox, ein Konglomerat aus mehreren Energieunternehmen, ist ebenfalls ein Totallieferant mit einer eigenen Infrastruktur.[53]

Die Akteure stehen in ständiger Interaktion miteinander durch Handel, die Vermietung von Glasfaserkabeln, gleichzeitig werden Kabel in gemeinsamen Schächten verlegt. Dies kann zum Teil zu Ausfällen bei mehreren Anbietern führen, wenn Kabel z.B. bei Bauarbeiten beschädigt werden. Akteure, welche die Infrastruktur für Zugangsnetze ausbauen, nutzen hauptsächlich die Kernnetzinfrastruktur von Telenor oder GlobalConnect. Dies führt zu einigen grundlegenden digitalen Verwundbarkeiten in der Infrastruktur für die elektronische Kommunikation in Norwegen:

- **Gemeinsame Verbindungsinfrastruktur**
  Die Kernnetzinfrastruktur von Telenor stellt das Rückgrat der Telekommunikationsinfrastruktur dar und ist somit ein sehr kritisches Element. Ein Großteil der Infrastruktur besteht aus Lichtleitfaser. In einigen Fällen werden auch Funk- oder Satellitennetze verwendet.
- **Zentralisierte Netzfunktionen**
  Die Telekommunikationsdienste sind abhängig von zentralisierten Funktionen.
- **Akkumulierte Anfälligkeit**
  Anfälligkeiten im Telekommunikationsnetz werden dadurch akkumuliert, dass Kabel von mehreren Anbietern im gleichen Schacht verlegt wird, oder indem Ausrüstung an gemeinsamen Masten oder Telezentralen montiert wird. Anfälligkeiten werden auch durch Kauf und Verkauf von Diensten oder die Vermietung von Infrastrukturen zwischen einzelen Akteuren akkumuliert und getarnt.[54]

Auch die Tatsache, dass beinahe jegliche elektronische Kommunikation vom Transportnetz von Telenor abhängig ist, stellt eine Verwundbarkeit dar. Die norwegische Regierung hat daher ein Pilotprojekt ins Leben gerufen, um ein zusätzliches nationales Netz für die Übertragung von Daten und Telekommunikation zu errichten.[55]

Tabelle 2 stellt die Bewertung der Konsequenzen eines Ausfalls der Telekommunikation für kritische Gesellschaftsfunktionen durch die Behörde DSB dar. Wie darin zu erkennen ist, sind der Transport-, Gesundheits- und Finanzsektor am stärksten von einem Zusammenbruch der elektronischen Kommunikation betroffen.

Tabelle 2: Abhängigkeit zentraler gesellschaftlicher Funktionen von elektronischer Kommunikation

Funktion	Grad der Konsequenzen eines Telekommunikations-Ausfalls	Erklärung
Energieversorgung	Gering	Energieversorgung in geringem Grad betroffen, fehlende Fehlerbehebung bei Stromausfällen

[53] Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning (2015), *NOU Digital sårbarhet – sikkert samfunn*, S. 107, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf, 23.08.2021.

[54] Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning (2015), *NOU Digital sårbarhet – sikkert samfunn*, S. 107, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf, 23.08.2021.

[55] DSB (2019), *Analyser av krisescenarioer 2019*, S. 10, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

Straßenverkehr	Moderat	Fehlende Überwachung von Tunnels, ausbleibende Verkehrswarnungen, moderate Verspätungen
Schienenverkehr	Hoch	Kompletter Ausfall des Zugverkehrs
Küstenschifffahrt	Moderat	Moderate Verspätungen
Zentrales Krisenmanagement	Hoch	Mangelhafte Koordinierung und Information ohne Telefon, Internet, Radio und TV. Notfalllösungen mit begrenzter Kapazität.
Wasserversorgung	Gering	Wasserversorgung ist nur in geringem Maß betroffen.
Bank- und Finanzwesen	Hoch	Keine Finanztransaktionen, begrenzte Nutzung von Zahlungsterminals.
Gesundheit und Pflege	Hoch	Krankenhäuser und Notaufnahmen ohne Kontakt zur Außenwelt, reduzierte Effektivität, verzögerte Behandlungen
Notrufzentralen	Hoch	Krankentransport, Polizei, Feuerwehr können nicht erreicht werden über Notrufnummern. Mangelhafte Koordinierung von Einsätzen.
Kommunikationssystem für die öffentliche Sicherheit (*Nødnett)*	Hoch	Das System funktioniert nur lokal.

Quelle: Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning (2015), *NOU Digital sårbarhet – sikkert samfunn*, S. 108, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf, 23.08.2021.

Nødnett: Ein digitales, nationales Kommunikationssystem

Das nationale Kommunikationssystem für die öffentliche Sicherheit, das sog. *Nødnett,* verknüpft die Dienste der Polizei, der Feuerwehr und des Rettungsdienstes sowie andere Akteure mit verantwortlichen Rollen in der Notfallbereitschaft miteinander. Das *Nødnett* verfügt seit 2015 über eine landesweite Reichweite und ermöglicht die sichere Kommunikation sowohl innerhalb als auch zwischen den einzelnen Akteuren. Die nationale Sicherheitsbehörde DSB besitzt, betreibt und verwaltet das Netz im Auftrag des norwegischen Justizministeriums. Der Ausbau des *Nødnett* ist eine der größten Investitionen in die zivile Sicherheit in Norwegen, die jemals getätigt worden sind und repräsentiert eine deutliche Steigerung der Notfall- und/oder Katastropenbereitschaft.[56] Hauptauftragnehmer für den Netzausbau war **Nokia Siemens Networks Norge AS**, gemeinsam mit **Motorola** und **Frequentis** als Kooperationspartner.[57]

Die **Feuerwehr**, der **Rettungsdienst**, **Notärzte** und die **Polizei** werden als „Kernnutzer" des nationalen Sicherheits-Kommunikationsnetzes gezählt. Die Verknüpfung mehrerer Nutzer ermöglicht ein besseres Teilen von Informationen und eine erhöhte Koordination dieser. Neben den Kernnutzern wird das Netz auch von freiwilligen Organisationen, staatlichen Akteuren, Kommunen, Organisationen der Arbeits- und Betriebssicherheit sowie Energieerzeugern genutzt.

Durch das *Nødnett* können die Nutzer in Gruppen über einzelne Organisationen und über geographische Grenzen hinweg sowie innerhalb der eigenen Organisation kommunizieren. Es ermöglicht den beteiligten Helfern, am Ort des Geschehens oder der benötigten Hilfe miteinander zu kommunizieren. Durch das *Nødnett* können Helfer einander finden und ein gemeinsames Verständnis für die jeweilige Notsituation entwickeln.

Das *Nødnett* folgt dem TETRA-Standard und wurde entwickelt, um die Bedarfe bei kritischer Kommunikation zu decken. Das TETRA-Netz bietet eine sichere, verschlüsselte Funkkommunikation innerhalb vorab definierter Gruppen, in 1:1-Gesprächen oder durch Textnachrichten.

Das Kernnetz steuert den gesamten Datenverkehr im *Nødnett,* hier steckt also die eigentliche Intelligenz des Netzes. Das Kernnetz und die Funkbasen sind durch ein **Transmissionsnetz** miteinander verknüpft. In diesem werden Signale durch physische Kabel und

[56] Nodnett.no, o. J., *Hva er Nødnett?*, https://www.nodnett.no/om-nodnett/hva-er-nodnett/, 14.10.2021.

[57] Regjeringen.no, *Prop. 100 S (2010–2011) Fullføring av utbygging og drift av Nødnett i hele Fastlands-Norge,* https://www.regjeringen.no/no/dokumenter/prop-100-s-20102011/id640914/?ch=5, 14.10.2021.

über Funksignale in der Luft gesendet. Das *Nødnett* verfügt über kein eigenes Transmissionsnetz, sondern nutzt die **kommerzielle Infrastruktur**, welche hauptsächlich im Besitz von Telenor ist.

Die Kernfunktionalität des *Nødnett* ist die sichere, schnelle und robuste Herstellung von Gesprächsverbindungen in vorab definierten Gesprächsgruppen. Durch die Nutzung dieser Gruppen werden die Ressourcen im Netz sehr effektiv genutzt und die Netzkapazität nur in sehr geringem Maß belastet.

Das *Nødnett* beinhaltet auch mehrere integrierte Mechanismen, um eine Kommunikation auch bei einem Netzausfall zu gewährleisten:

- Mit einer redundanten Ringstruktur, doppelten Komponenten und einer sich überschneidenden Netzabdeckung gebaut
- Stabile Reservestromkapazität an den Basisstationen. Alle Basen verfügen über mindestens acht Stunden Notstrom
- Alle Basen im *Nødnett* verfügen über mindestens zwei Funkapparate, welche wiederum vier Kanäle haben (einen für Kontrollsignale, drei für Gespräche). Pro Funkapparat können also drei gleichzeitige Gespräche stattfinden.[58]

Ausbau des 5G-Netzes

Der Ausbau des 5G-Netzes ist in Norwegen bereits gut vorangeschritten. Im März 2020 war die norwegische Technologiehauptstadt Trondheim die erste in Norwegen mit einer 5G-Abdeckung. Derzeit wird das 5G-Netz auch in Oslo, Stavanger und Bergen ausgebaut. Hierfür sind die Telekommunikationsbetreiber **Telenor**, **Telia** und **Ice** verantwortlich. Bis Ende 2024 soll der landesweite 5G-Roll-out abgeschlossen sein.[59] Die 5G-Technologie ist eine wichtige Voraussetzung für die Nutzung von Sensortechnologie und den Umgang mit Big Data sowie dem Internet of Things. Technologien für das Gesundheitswesen, Smart Cities und smarte Transportsysteme sind nur einige Beispiele dafür, wie das Internet of Things Möglichkeiten für eine erhöhte Wertschöpfung und mehr Produktivität schafft. Auch auf die Sicherheit im Hinblick auf Naturereignisse hat der Ausbau des 5G-Netzes Auswirkungen – so z.B. ebnet dieser den Boden für die Nutzung von Sensoren zur Hochwasserwarnung, den Pegelstand in einzelnen Kommunen oder die Überwachung in Lawinen- oder erdrutschgefährdeten Gebieten. Das 5G-Netz ermöglicht eine schnellere Datenübertragung, sodass dieses auch die Voraussetzungen für autonome Fahrzeuge oder die Nutzung von IoT-Technologien in der Industrie geschaffen werden. Das 5G-Netz wird in höherem Maß cloudbasiert funktionieren und deutlich mehr Akteure miteinander verknüpfen – dies führt somit auch eine höhere Gefahr vor verschiedenen digitalen Gefahren mit sich.[60]

2.3.2 Informations- und Kommunikationstechnik im Gesundheitssektor

Im Vergleich zu anderen Ländern war Norwegen auch bei der Nutzung von Informations- und Kommunikationstechnik (IKT) im Gesundheitswesen eines der Vorreiterländer. Das staatliche Organ ***Norsk Helsenett***, dessen Aufgabe es ist, ein Kommunikationsnetz für das Gesundheitswesen bereitzustellen und für den sicheren Austausch von Patienteninformation und -kommunikation zu sorgen, wurde bereits 2004 gegründet. *Norsk Helsenett* wurde errichtet, um eine standardisierte Infrastruktur für die elektronische Interaktion im Gesundheits- und Pflegesektor bereitzustellen. Übergeordnete Dienstleistungen und Sicherheitsroutinen können somit standardisiert werden. Das Gesundheitsnetz ist z.B. die Kommunikationsinfrastruktur für die digitale Patientenakte oder E-Rezepte.[61]

Die schnelle Entwicklung im Bereich der **Gesundheits- und Sozialtechnologie** bietet vielerlei neue Möglichkeit, sorgt aber auch für eine höhere Anfälligkeit – sowohl bei den Gesundheitsdienstleistern selbst als auch bei den Endverbrauchern, welche digitale

[58] Nodnett.no, o. J., *Hva er Nødnett?*, https://www.nodnett.no/om-nodnett/hva-er-nodnett/, 14.10.2021.

[59] Forskning.no, 04.03.2021, *Hva er egentlig 5G?*, https://forskning.no/internett-mobiltelefon/hva-er-egentlig-5g/1813874, 30.08.2021.

[60] Alt om samfunnssikkerhet, 09.03.2021, *Sikkerhet i Neste Generasjon Nødnett*, https://www.altomsamfunnssikkerhet.no/samfunnssikkerhet-og-beredskap/sikkerhet-i-neste-generasjon-nodnett/, 30.08.2021.

[61] Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning (2015), *NOU Digital sårbarhet – sikkert samfunn*, S. 185, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf, 23.08.2021.

Gesundheitsdienste von zu Hause aus nutzen. Um mögliche Angriffsflächen zu reduzieren, wird hier die Notwendigkeit einer stärkeren Kontrolle dieser Entwicklung hervorgehoben.[62]

2.3.3 Finanzwesen

Finanzielle Dienstleistungen sind eine kritische Funktion mit hoher Bedeutung für Wirtschaft und Verbraucher. In diesem Bereich werden immense Vermögenswerte verwaltet und es treten häufige Versuche von Internetbetrug auf. Laut DSB ist daher die Motivation cyberkrimineller Akteure für umfassende Angriffe auf die finanzielle Infrastruktur hoch. Der Finanzsektor hat sich in den vergangenen Jahrzehnten durch die Einführung digitaler Lösungen stark verändert.[63] Die norwegische Finanzwirtschaft hat in der Vergangenheit stark unternehmensübergreifend zusammengearbeitet, um IKT-Lösungen zu standardisieren. Dadurch wurden interne Prozesse effektivisert. So z.B. liegen die norwegischen Akteure weit vorn im digitalen Kundenmanagement. Dies hat eine Komplexität der IKT-Systeme und Wertschöpfungsketten mit sich geführt, welche die Branche für absichtliche und unabsichtliche Ereignisse anfällig macht. Gleichzeitig gibt es eine steigende Tendenz in der internationalen, organisierten Kriminalität. Diese richtet sich sowohl an internetbasierte Distributionskanäle, aber auch an mobile Lösungen oder an Kunden-Kontaktpunkte wie Ladengeschäfte oder Online-Shops.[64]

Ferner gehört Norwegen zu den Staaten, in denen am meisten **elektronische Zahlungsmittel** genutzt werden. Barzahlungen machen einen immer kleineren Teil der Transaktionen aus. Auch diese Entwicklung repräsentiert eine gewisse Verwundbarkeit. Durch ein neues Regelwerk sind die Banken verpflichtet, auf die Verteilung von Bargeldnoten vorbereitet zu sein. Dennoch ist davon auszugehen, dass die Verteilung hoher Bargeldmengen an Unternehmen und die Bevölkerung in einer Krisensituation herausfordernd ist. Ferner handelt es sich dabei um einen Prozess, der nicht in vollem Umfang erprobt werden kann.[65]

Die Beschreibung der Anfälligkeiten in den einzelnen Sektoren und Infrastrukturen zeigt in aller Deutlichkeit, dass Norwegen eine breite digitale Angriffsfläche bietet, welche kontinuierlich wächst. Ferner wird diese Situation immer komplexer durch den hohen Entwicklungstakt in den digitalen Märkten in denen Lieferanten ausgetauscht und Unternehmen aufgekauft werden sowie fortlaufend neue Technologien aufkommen.[66]

2.4 Öffentliche Verwaltung

2.4.1 Zuständigkeiten

Für die Prävention von Schäden durch Hochwasser und Erdrutsche sind viele Akteure verantwortlich. Die **Kommunen** tragen eine grundlegende Verantwortung dafür, dass Naturgefahren, darunter Überschwemmungen und Erdrutsche beobachtet und bei Flächenplanungs- und Bauvorhaben berücksichtigt werden. Die **Verwaltungsbezirke** (*Fylkeskommuner*) sind durch die regionale Planung für den Einsatz guter und ganzheitlicher Lösungen und das Management von Naturgefahren über kommunale Grenzen hinaus verantwortlich. In Norwegen gibt es umfassende und strenge Regelwerke für Bauvorhaben in gefährdeten Gebieten. Bei einer Neubebauung gibt es klare Sicherheitsanforderungen und das NVE unterstützt die Kommunen bei der Prävention von Schäden durch

---

[62] Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning (2015), *NOU Digital sårbarhet – sikkert samfunn*, S. 200, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou20152015001300 0dddpdfs.pdf, 23.08.2021.

[63] DSB (2019), *Analyser av krisescenarioer 2019*, S. 105, 201, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

[64] Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning (2015), *NOU Digital sårbarhet – sikkert samfunn*, S. 168, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou20152015001300 0dddpdfs.pdf, 23.08.2021.

[65] DSB (2019), *Analyser av krisescenarioer 2019*, S. 10, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

[66] DSB (2019), *Analyser av krisescenarioer 2019*, S. 197, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021; JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 27-28, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 19.08.2021.

Überschwemmungen und Erdrutsche. Das NVE ist für die Ausarbeitung von Gefahrenkarten zuständig, kommentiert kommunale Flächenpläne und unterstützt die Kommunen mit Sicherungsmaßnahmen, Überwachung und Warnung. Das NVE hilft den Kommunen auch fortlaufend mit Ratschlägen und mit der Beibehaltung der Sicherheit bei Ereignissen. Die staatliche Behörde DSB koordiniert die Arbeit zu ziviler Sicherheit und Bereitschaft auf staatlichem Niveau und gegenüber den Verwaltungsbezirken und Kommunen. Das DSB ist auch für die Zivilverteidigung verantwortlich.[67]

Die digitale Sicherheit ist in erster Linie ein Verantwortungsbereich der jeweiligen Unternehmen. Hier ist in der Regel die Führungsebene für Risikoeinschätzungen und entsprechende Maßnahmen zuständig. Ferner sind die Ministerien übergeordnet für die digitale Sicherheit in ihrem jeweiligen Sektor/Ressort verantwortlich. Die staatlichen Organe sollen die Voraussetzungen dafür bilden, dass Unternehmen sich gegen unerwünschte digitale Ereignisse schützen können – sowohl für die eigene digitale Sicherheit des Unternehmens als auch für die Funktionsfähigkeit der gesamten Gesellschaft.[68]

Kunnskapsbanken

Kunnskapsbanken (dt. „Wissensbank") ist eine technische Lösung, welche von der staatlichen Behörde DSB entwickelt wurde. Diese Datenbank basiert auf Daten aus verschiedenen Quellen enthält Informationen zu Risiken und Anfälligkeiten für Naturereignisse. Die Daten sind als Zahlen, Karten und Graphen verfügbar und werden regelmäßig mit neuen Inhalten aktualisiert. Man kann Daten für das gesamte Land, einzelne Verwaltungsbezirke oder Kommunen filtern. *Kunnskapsbanken* kann von jedem genutzt werden, ist aber speziell für Fachpersonal im Bereich der lokalen und regionalen zivilen Sicherheit entwickelt worden. Die Datenbank ist nicht nur ein Hilfsmittel, um Informationen für Risiko- und Gefährdungsanalysen zu finden, sondern auch eine wichtige Ressource für Wissenschaftler, Studierende, JournalistInnen und andere Interessensgruppen im Bereich der zivilen Sicherheit und Naturereignisse.

Quelle: Kunnskapsbanken, o. J., *Om Kunnskapsbanken,* https://kunnskapsbanken.dsb.no/om, 17.10.2021.

In Anhang 2 befindet sich eine Übersicht über ausgewählte zentrale Akteure mit Verantwortungsbereichen für Naturereignisse und/oder digitale Sicherheit.

2.4.2 Öffentliche Mittel

Viele Aktivitäten, die der zivilen Sicherheit dienen, finden in den jeweils einzelnen Sektoren statt und richten sich nach der jeweils für den Sektor geltende Gesetzgebungen und Anforderungen. Die Arbeit der Ministerien mit der zivilen Sicherheit soll einen integrierten Teil des Tagesgeschäfts darstellen. Ändern sich Risiken oder Anfälligkeiten, müssen Maßnahmen und öffentliche Mittel ebenfalls entsprechend angepasst werden – dies muss jedoch innerhalb der vorgesehenen Rahmen im Haushalt geschehen. Die Regierung verfolgt das Ziel, die Aktivitäten im Bereich der zivilen Sicherheit auf mehreren zentralen Gebieten zu stärken.[69]

Digitale Sicherheit

Die nationale Strategie für digitale Sicherheit aus dem Jahr 2019 beschreibt Maßnahmen im finanziellen Umfang von ca. 1,6 Mrd. NOK (ca. 157 Mio. €) über eine Periode von vier Jahren. Eine der Maßnahmen ist die Bewilligung von 497 Mio. NOK (ca. 48,8 Mio. €) für ein mehrjähriges Projekt über den Haushalt des Militärs für die Durchführung nationaler technischer Sicherheitsmaßnahmen,

[67] Regjeringen.no, 14.01.2021, *Naturfarer – hvem har ansvar for at nordmenn bor trygt?*, https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/oed/nyheter/2021/naturfarer-hvem-har-ansvar-for-at-nordmenn-bor-trygt/id2828628/, 15.10.2021.

[68] Departementene (2019), *Nasjonal strategi for digital sikkerhet*, s. 13, nasjonal-strategi-for-digital-sikkerhet.pdf (regjeringen.no), 14.10.2021.

[69] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 160, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 26.08.2021.

darunter **neuer Sensortechnologien für das Warnsystem für die digitale Infrastruktur (VDI)**. Ferner wurde die nationale Sicherheitsbehörde (NSM) 2020 mit 5,4 Mio. NOK (ca. 530.000 €) gestärkt, um die Kapazität für die **Analyse und Aufdeckung ernsthafter Angriffe auf die digitale Infrastruktur zu erhöhen.**[70]

Die norwegische Regierung legt einen besonderen Fokus darauf, dass digitale Kompetenzen in der Gesellschaft gestärkt werden. Für eine erhöhte digitale Sicherheitskompetenz entsprechend des Bedarfs der Gesellschaft (u.a. in Forschung und Ausbildung) wurden ca. 800 Mio. NOK (ca. 78,5 Mio. €) bewilligt.[71]

Ferner wurden dem DSB Gelder für eine **erhöhte Kapazität zur Vorbeugung, Aufdeckung und dem Management digitaler Ereignisse im *Nødnett*** genehmigt. Für die Durchführung von Ausschreibungen und die Inbetriebnahme dieser Prozesse hat das DSB ein eigenes Projekt ins Leben gerufen. Dienstleistungen und Lösungen für das Aufdecken von Sicherheitslücken oder -angriffen sowie Unterstützung bei der Analyse von Ereignissen werden durch öffentliche Ausschreibungen beschafft.[72]

Mobilbasierte Warnung der Bevölkerung

Das norwegische Parlament *Stortinget* hat im Haushaltsbudget für 2020 1,1 Mio. NOK (ca. 108.000 €) für die genauere Betrachtung eines Systems für die mobilbasierte Warnung der Bevölkerung bewilligt. Nach Abschluss dieser Untersuchung wird die norwegische Regierung abwägen, ob dieser Sachverhalt in den nächsten Jahren im Haushalt eine höhere Rolle spielen soll.[73] Das aktuelle Warnsystem basiert auf Sirenen und Radiomeldungen. Die Sirenen erreichen ca. 50 % der Bevölkerung – vor allem die Bewohner dicht besiedelter Gebiete und größerer Städte. Das neue System würde auf Geodaten vor Telefonnummern basieren und würde daher dafür sorgen, dass alle, die sich in einem definierten Gebiet aufhalten, eine Warnung erhalten – unabhängig von z.B. Nationalität oder Mobilfunkbetreiber.[74]

Schutz vor Überschwemmungen, Erdrutschen und Lawinen

Der Einsatz zum Schutz vor Überschwemmungen oder Erdrutschen wurde in den letzten Jahren erhöht. Im Zeitraum zwischen 2014 und 2019 wurden ca. 1,7 Mrd. NOK (ca. 156 Mio. €) für entsprechende Sicherheitsmaßnahmen aus dem Budget von NVE verwendet. Physische Sicherungsmaßnahmen können das Risiko in einzelnen Gefahrengebieten für die bestehende Bebauung reduzieren. Eine Verordnung über Beihilfen des NVE soll Kommunen dort mit Sicherheitsmaßnahmen unterstützen, wo die Herausforderungen so groß sind, dass es unverhältnismäßig wäre, die jeweiligen Bewohner oder die Kommune alleinig in Verantwortung zu ziehen. Das wesentliche Ziel dieser Verordnung ist es, die Kommunen fachlich und finanziell bei der Planung von Vorbeugungsmaßnahmen und der Sicherung existierender Bebauung zu unterstützen. Konkret unterstützt NVE durch die Untersuchung, Planung oder die Durchführung von Sicherungsmaßnahmen oder durch die Bezuschussung von Kommunen, wenn diese die Maßnahme selbst umsetzen. In beiden Fällen ist jedoch die Kommune der offizielle Durchführer der Maßnahme (entspr. norwegischem Baugesetz). Die Sicherung des Baubestands ist keine Pflicht – weder für den Eigentümer, die Kommune oder den Staat. Das NVE nimmt bei der Verteilung der Hilfen Priorisierungen nach Risiko und Konsequenzen für die Bebauung und Leib und Leben vor. Die Maßnahmen, bei denen eine Investition den größtmöglichen volkswirtschaftlichen Kosten-Nutzen-Effekt bringt, wird in der Regel priorisiert. 2020

[70] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 82, 160, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 26.08.2021.

[71] Regjeringen.no, 16.10.2020, *Vår digitale sikkerhet styrkes*, https://www.regjeringen.no/no/aktuelt/var-digitale-sikkerhet-styrkes/id2771497/, 26.08.2021.

[72] DSB (2021), *DSB årsrapport 2020*, S. 60, https://www.dsb.no/globalassets/dokumenter/rapporter/dsbs-arsrapport-2020.pdf, 30.08.2021.

[73] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 161, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 26.08.2021.

[74] Regjeringen.no, 07.10.2019, *Statsbudsjettet 2020. Sikrere og mer effektiv kommunikasjon*, https://www.regjeringen.no/no/aktuelt/sikrere-og-mer-effektiv-kommunikasjon/id2672558/, 26.08.2020.

wurden ca. 370 Mio. NOK (ca. 34 Mio. €) für Sicherungsmaßnahmen bewilligt, von denen 165 Mio. NOK (ca. 15,2 Mio. €) durch Maßnahmenpakete in Verbindung mit der Covid-19-Pandemie genehmigt wurden.[75]

Ferner hat die norwegische Regierung weitere 102 Mio. NOK (ca. 9,4 Mio. €) für notwendige **Sicherungsmaßnahmen nach dem Quickton-Erdrutsch in Gjerdrum** vorgeschlagen. Die Planung für die langfristige Sicherung des Erdrutschgebietes wurde bereits begonnen, aber wird noch einige Zeit andauern. Es wird erwartet, dass die Sicherungsarbeiten ebenfalls noch einige Jahre dauern werden.[76]

2.5 Überblick über das (Aus-) Bildungswesen im Bereich zivile Sicherheit

Die nationale Strategie für digitale Sicherheitskompetenz aus dem Jahr 2019 definiert Richtungen und Inhalte für die Maßnahmen im Bereich der Bildung und Forschung sowie Verantwortlichkeiten in diesem Bereich. Ferner behandelt die Strategie Maßnahmen zur Bewusstseinssteigerung, die sich an Bevölkerung, Kommunen und Unternehmen richten. Die Strategie ist ein Teil des fortlaufenden Prozesses zur Entwicklung von **Maßnahmen zur Steigerung der Sicherheitskompetenz** in Kooperation mit den Behörden, öffentlichen und privaten Unternehmen, dem Bildungswesen sowie Forschungsinstitutionen. Der langfristige Plan für Forschung und Hochschulausbildung sieht auch einen stärkeren Einsatz von Forschung und Entwicklung im Bereich der digitalen Sicherheit vor. Eine engere Zusammenarbeit soll ein höheres Gewicht auf digitale Sicherheit als Teil von Ingenieur- und Technologiestudiengängen legen. Die Strategie beleuchtet besonders die bisherige Wissensgrundlage für eine ausreichende digitale Sicherheitskompetenz. Das Justizministerium sorgt für aktualisierte Statistiken und Analysen, um fehlende Kompetenzen im Bereich der digitalen Sicherheit aufzudecken. Außerdem sollen auch die Voraussetzungen für eine verbesserte Sicherheitskultur in der Bevölkerung und innerhalb von Unternehmen geschaffen werden. Hierfür werden insgesamt über 800 Mio. NOK (ca. 73,7 Mio. €) vorgesehen. Ferner wurde in den Studiengängen im IT-Bereich in den vergangenen Jahren das Thema der digitalen Sicherheit stärker forciert. Verantwortliche Institutionen sind das Justiz- sowie das Bildungsministerium.[77]

In der Tabelle in Anhang 3 (siehe separates Dokument „Anhang“) sind alle relevanten Berufsausbildungen und Studiengänge, die in Norwegen angeboten werden, aufgeführt. Diese beziehen sich hauptsächlich auf die Schwerpunkte digitale Sicherheit und Geologie/Schutz vor Naturereignissen.

Die Tabelle in Anhang 4 stellt die relevanten Forschungsinstitutionen für die zivile Sicherheit im Hinblick auf Naturereignisse und Digitales dar.

2.5.1 Maßahmen und Projekte

Norwegian Cyber Range (NCR) ist die erste nationale, sektorenübergreifende Testarena für Cyber- und Informationssicherheit. Das NCR richtet sich sowohl an kommerzielle Akteure als auch die Wissenschaft und bietet kommerzielle Dienstleistungen für private und öffentliche Marktsegmente an. Dabei sollen realistische, aber sichere Umgebungen für das Testen, Üben und Trainieren im Umgang von cyberkriminellen Ereignissen simuliert werden. Das NCR sichert somit einen effektiven und realitätsnahen Kompetenzaufbau und vernetzt Gesellschaftmodelle, digitale Wertschöpfungsketten und digitale Infrastrukturen in einem vorab definierten Umfeld. Ferner trägt eine solche Testarena zu einem zielgerichteten **Fort- und Weiterbildungsangebot** im Bereich der nationalen IT-Sicherheit bei. Das NCR wird vom *Center for Cyber and Information Security* (NTNU CCIS) der

[75] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 8, 107, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 26.08.2021.

[76] NVE, o. J., *Kvikkleireskredet i Gjerdrum*, https://www.nve.no/naturfare/laer-om-naturfare/om-skred/kva-er-kvikkleire-og-kvikkleireskred/kvikkleireskredet-i-gjerdrum/, 26.08.2021.

[77] Departementene (2019), Tiltaksoversikt til nasjonal strategi for digital sikkerhet, S. 9-10, https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf, 11.10.2021.

technischen Universität in Trondheim (*Norges teknisk-naturvitenskapelige universitet*, NTNU) betrieben. Die Trainings- und Lernzentren befinden sich auf dem Campus der NTNU in Gjøvik in Mittelnorwegen.[78] Weitere Partner des Projektes ist der Verwaltungsbezirk Innlandet, *Cyberforsvaret* (die Einheit zur Abwehr von Cyberangriffen des norwegischen Militärs), die Zivilverteidigung (*Sivilforsvaret),* Telenor, dem IT-Unternehmen EVRY, das Zentrum für Informationssicherheit (*NorSIS*), die Wirtschaftsförderung Innovation Norway, das Verteidigungsministerium Estlands sowie die Technische Universität Tallinn. [79]

NORCICS ist eine Organisation basierend auf eine Public-Private Partnership der *NTNU Center for Cyber and Information Security* (NTNU CCIS) und besteht aus vier Forschungspartnern (NTNU IIK, SINTEF Energi, SINTEF Digital, Norsk Regnesentral, UiA) sowie Partnern aus den verschiedenen Nutzergruppen. Diese können in drei Gruppen eingeteilt werden:

- **Organisationen mit Aktivitäten in verschiedenen kritischen Sektoren,** z.B. Energieanbieter, Krankenhausbetreiber oder Unternehmen der Prozessindustrie wie Elvia, Kongsberg Gruppen, Yara International, Sykehuset Innlandet HF, Equinor, Lyse Elnett, Helgeland Kraft oder NC-Spectrum.
- **Kommerzielle Anbieter von Cyber Security-Lösungen oder operativer Technologie:** Mnemonic, Memoscale, Siemens, SINTEF Manufacturing.
- **Organisationen, die sich für die Sicherheit der Gesellschaft einsetzen, das Sicherheitsbewusstsein stärken und Norwegens Einwohner und Unternehmen zu digitalen Gefahrenquellen beraten:** Oslo politidistrikt, NorSIS.[80]

Norwegen ist eines der am stärksten digitalisierten Länder der Welt. Die Vision von NORCICS ist es, dazu beizutragen, dass Norwegen das am sichersten digitalisierte Land der Welt wird, indem es die Cybersicherheit und Widerstandsfähigkeit seiner kritischen Sektoren durch forschungsbasierte Innovation verbessert. Da die Cybersicherheit bei den meisten Betriebstechnologien der kritischen Sektoren nicht berücksichtigt wurde, da letztere traditionell aufgrund ihrer Isolierung als sicher gelten; hat die Integration der Betriebstechnologie (OT) mit der Informationstechnologie (IT) und ihre Verbindung mit dem Internet zu einer Reihe von Cyberschwachstellen geführt. Das Hauptziel von NORCICS besteht darin, die **Fähigkeit von Akteuren des privaten und öffentlichen Sektors zu verbessern, auf aktuelle und künftige Cybersicherheitsrisiken zu reagieren, indem innovative Technologien innerhalb eines cyber-physischen Sicherheitsökosystems, das hochqualifiziertes Forschungspersonal entwickelt, validiert und eingesetzt werden**. [81]

Eine Reihe von international hoch angesehenen Zentren, die auf dem Gebiet der Cybersicherheit tätig sind, arbeiten mit NORCICS zusammen. Partner aus Deutschland sind die Technische Universität München, die Universität Passau und die Technische Universität Hamburg.[82]

---

[78] Departementene (2019), *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*, S. 20, https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf, 30.08.2021.

[79] NTNU, o. J., *Norwegian Cyber Range*, https://www.ntnu.no/ncr, 11.10.2021.

[80] Mediaplanet, 27.09.2021, *Alt om samfunnssikkerhet: Setter Norge på kartet som verdensledende på digitalisering og digital sikkerhet*, https://www.altomsamfunnssikkerhet.no/samfunnssikkerhet-og-beredskap/setter-norge-pa-kartet-som-verdensledende-pa-digitalisering-og-digital-sikkerhet/, 14.10.2021.

[81] SFI Norwegian Centre for Cybersecurity in Critical Sectors (2020), *SFI NORCICS Annual Report 2020*, S. 2-3, https://www.ntnu.edu/documents/1294734959/1300988649/SFI+NORCICS+Annual+Report+2020.pdf/c2189003-5079-9646-4d3b-8dbc1c4a063c?t=1624015907570, 15.10.2021.

[82] SFI Norwegian Centre for Cybersecurity in Critical Sectors (2020), *SFI NORCICS Annual Report 2020*, S. 9, https://www.ntnu.edu/documents/1294734959/1300988649/SFI+NORCICS+Annual+Report+2020.pdf/c2189003-5079-9646-4d3b-8dbc1c4a063c?t=1624015907570, 15.10.2021.

3 Marktstruktur und -entwicklung

3.1 Schutz vor Naturereignissen

Wie in Kapitel 2 skizziert, bestehen die deutlichsten Herausforderungen für die zivile Sicherheit in Norwegen durch klimabedingte Naturereignisse wie starke Niederschläge und eine hohe Niederschlagsintensität mit einer daraus folgenden Hochwasser- oder Erdrutschgefahr. Auch in der Zukunft werden Extremwetterereignisse häufiger und kräftiger auftreten, gleichzeitig wird ein Anstieg der Temperaturen und Niederschläge im gesamten Land und über alle Jahreszeiten prognostiziert. Darüber hinaus gibt es in Norwegen mehrere Areale, die als Gefahrengebiet für Erdrutsche aufgrund von Quickton-Erdmassen definiert sind. Dieses Thema ist aktuell besonders im Fokus aufgrund des verheerenden Erdrutsches am 30. Dezember in Ask, nordöstlich von Oslo. Dies war einer der schwersten Quickton-Erdrutsche in Norwegen.

Das Ausmaß der Konsequenzen der verschiedenen, zu erwartenden Klimaextreme ist stark abhängig davon, wie sich die Gesellschaft darauf vorbereitet. Eine widerstandsfähige Infrastruktur sowie die Implementierung von Frühwarnsystemen sind wichtige Anpassungsmaßnahmen. [83]

3.1.1 Marktakteure und Entwicklungsprozesse

Im Teilbereich «Schutz vor Naturereignissen“ zählen die **spezialisierten Forschungsinstitute** (siehe Anhang 4) zu den wichtigsten Marktakteuren. In der Regel werden Technologien von solchen Instituten entwickelt, welche diese selbst oder über ein Spin-Off vermarkten. Im Dienstleistungssegment ist es üblicher, dass die Institute auch selbst die Lösungen anbieten, die sie entwickelt haben.

Im Bereich Schutz vor Naturereignissen sind die **spezialisierten Forschungsinstitute** die wichtigsten Akteure auf dem Markt. In der Rel werden Technologien von diesen Instituten entwickelt, welche diese dann weiter vertreiben oder über ein Spin-Off vermarkten. Im Dienstleistungssegment ist es üblicher, dass die Institute selbst auch die Lösungen anbieten, die sie entwickelt haben. Ein Beispiel dafür ist NGI Digital, die Einheit für Digitalisierung und digitale Innovation des geotechnischen Instituts NGI (*Norges Geotekniske Institutt,* NGI). Durch NGI Digital werden neue Lösungen sowohl für den internen und externen Gebrauch als auch für Forschungsprojekte entwickelt und freigegeben. GeoHub ist die cloudbasierte Plattform, mit der diese Lösungen realisiert werden können. Das Herzstück von GeoHub ist eine moderne Datenplattform und eine Reihe von eigenentwickelten, maßgeschneiderten Anwendungen.[84] Ein anderes alltägliches, aber dennoch nicht minder wichtiges Beispiel ist das Wetterportal yr.no[85]. Das Portal wurde vom meteorologischen Institut MET entwickelt und 2007 lanciert. Die zugehörige App, eine vereinfachte Version der Website, wurde 2017 veröffentlicht. Die App ist besonders beliebt und ca. 50 % der Nutzer von yr greifen über die Mobilapplikation auf das Portal zu. Die App gehörte auch zu den Gewinnern der «WMO International Weather Apps Awards 2020“ der Welt-Meteorologieorganisation WMO für Design und die Präsentation von Informationen.[86] Yr war im März 2018 der weltweit erste meteorologische Dienst, welcher private Wetterbeobachtungen genutzt hat, um Temperaturvorhersagen zu verbessern. Seit September 2021 nutzt Yr auch Observationen privater Niederschlagsmesser.[87]

Die Branche wird außerdem stark durch **Start-ups** geprägt. Die Anzahl dieser ist in den vergangenen Jahren stark gestiegen – dies ist mitunter darauf zurückzuführen, dass viele Ingenieure ihre Jobs in der Öl- und Gasindustrie verloren und somit ihre eigenen

[83] DSB (2019), *Analyser av krisescenarioer 2019*, S. 36, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 17.10.2021.

[84] NGI, *Digital Services,* https://www.ngi.no/eng/Services/Technical-expertise/Digital-services, 12.10.2021.

[85] Gespräch mit NGI, Dominik Lang, Director Natural Hazards, 02.09.2021.

[86] NTB, 15.12.2020, *Yr-appen er prisvinner*, https://kommunikasjon.ntb.no/pressemelding/yr-appen-er-prisvinner?publisherId=17846853&releaseId=17897837, 10.09.2021.

[87] NTB, 06.09.2021, *Yr får betre nedbørvarsel*, https://kommunikasjon.ntb.no/pressemelding/yr-far-betre-nedborvarsel?publisherId=17846853&releaseId=17915030, 10.09.2021.

Unternehmen gegründet haben. Die Entwicklungsarbeit wird vor allem dadurch geprägt, dass einzelne Technologieelemente in ein System integriert werden. Ein typisches Beispiel hierfür sind Sensoren, die häufig von anderen Produzenten bezogen und schließlich im eigens entwickelten System implementiert werden.[88] Ein solcher Fall ist z.B. das Unternehmen Cautos Geo AS, welches 2009 von zwei Personen gegründet wurde und heute 15 Angestellte beschäftigt. Das Unternehmen überwacht Naturgefahren, die Stabilität von Felsmassen, Erdmassen, Konstruktionen und Bedingungen an Land und im Wasser. Cautos Geo AS entwickelt und betreibt verschiedene Messsysteme und bietet eine eigene Weblösung für die Sammlung, Bearbeitung, Analyse und Warnung durch Daten aus verschiedenen Quellen. Das Unternehmen arbeitet mit mehreren internationalen Partnern zusammen und nutzt u.a. SAAF (ShapeAccelArrayField)-Sensoren von Measurand und GNSS und Totalstationssysteme von Trimble.[89] Andere bedeutende Produzenten geotechnischer Sensoren oder Umweltsensoren sowie von Loggsystemen, die auf dem norwegischen Markt über Händler vertreten sind, sind z.B. Geosense, Solinst, NexSens Technology, Campbell Scientific und Eureka.[90]

Weitere Beispiele aus der Startup-Szene sind Hawaal, ein Unternehmen aus dem Bereich der Hochwassersicherung und Forsyst AS, welches Lösungen für die Hochwasserwarnung bietet. Hawaal wurde 2016 gegründet und mit nur vier Angestellten ist das Unternehmen bereits in anderen europäischen Ländern unterwegs, darunter z.B. mit Aufträgen in Görlitz, Halle und Niedersachsen. Die Gründer von Hawaal haben *Flood Grating* entwickelt, eine innovative Lösung zum Hochwasserschutz, welche ohne professionelle Hilfe oder Werkzeuge installiert werden kann.[91] Forsyst ist ein noch sehr junger Akteur auf dem Markt (gegr. 2020) und hat ein Hochwasserwarnsystem entwickelt, welches durch künstliche Intelligenz den Wasserstand für vier bis sieben Tage in die Zukunft berechnen kann.[92] Das Unternehmen hält eine zentrale Rolle im Projekt **Digi Rogaland,** einem Pilotprojekt für Hochwasserwarnungen, inne. Digi Rogaland ist eine Kooperation aus 23 Kommunen und wurde in der kleinen Stadt Sauda durchgeführt, welche in der vergangenen Zeit häufiger von Überschwemmungen heimgesucht wurde. Durch Sensoren, welche von Forsyst platziert worden sind, wird der Wasserstand zwei Mal pro Minute gemessen und den Wetterdaten gegenübergestellt. Alle 30 Minuten wird durch ein LoRaWAN-Gateway in einem Funkmast durch die Splunk-Lösung der Kommune die Daten gesendet. In der Splunk-Lösung werden die Daten gesammelt, ausgewertet und kategorisiert, bevor sie an ein Datenhub in der Kommune Stavanger weitergeleitet werden. Von hier aus wird ein API-Zugang u.a. an Forsyst erteilt. Forsyst hat nun wiederum die Verantwortung für die Warnungen. Bestehende, offene Daten des NVE und MET sowie Daten der lokalen Stromproduzenten und eigene Daten der fünf platzierten Ultraschallsensoren werden zu Grunde gelegt. Kern der Methode von Forsyst ist es, es dem Algorithmus beizubringen, Datenmuster durch das Training mit historischen Daten wiederzuerkennen. Während NVE eher auf Makroniveau warnt, erteilt Forsyst Warnungen durch maschinelles Lernen in Kombination mit stochastischer Regressionsanalyse auf lokalem Niveau. Das IT-Consulting-Unternehmen Bouvet war bei diesem Digitalisierungs-Case beteiligt.[93]

3.1.2 Digitales Werkzeug für verbesserte Hochwasserwarnungen

Sechs Kommunen in der Region Nord-Gudbrandsdal haben das Projekt ***Flomrespons*** initiiert, welches den Markt dazu herausfordern soll, ein neues und zukunftsgerichtetes Tool für Hochwasserwarnungen zu entwickeln. Dieses soll lokale Überschwemmungen ankündigen, bevor diese eintreffen, sodass lokale Behörden und die Bevölkerung rechtzeitig Maßnahmen ergreifen können. Das Projekt wird derzeit in Kooperation mit der Universität NTNU, der Straßenbaubehörde Statens Vegvesen und der Energiebehörde NVE entwickelt. Der norwegische Forschungsrat hat 8 Mio. NOK (ca. 785.000 €) für das Projekt bewilligt. 15 nationale und

[88] Gespräch mit NGI, Dominik Lang, Director Natural Hazards, 02.09.2021.

[89] Cautos Geo AS, o. J., *Om oss*, https://cautusgeo.com/om-oss/, 13.09.2021.

[90] Siehe www.measureit.no/, 13.09.2021.

[91] Tu.no, 13.08.2021, *Norsk flomsikringstartup sikter mot Europa*, https://www.tu.no/artikler/norsk-flomsikringstartup-sikter-mot-europa/512412?utm_source=newsletter-tudaily&utm_medium=email&utm_campaign=newsletter-2021-08-14&key=gSOhW0ZF, 13.09.2021.

[92] NRK.no, 13.06.2021, *Får mer nøyaktig flomvarsel: – Da kan vi forberede oss*, https://www.nrk.no/sorlandet/flomvarslingssystem-basert-pa-kunstig-intelligens-skal-gi-mer-presis-varsling-1.15511293, 15.09.2021.

[93] Tu.no, 08.11.2020, *Sensorteknologi skal verne mot villere vær lokalt*, https://www.tu.no/artikler/sensorteknologi-skal-verne-mot-villere-vaer-lokalt/501912, 19.10.2021.

internationale Lieferanten haben im Zuge der Ausschreibung ein Angebot eingereicht. Vier ausgewählte Unternehmen erhielten einen Zuschlag: Skred AS mit Dryp als Unterlieferant, Pipelife Norge und Knowit als Unterlieferant, Sintef Energi und Deltares sowe Sweco Norge. Sweco, Europas größtes Architekten- und Ingenieurunternehmen hat den Auftrag für die Entwicklung des digitalen Werkzeugs erhalten. Skred/Dryp, Sintef/Deltares und Pipelife/Knowit haben mit Phase 2 fortgesetzt und werden bis Januar 2022 im engen Dialog mit den Anwendern der Kommunen ihre Lösungen entwickeln.[94] Laut Sweco sind die im Markt vorhandenen Hochwassermodelle sehr allgemein, während die norwegische Topografie, geprägt durch hohe Berge und steile Talseiten, sehr komplex ist. Daher sind Vorhersagen sehr schwer zu treffen, weil eine Situaton im gleichen Zeitraum in zwei benachbarten Tälern völlig verschieden sein kann. *Flomrespons* sammelt Inputs verschiedener Variablen wie z.B. Niederschläge, Schmelzmengen und andere Daten in Terrains mit großen Binnenseen und Wasserläufen mit und ohne Stromproduktion. Nach Sammlung all dieser Daten ist es möglich, die Situation vorauszusagen. Aktuell gibt es kein ausreichend detailliertes Hochwasserwarnungssystem. Die aktuellen Voraussagen decken oft größere Areale ab und sind daher nur schwer für lokale Behörden nutzbar, die oftmals auch nicht über besonders spezifische Kompetenzen hierzu verfügen. Sweco entwickelt derzeit ein Hybridmodell, indem detaillierte Geodaten und physische Modelle mit maschinellem Lernen kombiniert werden, welches fehlende Details aufgrund von u.a. zu wenigen Messstationen kompensieren kann. So können Messresultate mit einer konkreten Situation verknüpft werden, ohne dass ein Detailmodell verfügbar ist.[95]

3.1.3 Satelitten für die Überwachung von Hochwasser, Erdrutschen und Eis

Satellitendaten werden ein immer wichtigeres Werkzeug für Prävention von Unglücken und Schäden durch Naturereignisse wie Lawinen oder Erdrutsche. Die Daten der **Sentinel-Satelliten** werden immer häufiger für die Warnungen des NVE genutzt. Das Institut für geologische Untersuchungen NGU, NVE und das Raumfahrtszentrum *Norsk Romsenter* haben InSAR Norge lanciert, das erste landesweite und kostenlose internetbasierte Kartendienst für **InSAR-Daten**. Somit sind die InSAR-Daten für alle in Norwegen zugänglich. Das Forschungsinstitut Norce (früher Norut) hat bei der Entwicklung dieser Technologie eine zentrale Rolle gespielt. [96] InSAR-Daten werden für das Mapping schwerer Felsstürze genutzt und wo diese ein Risiko darstellen können, während Radardaten zur Überwachung von Lawinen und die Ausbreitung von Überschwemmungen genutzt werden. Die Satellitendaten werden u.a. für die Aufdeckung und Überwachung von Eistauseen eingesetzt, welche katastrophale Überschwemmungen auslösen können.[97]

3.1.4 Trend: Naturbasierte Lösungen

Ein wichtiger Trend in Norwegen ist die Entwicklung und Nutzung **naturbasierter Lösungen** in der Risikominimierung für klimabedingte Naturschäden. Hintergrundgedanke ist es, dass die Natur selbst Ideenquelle für Lösungen ist, welche flexible Alternativen zu traditionellen Ingenieurslösungen darstellen. Ein wichtiges Forschungsprojekt ist in diesem Zusammenhang PHUSICOS, welches durch das Horizon 2020-Programm der EU finanziert wird. Hinter dem Projekt stehen 15 europäische Partner aus Forschung, Wissenschaft und regionalen Behörden aus sieben Ländern (u.a. Deutschland), das Projekt wird vom NGI geleitet.[98] Es soll zeigen, wie naturbasierte Lösungen robuste, nachhaltige und kosteneffiziente Maßnahmen zur Verringerung des Risikos extremer Wetterereignisse in ländlichen Berglandschaften bieten. Ein wichtiger Vorteil naturbasierter Lösungen ist, dass sie häufig positive Zusatzeffekte wie Rekreation, Bewahrung der natürlichen Vielfalt oder grüne Lungen in städtischen Gebieten mit sich bringen. In diesem Zusammenhang kann auch erwähnt werden, dass im norwegischen Markt auch sehr viel Wert auf Ästhetik gelegt wird – ein offensichtlicher Vorteil naturbasierter Lösungen gegenüber technischen Lösungen. Naturbasierte Lösungen können jedoch

[94] flomrespons.no, o. J., *Fremtidens lokale verktøy for flomvarsling*, https://www.flomrespons.no/, 13.10.2021.

[95] Samferdsel & Infrastruktur, 19.01.2021, *Flomvarsling: digital verktøy for bedre beredskap,* https://www.samferdselinfra.no/flomvarsling-digitalt-verktoy-for-bedre-beredskap/, 13.10.2021.

[96] Norges Geologiske Undersøkelse (NGU), 10.10.2018, *INSAR Norge*, https://www.ngu.no/emne/insar-norge, 20.10.2021.

[97] Regjeringen.no (2019-2020), *6.3.2 Overvåking av flom, skred og is*, https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20192020/id2682361/?ch=6, 20.10.2021.

[98] PHUSICOS, o. J., *Solutions to reduce risk in mountain landscapes*, https://phusicos.eu/, 13.09.2021.

auch Nachteile mit sich bringen, wie z.B. hohe Anforderungen an die Flächennutzung, eine Unsicherheit hinsichtlich Kosten sowie eine lange Implementierungszeit. Außerdem sind diese Lösungen aufgrund verschiedener klimatischer Bedingungen auch nicht in allen Gebieten gleichermaßen geeignet und erfordern häufig einen höheren Instandhaltungsaufwand als die traditionellen Lösungen.[99]

3.1.5 Herausforderung: Fachkräftemangel

Für die Bewertung von Gefahren durch Naturereignisse in besiedelten Gebieten sind vor allem die Kommunen verantwortlich. Durch Risiko- und Gefährdungsanalysen untersuchen und bewerten und verfolgen sie die Risiken für Überschwemmungen und Erdrutsche. Diese Arbeit wird vor allem von beratenden Ingenieurgesellschaften durchgeführt. Dies sind Unternehmen unterschiedlichster Größe. Hierbei werden häufig auch das geotechnische Institut NGI, SINTEF und die Energiebehörde NVE involviert. Für diese Akteure besteht die Herausforderung, Fachkräfte mit ausreichenden Kompetenzen zu finden. Die Resultate werden nicht selten einfach den Kommunen überlassen und die Tatsache, dass viele Kommunen weder Ressourcen, Kapazitäten oder Kompetenzen haben, um diese Arbeit ausreichend weiter zu verfolgen, ist besorgniserregend. Erst kürzlich wurde in den norwegischen Nachrichten gemeldet, dass die Stadt Trondheim die einzige norwegische Kommune ist, welche eine eigene geotechnische Abteilung unterhält und eigene Ausrüstung für die Analyse von Bodenproben besitzt.[100]

3.2 Digitale Sicherheit

3.2.1 Marktakteure und Fokusbereiche

Die norwegische IT-Branche ist in verschiedenen Branchenverbänden und Clustern organisiert. Die wichtigsten hier sind IKT Norge und Abelia (zugehörig zum norwegischen Arbeitgeberverband NHO). Da diese beiden Organisationen ein breites Spektrum an Kompetenz- und Technologieunternehmen abdecken, ist es nicht möglich, spezifische Brancheninformationen nur für die Akteure im Bereich der digitalen Sicherheit abzugrenzen.

Laut dem wirtschaftspolitischen Sprecher für Technologie und Digitalisierung bei Abelia gibt es auf dem norwegischen Markt für digitale Sicherheit einige größere Akteure wie z.B. Thales, Sopra Steria, Watchcom Security Group AS, Defendable AS, mnemonic AS, Atea AS und Netsecurity AS. Neben diesen gibt es eine Reihe kleiner Unternehmen, welche verschiedene Lösungen innerhalb der einzelnen Branchensegmente anbieten.[101] Es gibt jedoch nur wenige Anforderungen oder gesetzliche Regelungen, welche es ermöglichen, dass norwegische Unternehmen die Qualität der Anbieter unterscheiden können. Die Behörden haben allerdings durch die nationale Sicherheitsbehörde (NSM) eine Genehmigungsordnung für das Management riskanter Ereignisse erarbeitet, welche relativ hohe Anforderungen an potenzielle Dienstleister beinhaltet. Bisher haben nur fünf Unternehmen diese Genehmigung erhalten (siehe Kapitel 4.3.5). Diese haben enorme Ressourcen eingesetzt, um diese Zulassung zu erhalten.[102]

Laut Abelia sind private norwegische Unternehmen im Vergleich zu anderen Ländern nicht besonders stark im Bereich der Forschung und Entwicklung neuer Technologien und Lösungen auf dem Feld der IT-Sicherheit. Viele Forschungs- und Entwicklungsaktivitäten finden in öffentlichen Organisationen und Instituten wie SINTEF, NORCE oder IFE statt. Diese fungieren häufig als Wissens- oder Kooperationshubs. Der teilprivatisierte Telekommunikationsbetreiber Telenor AS, der landesweit größte Digitalisierungsdienstleister, arbeitet z.B. sehr umfassend mit dem F&E-Sektor zusammen.[103]

---

[99] Menon Economics, NINA & SWECO (2017), *Naturbaserte løsninger for klimatilpasning*, S. 4-5, https://www.miljodirektoratet.no/globalassets/publikasjoner/m830/m830.pdf, 13.09.2021.

[100] Gemini.no, 02.03.2021, *Vi trenger flere eksperter på skred og flom*, https://gemini.no/2021/03/vi-trenger-flere-eksperter-pa-skred-og-flom/, 19.10.2021.

[101] Gespräch mit Abelia, Mikal Kvamsdal, wirtschaftspolitischer Sprecher Technologie und Digitalisierung, 17.09.2021.

[102] Atea, 25.02.2021, *Når kompetanse, vekst og sikkerhetsmarkedet går hånd i hånd,* https://www.atea.no/siste-nytt/kompetanse-vekst-og-sikkerhetsmarkedet/, 18.10.2021.

[103] Gespräch mit Abelia, Mikal Kvamsdal, wirtschaftspolitischer Sprecher Technologie und Digitalisierung, 17.09.2021.

IT-Sicherheit ist ein Markt unter rapider Entwicklung und ein Fachbereich, in dem der Fachkräftemangel in Norwegen derzeit auf ca. 1.900 Personen beziffert wird. Für das Jahr 2030 wird dieser auf ca. 4000 Personen geschätzt. Die Kombination aus mangelnder Kompetenz im Markt und einem komplexen Gefährdungsbild hat dazu geführt, dass sowohl die nationale Sicherheitsbehörde, NorSis und der Sicherheitsrat der Wirtschaft (*Næringslivets sikkerhetsråd*) inzwischen norwegischen Unternehmen ohne eigene Abteilung für IT-Sicherheit empfiehlt, IT-Sicherheitsdienstleistungen extern von Experten einzukaufen.[104]

Abelia hat gemeinsam mit seinem Mitgliedsunternehmen Watchcom ein **Forum für Digitale Sicherheit** ins Leben gerufen. Große und bedeutende Akteure aus dem norwegischen Technologieumfeld und tonangebende staatliche Institutionen sind hier ebenfalls beteiligt. Ziel des Forums ist es, zentrale Technologieführer aus der Sicherheitsbranche zu sammeln, um Erfahrungen zu teilen und voneinander zu lernen. Dabei soll zu Technologieinnovationen inspiriert werden, welche die Sicherheit erhöhen und das Bewusstsein für mögliche Problemstellungen unter den Teilnehmern gestärkt werden.[105]

Auf der Website des norwegischen IT-Verbandes IKT Norge **werden Telekommunikation und Infrastruktur, Datenschutz, Sicherheit und Bereitschaft sowie FinTech** als wichtige Fokusbereiche hervorgehoben. Dabei kann erwähnt werden, dass die norwegische FinTech-Branche jung und stark wachsend ist. Sie besteht aus Akteuren in den Bereichen Sicherheit, Authentifizierung, Zahlungsmethoden, Verwaltung, Blockchain, P2P-Kredite usw.[106] Zentrale Branchennetzwerke sind NCE Finance Innovation und Oslo Fintech Hub.

3.2.2 Strukturen und Kooperationen

Die **Entwicklung digitaler Dienstleistungen und Produkte** findet häufig in privaten Unternehmen oder in Forschungs- und Entwicklungsorganisationen statt. Ein großer Anteil der kritischen Infrastrukturen des Landes ist im Besitz von privaten Unternehmen oder wird durch diese betrieben. Dies bedeutet, dass wichtige Beschlüsse zur Entwicklung und Sicherheit im digitalen Raum in hohem Maße von kommerziellen und nichtstaatlichen Akteuren gefasst werden. Somit ist die Rolle der öffentlichen Institutionen häufig begrenzt – dies erfordert eine enge **Kooperation zwischen öffentlichen und privaten Akteuren**. Diese Zusammenarbeit ist wichtig, um digitale Sicherheitsherausforderungen zu identifizieren, beleuchten und Erfahrungen zu diesen auszutauschen. Die Behörden sollen dazu beitragen, dass digitale Sicherheitsdienstleistungen in der freien Wirtschaft nachgefragt, entwickelt und angeboten werden, während durch den Aufbau nationaler Kapazitäten für die digitale Sicherheit auch die Inklusion der Kapazitäten privatwirtschaftlicher Akteure ermöglicht werden soll. In der sog. **„zivil-militärischen Zusammenarbeit“** sind die Einheiten des Verteidigungssektors von den Infrastrukturen und digitalen Diensten des zivilen Sektors abhängig. Dies bedeutet auch, dass die Herausforderungen im Hinblick auf digitale Sicherheit im zivilen Sektor auch eine Bedeutung für die Fähigkeit des Staates haben, sicherheitspolitische Krisen zu managen und Militäroperationen durchzuführen. In letzter Instanz bedeutet dies, dass digitale Angriffe auf die zivile Infrastruktur die Fähigkeit Norwegens, die nationale Sicherheit zu bewahren, herausfordern kann. Das **„Konzept der ganzheitlichen Verteidigung“ (*Totalforsvarskonseptet)*** umfasst sowohl die militärische Unterstützung der Zivilgesellschaft als auch zivile Unterstützung des Militärs. **Die internationale Cyberpolitik Norwegens,** festgehalten in einem offiziellen Dokument, soll die norwegischen Interessen bedienen, stabile und voraussehbare Rahmenbedingungen gewährleisten und Herausforderungen und Bedrohungen vorbeugen und vor diesen schützen. Die relevanten Behörden arbeiten mit anderen Nationen in der Prävention, Dedektion, Warnung vor und dem Management von digitalen Vorfällen zusammen. Ferner ist die Cyberpolitik ein wichtiges Element für die norwegische Teilnahme an relevanten internationalen Arenen. [119]

[104] Atea, 25.02.2021, *Når kompetanse, vekst og sikkerhetsmarkedet går hånd i hånd,* https://www.atea.no/siste-nytt/kompetanse-vekst-og-sikkerhetsmarkedet/, 18.10.2021.

[105] Abelia, 11.01.2016, *Sikkerhet*, https://www.abelia.no/bransjer/teknologi-og-digitalisering/sikkerhet/, 09.09.2021.

[106] IKT Norge, o. J., FinTech, https://www.ikt-norge.no/tema/fintech/, 09.09.2021.

3.2.3 Elektronische Kommunikation: Gesellschaftliche und technologische Entwicklungen

Die **nationale Telekommunikationsbehörde (Nkom)** ist die ausübende Aufsichts- und Verwaltungsbehörde für Post- und Telekommunikationsdienstleistungen. Die Behörde ist dem Ministerium für kommunale Angelegenheiten und Modernisierung untergeordnet, das Verkehrsministerium (*Samferdselsdepartementet, SD)* trägt die fachliche Verantwortung für Postangelegenheiten.[107] Nkom ist ein Teil des norwegischen Verteidigungssystems und arbeitet intensiv sowohl mit anderen regionalen Behörden als auch anderen Sicherheitsbehörden zusammen im Hinblick auf die Themen Sicherheit und Notfallbereitschaft. Die jährlichen Gefährdungs- und Risikoeinschätzungen des Nachrichtendienstes (*E-Tjenesten*), des Inlandsnachrichtendienstes (PST) und der nationalen Sicherheitsbehörde NSM sind wichtige Quellen für die Sicherheitsarbeit von Nkom. Nkom leitet auch das ***Ekomsikkerhetsforum***, ein Branchenforum bestehend aus Sicherheitsbehörden und Anbietern, welche sich gegenüber dem Sicherheitsgesetz verhalten müssen, zum gegenseitigen Austausch von Informationen zu Gefahrenquellen auf einem hochrangigen Niveau.[108] 2020 hat Nkom sich vor allem vier Risikobereichen gewidmet:

1. Schäden und **Unterbrechungen in der Telekommunikationsinfrastruktur als Konsequenz von Naturereignissen**. Sicherung der Funktionalität für eine weitere Digitalisierung, Erhöhung der Widerstandsfähigkeit der Infrastruktur im Takt mit physischen Belastungen.
2. **Kritische Kernfunktionen im Internet.** Grenzüberschreitende Anfälligkeiten und Herausforderungen, die auf internationalem Niveau gemanagt werden müssen. Schaffung von Funktionalität und Autonomie im „norwegischen Teil des Internets".
3. **Wachsende Bedeutung drahtloser Kommunikation.** Wachsende Anzahl von Endgeräten und Einheiten, die auf drahtloser Ebene kommunizieren, auch in kritischen Funktionen - erfordert erhöhte Aufmerksamkeit gegenüber Gefährdungen für die Datenintegrität und Konfidenzialität sowie Interferenzen, Jamming und Spoofing.
4. **Komplexe digitale Wertschöpfungs- und Lieferketten** aufgrund des neue **5G-Ökosystems**. Neue Akteure und Drittparteien werden enger in die Netzdienste verknüpft, wachsende Nutzung von u.a. Cloudlösungen und komplexen Automationslösungen. Integration von 5G in immer mehr **kritische Gesellschaftsfunktionen**. Die steigende Komplexität der Wertschöpfungs- und Lieferketten bringt im 5G-Ökosystem auch neue Risiken mit sich. Potenzielle Einfallstore für Cyberangriffe sollten identifiziert werden. Neben den großen Ausrüstern sollte auch kleineren Unterlieferanten Beachtung geschenkt werden, da diese auch Anfälligkeiten mit sich bringen können und leichter „unter das Radar" geraten können.[109]

Management von Cybervorfällen - Nkom EkomCERT

Nkom EkomCERT ist das digitale Reaktionsumfeld des norwegischen Telekommunikationssektors und stellt eine operative Einheit mit digitalen nationalen und internationalen Kontaktflächen aus. CERT steht hier für *Computer Emergency Response Team*. EkomCERT arbeitet eng mit den Sicherheitsorganisationen der Telekommunikationsakteure, dem nationalen Zentrum für Cyber Security (NSM NCSC) und anderen branchenverwandten Akteuren zusammen. EkomCERT verfügt über Spitzenkompenzen im Bereich der Gefährdungslage und im Bereich der sektorspezifischen Herausforderungen. Bei ernsthaften digitalen Vorfällen leistet EkomCERT den Telekommunikatonsakteuren auch Beistand in Form von Informationseinholung, Beratung und Koordinierung.[110]

Massives Wachstum des Internet der Dinge

Die Ausbreitung des sog. *Internet of Things* (IoT) ist ein zentraler Bestandteil in der weiteren Digitalisierung der Gesellschaft. Das Entwicklungspotenzial ist enorm und bereitet den Boden für neue Anwendungsfelder in mehreren Branchen und Sektoren. So z.B.

---

[107] Nasjonal Kommunikasjonsmyndighet (Nkom), o. J., *Om Nkom,* https://www.nkom.no/om-nkom, 13.10.2021.

[108] Nasjonal Kommunikasjonsmyndighet (Nkom) (2020), *EKOMROS 2020: Den digitale grunnmuren satt på prøve,* S. 19, https://issuu.com/nasjonalkommunikasjonsmyndighet/docs/ekomros_2020?fr=sZTZjZDE1Mjg1NjA, 13.10.2021.

[109] Nasjonal Kommunikasjonsmyndighet (Nkom) (2020), *EKOMROS 2020: Den digitale grunnmuren satt på prøve,* S. 27-29, https://issuu.com/nasjonalkommunikasjonsmyndighet/docs/ekomros_2020?fr=sZTZjZDE1Mjg1NjA, 13.10.2021.

[110] Nasjonal Kommunikasjonsmyndighet (Nkom), o. J., *Håndtering av cyberhendelser - Nkom EkomCERT*, https://www.nkom.no/sikkerhet-og-beredskap/nkom-ekomcert, 13.10.2021.

hat Oslo Sporveier, Betreiber des Straßenbahnnetzes in der norwegischen Hauptstadt, entschieden, seine alten **Signalanlagen** mit einer Lösung auszurüsten, welche auf das Mobilnetz von Telia zurückgreift. Die gleiche Infrastruktur, welche z.B. Pendler auf dem Weg zur Arbeit zum Surfen nutzen, sorgt also auch dafür, dass die Bahn pünktlich an ihr Ziel kommt. Dies ist nur ein Beispiel für den steigenden, kritischen Gebrauch der Mobilnetze. Neben neuen IoT-Anwendungen basierend auf 4G und 5G gibt es auch immer mehr **Lösungen, die auf freie Frequenzen basieren.** Ein beliebtes Kommunikationsprotokoll für das IoT ist LoRaWAN, welches v.a. für Sensornetzwerke, industrielle Steuerungen, Smart Homes oder Smart Cities geeignet ist. Mittelfristig wird erwartet, dass verschiedene IoT-Lösungen in zentrale Teile der Wertschöpfungsketten mehrerer kritischer Funktionen integriert werden. Die Nutzer der IoT-Lösungen sollten sich daher bewusst sein, dass die verschiedenen Kommunikationsprotokolle und -lösungen auch in unterschiedlichem Maß angreifbar bzw. anfällig sind. [111]

3.2.4 Wachsende Nachfrage nach IT-Sicherheit

Die Nachfrage nach IT-Sicherheit wächst. Die Anzahl relevanter Stellenausschreibungen im ersten 2021 war so hoch wie noch nie und mehrere Unternehmen in dem Bereich vermelden lange „Warteschlangen" unter ihren Kunden. **Atea, Mnemonic, Painkiller, Glasspaper und Accenture** sind externe IT-Beratungen in Norwegen. In einem Interview mit E24, Norwegens größtem Portal für Wirtschaftsnachrichten, geben alle die Rückmeldung, dass auch die Nachfrage nach ihren IT-Sicherheitsberatern im Laufe des letzten Jahres gewachsen ist. Sowohl international, als auch in Norwegen steigen die Cyberangriffe in ihrer Anzahl und Aggressivität. In Norwegen wurden u.a. Volua, Akva group, Toten Kommune und das norwegische Parlament im Laufe des Jahres 2021 angegriffen. Der norwegische Ölfonds hat inzwischen fünf Sicherheitsexperten rekrutiert, welche Penetrationstests (Hacking) durchführen, um Anfälligkeiten und Risiken aufzudecken. Der Ölfonds sucht weiterhin nach IT-Sicherheitsberatern.[112]

3.2.5 Satellitenbasierte Breitbandsysteme

Der Markt für Satellitenkommunikation entwickelt sich derzeit in die Richtung, dass höhere Leistungen zu niedrigeren Preisen erzielt werden können. Die bisher dominierende Lösung mit Satelliten in geostationären Bahnen wird nun durch Alternativen in niedrigeren Umlaufbahnen herausgefordert. Hierfür gibt es bereits heute fundierte Systeme, welche Datenverkehr und Telefondienstleistungen anbieten (z.B. **Globalstar** und **Iridium**). Aber auch neue Initiativen sind im Kommen, allen voran **Starlink**. Neue Systeme für niedrige Umlaufbahnen können, wenn sie sich durchsetzen, künftig als selbstständige alternative Kommunikationslösung für landbasierte Mobilnetze fungieren. Sie können jedoch auch ein integrierter Teil anderer Kommunikationslösungen werden. So z.B. hat das nationale Sicherheitsnetz ***Nødnett*** derzeit transportable Basisstationen mit satellitenbasierter Übertragung und Stromaggregaten. Somit können die Basisstationen installiert werden, ohne dass sie an die Infrastruktur im Boden angekoppelt werden müssen.[113]

3.2.6 Die digitale Transformation in kritischen Gesellschaftsfunktionen

Die digitale Transformation wird v.a. durch einen Bedarf nach höherer Wertschöpfung und der Erneuerung und Optimierung von Unternehmen und dem öffentlichen Sektor vorangetrieben. Sie bringt starke Änderungen für Infrastrukturen und Organisationen mit sich. Die Auswirkung auf die zivile Sicherheit ist davon abhängig, wie umfassend die digitale Transformation in den jeweiligen kritischen Funktionen sich gestaltet und wie abhängig die Gesellschaft von den neuen Diensten ist.[114]

---

[111] Nasjonal Kommunikasjonsmyndighet (Nkom) (2020), *EKOMROS 2020: Den digitale grunnmuren satt på prøve,* S. 24, https://issuu.com/nasjonalkommunikasjonsmyndighet/docs/ekomros_2020?fr=sZTZjZDE1Mjg1NjA, 13.10.2021.

[112] E24.no, 14.08.2021, *Bedriftene står i kø for IT-ekspertise: – Udekket behov som bare øker,* https://e24.no/naeringsliv/i/Ep6yoa/bedriftene-staar-i-koe-for-it-ekspertise-udekket-behov-som-bare-oeker, 15.10.2021.

[113] Nasjonal Kommunikasjonsmyndighet (Nkom) (2020), *EKOMROS 2020: Den digitale grunnmuren satt på prøve,* S. 25, https://issuu.com/nasjonalkommunikasjonsmyndighet/docs/ekomros_2020?fr=sZTZjZDE1Mjg1NjA, 13.10.2021.

[114] FFI (2020), *Samfunnssikkerhet mot 2030*, S. 83, https://publications.ffi.no/nb/item/asset/dspace:6641/20-00530.pdf, 31.08.2021.

Bedarf für neue Sicherheitslösungen durch das 5G-Netz

Wie in Kapitel 3.2.3 erwähnt, wird erwartet, dass 5G in immer mehr kritische Gesellschaftsfunktionen integriert wird. Trotz der vielen Vorteile des 5G-Netzes wird dessen Komplexität jedoch so hoch sein, dass für den Betrieb und die Instandhaltung künstliche Intelligenz genutzt werden muss. So wird das Netzwerk viel dynamischer – jedoch werden die Betreiber keine gänzliche Übersicht über ihre Systeme haben und eine Sicherheitsgarantie ist beinahe unmöglich. Außerdem werden durch die steigende Nutzung von Software die Netzwerke anfälliger für Angriffe, die wir schon heute aus der IT-Welt kennen.[115] Somit steigt der **Bedarf für Sicherheitslösungen,** welche spezifisch zum Schutz der neuen Netzwerktechnologien entwickelt worden sind. **Künstliche Intelligenz und maschinelles Lernen** können für das schnellere Aufdecken von Verdachtsaktivitäten in solchen software-definierten Netzwerken entscheidend sein.[116]

Die **Clouddienste** der Zukunft schaffen neue Möglichkeiten für Cyberkriminelle. Die wachsende Nutzung von Clouddiensten bedingt, dass immer mehr Daten in Clouds liegen. Daher wird erwartet, dass Clouddienstleister künftig Angriffsziele sind. Man muss auch damit rechnen, dass Cyberkriminelle künftig versuchen werden, Informationen in Datenströmen in und aus der Cloud auszunutzen und versuchen, sich Zugang zu den Datenströmen einzelner Organisationen oder Unternehmen zu verschaffen.[117]

Nødnett: Vorbeugung von digitalen Vorfällen und „Das Nødnett der nächsten Generation"

Der staatlichen Sicherheitsbehörde DSB wurden Mittel für **die Stärkung der Kapazitäten zur Prävention, Aufdeckung und dem Management digitaler Vorfälle im Nødnett** bewilligt. Dafür hat das DSB ein Projekt für die Beschaffung, Gründung und Inbetriebnahme dieses Prozesses ins Leben gerufen. Dienstleistungen und Lösungen für das Aufdecken von Sicherheitsvorfällen sowie Unterstützung zur Analyse solcher Vorfälle werden durch öffentliche Ausschreibungen beschafft (mehr dazu in Kapitel 5.1). Diese Dienste werden in der Regel von Unternehmen angeboten, welche 24/7-Sicherheitszentren betreiben und Spitzenkompetenzen auf dem Gebiet der Aufdeckung und des Managements digitaler Vorfälle besitzen.[118]

Das aktuelle Kommunikationsnetz für die zivile Sicherheit (*Nødnett*) wurde als separates Kommunikationsnetzwerk mit eigenen Basisstationen und Kommunikationslinien errichtet. Das DSB und die nationale Kommunikationsbehörde Nkom untersuchen derzeit die Möglichkeiten für den Bau des „***Nødnett* der nächsten Generation"** basierend auf kommerzielle Netze**.** Das 5G-Netz als einer der möglichen Kandidaten ermöglicht eine deutlich höhere Flexibilität für die Einführung fortgeschrittenerer Dienste im *Nødnett*. Eine Bedingung dafür, das *Nødnett* in kommerziellen Netzen zu betreiben ist, dass Sicherheit und Widerstandsfähigkeit mindestens genau den gleichen Standard wie im aktuellen Netz innehalten. Im Dezember 2017 wurde entschieden, dass die Frequenzressourcen im 700 MHz-Band für interessierte kommerzielle Telekommunikationsanbieter in Norwegen geöffnet werden sollen. Die Frequenzen haben gute Netzdeckungseigenschaften und sind wichtig für die Ausbreitung avancierter Mobildienstleistungen im ganzen Land. Das 700 MHz-Band ist eine der ausgewählten Ressourcen für den künftigen Ausbau von 5G. Künftige Kommunikationslösungen für Notruf- und Bereitschaftseinheiten sowie das Militär sollen auch von den kommerziellen Mobilfunkdienstleistern geliefert werden können. Es soll daher dafür gesorgt werden, dass die Bedarfe dieser systemrelevanten Nutzer durch eine Kombination von behördlichen Auflagen und kommerziellen Ausschreibungen geschützt werden.[119]

---

[115] FFI (2020), *Samfunnssikkerhet mot 2030*, S. 33, https://publications.ffi.no/nb/item/asset/dspace:6641/20-00530.pdf, 31.08.2021.

[116] Computerworld, 05.03.2020, *Hvor bekymret bør vi være for 5G-sikkerheten?*, https://www.cw.no/artikkel/debatt/hvor-bekymret-bor-vi-vaere-5g-sikkerheten, 31.08.2021.

[117] FFI (2020), *Samfunnssikkerhet mot 2030*, S. 35, https://publications.ffi.no/nb/item/asset/dspace:6641/20-00530.pdf, 31.08.2021.

[118] DSB (2021), *DSB årsrapport 2020*, S. 60, https://www.dsb.no/globalassets/dokumenter/rapporter/dsbs-arsrapport-2020.pdf, 30.08.2021.

[119] Departementene (2019), *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*, S. 24, https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf, 30.08.2021.

IT-Lösungen im Gesundheitssektor

Als einer der Pioniere in dem Bereich der Nutzung von IT-Lösungen im Gesundheitssektor, werden in Norwegen u.a. digitale Sicherheitslösungen für das zentrale elektronische Management des Sektors (Infrastruktur) sowie digitale Sicherheitslösungen in Gesundheits- und Sozialdiensten sowie in cyberphysischen Systemen nachgefragt. Auch die digitale Sicherheit der häuslichen Pflege via 5G wird in Zukunft ein wichtiges Thema darstellen.[120]

4 Rechtliche Rahmenbedingungen

4.1 Allgemeines

Obwohl Norwegen kein EU-Mitglied ist, ist das Königreich seit 1994 als **Mitglied des Europäischen Wirtschaftsraums** (EWR) an das europäische Recht angebunden. Der EWR-Vertrag (das Abkommen über den europäischen Wirtschaftsraum) ist ein völkerrechtliches Abkommen zwischen den EFTA-Staaten auf der einen Seite und der EU auf der anderen. Als EWR-Mitglied nimmt Norwegen am europäischen Binnenmarkt teil, weswegen alle binnenmarktrelevanten Verordnungen und Richtlinien auch in Norwegen in nationales Recht umgesetzt werden.

Der EWR-Vertrag hat den grenzüberschreitenden Handel von Waren und Dienstleistungen zwischen Norwegen und den EU-Ländern in hohem Maße vereinfacht. Die laufende Harmonisierung in der EU, welche durch den EWR-Vertrag weitergeführt wird, beinhaltet, dass Gewerbetreibende in stetig mehr Bereichen innerhalb des EWR auf gleiche oder ähnliche Regelungen wie in ihrem Heimatland treffen. Große Teile des EU-Rechts, u.a. die Grundfreiheiten, freier Warenverkehr, Personenfreizügigkeit, Dienstleistungsfreiheit, freier Kapital- und Zahlungsverkehr, sowie das Wettbewerbs- und Beihilfereglement der EU sind im EWR-Vertrag enthalten und in das interne Recht der EWR/EFTA-Staaten umgesetzt worden. Beispielsweise wurde bereits zum 1.1.2006 die EU-Richtlinie 96/71/EF EG zur Entsendung von Arbeitnehmer in Norwegen implementiert. Auch wurde bereits am 21.07.2007 die Richtlinie 2006/123/EG bzgl. der gegenseitigen Anerkennung von Berufsqualifikationen in Norwegen umgesetzt. Weiterhin hat der Grundsatz des Verbotes der Ungleichbehandlung zwischen nationalen Unternehmern und Unternehmern anderer Staaten dazu beigetragen eine Vielzahl von Handelshindernissen zu beseitigen.

Durch den EWR-Vertrag wurden Steuern und Abgaben noch nicht harmonisiert. Beim Export von Deutschland nach Norwegen können also Zölle und Abgaben zu zahlen sein.

Da europäische Richtlinien in nationales Recht umgesetzt werden, entspricht Vieles in Norwegen dem, was man aus Deutschland kennt. In vielen Bereichen, wie dem Handelsvertreterrecht, entspricht das norwegische Recht dem deutschen. Auch eine Vielzahl von Verbraucherschutzbestimmungen sind gleich. Das darf jedoch nicht über die teils erheblichen Unterschiede hinwegtäuschen.

Besonders für ausländische Unternehmen, gibt es eine Reihe wichtiger Bestimmungen zu beachten. So muss z.B. ein **Fiskalvertreter** benannt werden, wenn ein ausländisches Unternehmen in Norwegen nur als unselbständige Filiale auftritt, jedoch innerhalb einer Periode von 12 Monaten umsatzsteuerpflichtigen Umsatz von über 50.000 NOK (ca. 5.000 EUR) erzielt.

In Norwegen gibt es **kein allgemeines zivilrechtliches Gesetzbuch**, wie es das deutsche Recht in Form des Bürgerlichen Gesetzbuches (BGB) kennt. Das norwegische Zivilrecht besteht aus einer Vielzahl von Einzelgesetzen. Einige Themen, wie z.B. Werkverträge, werden vom norwegischen Recht überhaupt nicht behandelt.

Verträge sind teilweise weniger detailliert als in Deutschland üblich. Details werden häufig erst später und im Einzelfall geklärt. Bei Streitigkeiten zwischen Vertragspartnern tendieren die norwegischen Gerichte häufiger zu einer Schlichtung durch einen

[120] Gespräch mit Norwegian Center for Cybersecurity in Critical Sectors, Prof. Sokratis K. Katsikas, Director, 01.02.2020.

Vergleich. Dennoch müssen Ansprüche im Streitfall rechtlich fundiert begründet und bewiesen werden. Es ist grundsätzlich empfehlenswert, einen Vertrag nach norwegischem Recht, der die wichtigsten Punkte im Detail festhält, aufzusetzen. Einige Branchenorganisationen stellen Musterverträge bereit. Zu beachten ist, dass das norwegische Recht keinen Eigentumsvorbehalt kennt. Werden beim Warenexport aus Deutschland die deutschen allgemeinen Geschäftsbedingungen zugrunde gelegt, verliert der Eigentumsvorbehalt seine Wirkung. Eine Absicherung bietet das Verkäuferpfandrecht. Somit könnten Waren zwangsversteigert und der Erlös dem Verkäufer zugeschrieben werden. Das Verkäuferpfandrecht ist grundsätzlich insolvenzfest und verhindert außerdem, dass Waren durch den Käufer ohne Zustimmung des Verkäufers an Dritte weiterverkauft werden. Für Waren, die für den Weiterverkauf bestimmt sind, kann vom Verkäuferpfandrecht abgesehen werden.

Die Zahlungsmoral ist in Norwegen sehr hoch. Allerdings wird auch eine pünktliche Lieferung erwartet. Sollte es zu einem Zahlungsverzug kommen und Mahnungen keine Wirkung zeigen, kann eine formelle Zahlungsaufforderung ausgesprochen werden. Dabei wird eine Frist gesetzt und eine Zwangsvollstreckung angedroht. Auch eine Klage ist ein möglicher Weg. Jedoch muss der Schuldner darüber vorher informiert werden. In der Regel wird die Klage bei dem örtlichen Vergleichsgericht eingereicht. Erst wenn die Klage dort eingestellt wird, was bei wirtschaftsrechtlichen Angelegenheiten häufig der Fall ist, ist der Weg zu den ordentlichen Gerichten frei.

Das norwegische Gesellschaftsrecht kennt im Wesentlichen **drei verschiedene Unternehmensformen**: Gesellschaften mit beschränkter Haftung, Personengesellschaften (bei denen die Teilnehmer entweder gemeinsam oder jeder für sich in vollem Umfang persönlich für die Verbindlichkeiten des Unternehmens haften) und die norwegische Niederlassung/Filiale einer ausländischen Gesellschaft. Die Mehrheit der Unternehmen operiert als Gesellschaften mit beschränkter Haftung. Innerhalb der Geschäftsführung wird zwischen zwei Organen unterschieden: dem Vorstand und dem Geschäftsleiter.

4.1.1 Administratives

Ausländischen Unternehmen, welche in Norwegen wirtschaftlich in Erscheinung treten möchten, z.B. um ein Projekt auszuführen oder Personal zu entsenden, stellen sich eine Reihe administrativer, sowie rechtlicher Herausforderungen, die es zu beachten gilt. Da diese oft ein nicht unerhebliches Maß an Zeit- und Organisationsaufwand, sowie Kosten mit sich bringen, empfiehlt es sich, sich frühzeitig über die jeweils zu erfüllenden Verpflichtungen zu informieren. Zu den wichtigen Punkten zählen u. a. folgende Themen:

- Registrierung im zentralen norwegischen Handelsregister
- Umsatzsteuerliche Registrierung (Fiskalvertretung)
- Steuerliche Meldepflichten
- ID-Kontrolle
- Polizeiliche Aufenthaltsmeldung
- Sozialversicherung
- Lohnsteuerpflicht/A-Meldung

Details zu diesen Verpflichtungen stellt die Deutsch-Norwegische Handelskammer auch auf Ihrer Website bereit und steht für Fragen hinsichtlich administrativer Verpflichtungen, sowie Steuerrecht und Arbeitsrecht für ausländische Arbeitnehmer in Norwegen zur Verfügung.

4.1.2 Zollinformationen

Wer Waren oder Dienstleistungen nach Norwegen exportieren möchte, sollte sich rechtzeitig mit den geltenden Vorschriften auseinandersetzen. Im Nicht-EU-Land Norwegen weicht das Procedere zum Teil erheblich von gewohnter EU-Praxis ab. Für den Import von Waren und Dienstleistungen ist eine Organisationsnummer (s.o. unter 4.1) zwingend erforderlich. Spätestens nach Vertragsunterzeichnung und sobald sich eine Zeitperspektive abzeichnet, sollte man sich in Norwegen registrieren lassen und sich Gedanken über die Etablierungsform machen.

Beim Import nach Norwegen sind in erster Linie Importabgaben zu bezahlen. Hinzu kommen eventuell Zoll und Verbrauchssteuer. Die Importabgaben können für ein Unternehmen mit hohen Kosten verbunden sein. Neu gegründete Unternehmen können unter bestimmten Voraussetzungen eine Voranmeldung der MwSt. beantragen, um die bereits beglichene MwSt. (hierunter auch Importabgaben) zurück zu erhalten. Die Einrichtung eines Zollagers beim Warenimport nach Norwegen, kann finanzielle Vorteile bringen. Beim Import von Arbeitsausrüstung beziehungsweise industriellen oder landwirtschaftlichen Gütern, die vorübergehend zur Reparatur oder Bearbeitung importiert und später wieder ausgeführt werden, können gesonderte Regelungen bei Ankunft der Güter in Norwegen geltend gemacht und so Kosten eingespart werden.

Generell ist der Wareneigentümer verpflichtet den Import der nach Norwegen verbrachten Waren vorzunehmen und die Einfuhrumsatzsteuer zu tragen. Bei klassischen Werkverträgen obliegt somit diese Pflicht dem liefernden Unternehmen. Hier bietet es sich an, mit einem norwegischen Zollagenten die einzelnen Schritte hinsichtlich der Verzollung/ Vorfinanzierung abzustimmen. Von Leistungen losgelöste einfache Warenlieferungen können, sofern diese vertraglich unabhängig von einer Leistung vereinbart werden, vom norwegischen Kunden importiert werden. Für die vorübergehende Einfuhr von Geräten und Werkzeugen kann in Einzelfällen ein ATA-Carnet von der örtlichen IHK ausgestellt werden. Sofern dieses nicht vorliegt, fallen grundsätzlich bei der Einfuhr von Geräten die Einfuhrumsatzsteuer in Höhe von 25 Prozent und ggfs. weitere Abgaben an.

Beim Import zollpflichtiger Produkte aus einem Land, das ein Freihandelsabkommen mit Norwegen unterzeichnet hat, hat ein Importeur unter bestimmten Voraussetzungen Anspruch auf einen so genannten Präferenzzollsatz, also einen niedrigeren Zollsatz. Diesbezügliche Ansprüche sind in der Zollerklärung beim Import geltend zu machen. Andernfalls ist es unter bestimmten Voraussetzungen möglich, innerhalb von drei Jahren eine entsprechende Korrektur zu beantragen.

4.2 Regelwerke und Gesetze bei Naturereignissen und absichtlichen Handlungen

Die norwegische Regierung hat sich für die Entwicklung von Regelwerken sowohl im Hinblick auf Naturereignisse als auch auf absichtliche kriminelle Handlungen eingesetzt. Die Entwicklung der Regelwerke definiert gleichzeitig den Rahmen für die Präventionsarbeit.[121]

Sicherheitsgesetz (*Sikkerhetsloven*)

Das neue Sicherheitsgesetz trat 2019 in Kraft und stärkt die Fähigkeit der Gesellschaft, absichtliche kriminelle Handlungen, welche einen Angriff auf die nationale Sicherheit darstellen können, vorzubeugen, aufzudecken und entgegenzuwirken. Die Implementierung des Sicherheitsgesetzes sorgt für ein vertretbares Sicherheitsniveau für zu schützende Informationssysteme, Objekte und Infrastrukturen.[122]

Der Begriff der **nationalen Sicherheit** bezieht sich auf das Sicherheitsgesetz und beschreibt den Schutz der nationalen Sicherheitsinteressen. Im Gesetz wird darin die Souveränität des Staates, die territoriale Integrität und die demokratische Staatsordnung verstanden. Darüber hinaus bezieht sich der Begriff auf sicherheitspolitische Interessen bzgl.

- Die Aktivitäten, Sicherheit und Handlungsfreiheit der obersten Staatsorgane
- Das Militär, die Sicherheits- und Bereitschaftsorgane
- Das Verhältnis zu anderen Staaten und internationalen Organisationen
- Die ökonomische Stabilität und Handlungsfreiheit
- Die grundlegende Funktionalität und Sicherheit der Gesellschaft bzw. Bevölkerung.

[121] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 8, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 26.08.2021.

[122] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 8, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 26.08.2021.

Das Wirkungsfeld des Sicherheitsgesetzes ist die Staatssicherheit und dieser Teil der zivilen Sicherheit ist von wesentlicher Bedeutung für die Fähigkeit des Staates, die nationalen Sicherheitsinteressen zu wahren. Das neue Sicherheitsgesetz hat noch ein weiteres Wirkungsfeld im Gegensatz zu der vorangegangenen Version. Dieses ist an die gesellschaftliche Entwicklung und die veränderte Gefährdungslage angepasst, darunter die **enge Verknüpfung zwischen ziviler Sicherheit und Staatssicherheit.** Das Wirkungsfeld des Gesetzes wird deutlicher durch die Identifikation grundlegender nationaler Funktionen definiert. Dies sind Dienstleistungen, Produktion oder andere Unternehmensformen mit einer so hohen Bedeutung, dass eine eingeschränkte oder geschädigte Funktionalität die Fähigkeit des Staates, nationale Sicherheitsinteressen zu wahren, einschränkt.[123]

Bereitschaftspflicht der Kommunen

Durch die Bereitschaftspflicht der Kommunen, welche im **Gesetz zum Schutz der Zivilbevölkerung (*sivilbeskyttelsesloven*)** festgeschrieben ist, ist die Rolle der Kommunen für die zivile Sicherheit definiert. Das Gesetz verpflichtet die Kommunen, systematisch und ganzheitlich über alle kommunalen Sektoren hinweg die zivile Sicherheit zu fördern. Diese Aktivitäten sollen das Risiko für den Verlust von Leben, Gesundheit und materiellen Werten minimieren. Die Kommunen unterliegen strengen Gesetzen, welche Anforderungen an die zivile Sicherheit stellen. Durch die Bestimmungen zur kommunalen Bereitschaftspflicht kommt den Kommunen die Rolle als lokaler Koordinator durch gesetzliche Pflichten zu. Diese bestehen darin, dass die Kommunen besondere Maßnahmen für die systematische Arbeit mit der zivilen Sicherheit nutzen, eine intersektorale Perspektive einnehmen und mit anderen relevanten Sicherheitsakteuren zusammenarbeiten können.[124] **Das Plan- und Baugesetz (*Plan- og bygningsloven*)** ist das zentrale Mittel, um eine gute Planung sicherzustellen.

Staatliche Planungsrichtlinien zur Klimaanpassung

Klimaänderungen, die zu häufigeren Überschwemmungen und Erdrutschen sowie zu Problemen mit Oberflächenwasser in städtischen Gebieten führen, fordern die Flächennutzung besonders heraus. Das norwegische Plan- und Baugesetz verlangt die Gefahreneinschätzung für Naturschäden im Rahmen aller Planungs- und Bauaktivitäten und gibt den Kommunen die Möglichkeit, die Erschließung neuer Gebiete so zu steuern, dass dabei Areale gewählt werden, die weniger anfällig für Klimaänderungen sind, oder wo Maßnahmen durchgeführt werden können, die eine Anfälligkeit vorbeugen.[125]

Die staatlichen Planungsrichtlinien für Klimaanpassung wurden 2018 definiert und enthalten Vorgaben für die Planungsvorhaben der Kommunen, Verwaltungsbezirke und des Staates, um das Risiko durch Klimaänderungen zu begrenzen oder zu umgehen. Diese Vorgaben sollen auch zur Reduktion von Klimagasemissionen und zu einer umweltfreundlichen Energiewende beitragen. Die Planungsprozesse sollen auch zur Vorbereitung und Anpassung der Gesellschaft auf die Klimaänderungen beitragen.[126]

Versicherungen gegen Schäden für Naturereignisse

Da einzelne Gebiete in Norwegen besonders gegenüber Naturereignissen ausgesetzt sind, gibt es hier eine einzigartige, gesetzlich festgelegte Versicherungsordnung bei Naturschäden, welche beinhaltet, dass alle Versicherungen für Gebäude oder mobile Güter auch Schäden durch Naturereignisse umfassen. Die Versicherungsgesellschaften, die auch gegen Brände versichern, müssen laut dem norwegischen Versicherungsgesetz auch Mitglied im *Naturskadepool* sein, welcher von der Branchenorganisation Finans Norge verwaltet wird. Die Schadensversicherung für Naurereignisse deckt somit Gebäudeschäden und Schäden an beweglichen Gütern. Es

[123] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 12, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 26.08.2021.

[124] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 104-105, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 31.08.2021.

[125] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 105-106, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 26.08.2021.

[126] Regjeringen.no, 28.09.2018, *Statlige planretningslinjer for klima- og energiplanlegging og klimatilpasning*, https://www.regjeringen.no/no/dokumenter/statlige-planretningslinjer-for-klima--og-energiplanlegging-og-klimatilpasning/id2612821/, 31.08.2021.

gilt eine gleiche Prämienrate für alle Versicherten, sodass alle gleichermaßen einzahlen und das Risiko für die Bewohner der Risikogebiete tragen. Die Versicherungsbranche hat somit eine gute Grundlage für das Management versicherungstechnischer Folgen von Naturkatastrophen geschaffen. Dies umfasst Bereitschaftsprozesse, die Tätigkeit der Sachverständigen sowie Rückstellungen von Kapital.[127]

Gesetz zur digitalen Sicherheit

Digitale Sicherheit gehört zu den Prioritäten der norwegischen Regierung. Diese möchte ein Gesetz zur digitalen Sicherheit verabschieden, welches die NIS-Richtlinie, die Richtlinie zu den Maßnahmen für ein hohes, gemeinsames Sicherheitsniveau in Netzwerken und IT-Systemen in der gesamten EU, umsetzt. Ferner untersucht die norwegische Regierung fortlaufend, wie EU-rechtliche Anforderungen zur digitalen Sicherheit in das norwegische Recht aufgenommen werden können.[128] Die NIS-Richtlinie wurde 2016 von der EU beschlossen und verfolgt das Ziel, die digitale Sicherheit in der EU zu erhalten.[129]

Am 16. Dezember 2020 hat die EU-Kommission einen Vorschlag vorgelegt, welcher die NIS-Richtlinie künftig ersetzen soll. Dieser ist Teil eines Maßnahmenpaketes, welches die Widerstandsfähigkeit der digitalen und physischen Infrastruktur im öffentlichen und privaten Sektor, den relevanten Behörden und der gesamten EU verbessern soll. Der Vorschlag zur neuen Richtlinie ist umfassend und betrifft viele verschiedene Gesellschaftsbereiche. Die NIS2-Richtlinie wird ein deutlich breiteres Wirkungsfeld umfassen als ihr Vorgänger, indem noch mehr Sektoren in Betracht gezogen werden, welche sowohl für die Wirtschaft als auch die Gesellschaft als kritisch angesehen werden.[130]

Zum aktuellen Zeitpunkt ist die geltende NIS-Richtlinie noch kein Teil des EWR-Vertrages, aber es wird erwartet, dass sich dies demnächst ändert. In Norwegen wurde ein Gesetzesvorschlag ausgearbeitet, der die geltende Richtlinie in das norwegische Recht implementiert. Der Vorschlag zur neuen Richtlinie hat keine direkten Konsequenzen für den norwegischen Gesetzesvorschlag. Sollte jedoch das Gesetz beschlossen werden, wird dies Gegenstand einer Revision, sollte die NIS2-Richtlinie ein Teil des EWR-Vertrages werden.[131]

Digitale Sicherheit bei Produkten und Dienstleistungen

Die 5G-Technologie ermöglicht eine umfassendere Nutzung von Sensortechnologie und die Sammlung von Big Data durch Produkte und Dienste, die mit dem Internet verbunden sind. Gesundheits- und Pflegetechnologie, Smart Cities und smarte Transportsysteme sind Beispiele für die Nutzung des Internet of Things, welche neue Möglichkeiten der Wertschöpfung und eine höhere Produktivität mit sich bringen.[132]

Der IKT-Sicherheitsausschuss der norwegischen Regierung empfiehlt, dass die Verantwortung für digitale Sicherheit bei Produkten und Diensten, die mit dem Internet verbunden sind, stärker vom Verbraucher auf die Produzenten oder Dienstleister umgelagert wird. Der Ausschuss ist der Meinung, dass Norwegen seine internationale Kooperation fortsetzen sollte, insbesondere im Hinblick auf Regelwerksprozesse in der EU. Die norwegische Regierung betont, dass Verbraucher smarte Produkte

[127] Finans Norge, o. J., *Naturskadeforsikring*, https://www.finansnorge.no/tema/skadeforsikring/naturskadeforsikring/, 13.09.2021.

[128] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 8, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 26.08.2021.

[129] Regjeringen.no, 19.04.2021, *NIS2-direktivet*, https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/, 31.08.2021.

[130] Regjeringen.no, 19.04.2021, *NIS2-direktivet*, https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/, 31.08.2021.

[131] Regjeringen.no, 19.04.2021, *NIS2-direktivet*, https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/, 31.08.2021.

[132] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 86, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 31.08.2021.

und Online-Dienste nutzen können, ohne befürchten zu müssen, dass ihre Personendaten missbraucht werden. Datensicherheit ist auch eine Voraussetzung dafür, dass die Produkte und Dienste im Sinne ihres Zwecks funktionieren.[133]

Digitale Sicherheit im Zusammenhang mit smarten Produkten und Online-Diensten ist ein internationales Thema. Daher beteiligt sich die norwegische Regierung auch an der internationalen Arbeit in diesem Bereich. Dies gilt insbesondere für die Implementierung EU-rechtlicher Anforderungen in das norwegische Recht. Eine relevante Initiative ist die EU-Verordnung **Cybersecurity Act**. Dessen Ziel ist es, einen funktionierenden Binnenmarkt mit einem hohen Niveau an Cybersicherheit, Widerstandsfähigkeit Vertrauen zur EU zu sichern. Dies soll u.a. durch einen gemeinsamen europäischen Rahmen für die Sicherheitszertifizierung von IKT-Produkten, -dienstleistungen und -prozessen erreicht werden. Die Initiative ergänzt und unterstützt die Implementierung der NIS-Richtlinie.[134] Die Cyber-Security-Verordnung erfordert Gesetzesänderungen und eine Implementierung in den EWR Vertrag verlangt daher die Zustimmung des Parlaments. Das Justizministerium wird mit anderen, betroffenen Ministerien einen Vorschlag für die Durchführung im norwegischen Recht vorlegen. Eine vorläufige Bewertung schreibt vor, dass die Verordnung in Gesetzesform implementiert wird, mit der Option darauf, dass eventuelle Implementierungsrechtsakte als Vorschriften in diesem Gesetz festgesetzt werden.[135]

Sowohl künstliche Intelligenz als auch die Virtualisierung in der Cloud kann sich auf die zivile Sicherheit auswirken. Zum einen wird die Entwicklung die juristischen Herausforderungen, die Cloud-Daten mit sich bringen, verstärken. Bisher konnte immer sehr genau angezeigt werden, wo eigene Daten gespeichert sind. Durch die Virtualisierung wird dies deutlich schwieriger. Die Konsequenzen sind, dass die Behörden weniger Regulierungsmöglichkeiten erhalten und dass es in häufigeren Fällen unklar ist, welche Rechtssprechung gilt. Dadurch ändert sich auch die Möglichkeit der Behörden, neue Anfälligkeiten durch neue Technologien zu kontrollieren oder zu managen.[136]

Rahmen für IT-Sicherheitsvorfälle

NSM hat Kapazitäten, um bei der Prävention und dem Management von Netzwerkoperationen im öffentlichen und privaten Sektor zu unterstützen. Es wurde ein eigener Rahmen für IT-Sicherheitsvorfälle entwickelt, welcher die Kooperation zwischen betroffenen Organisationen, den Reaktionsumfeldern der Sektoren und NSM NorCert reguliert, um sich auf einen Vorfall vorzubereiten oder auf diesen zu reagieren, sobald es diesen gibt. Dieser Rahmen wurde vor allem für Vorfälle in Friedenszeiten entwickelt, kann aber auch auf Situationen übertragen werden, in denen das nationale Bereitschaftssystem zur Anwendung kommt.[137]

4.3 Technische Standards (Standards, Normen und Zertifizierung)

Meteorologische Gefahrenwarnungen

Seit Mai 2018 stuft das meteorologische Institut Norwegens seine Gefahrenwarnungen in die Farben gelb, orange und rot ein. Rot wird dann verwendet, wenn eine extreme Wetterlage erwartet wird. Die Gefahrenwarnungen werden entsprechend des *Common Alerting Protocol* (CAP) ausgestellt, einem internationalen Standard. Neben Extremwetterwarnungen enthält die CAP-Meldung Informationen zum Gefahrengrad und die Wahrscheinlichkeit des Eintreffens. Um das Verständnis für die Warnungen zu erhöhen, enthält die CAP-Meldung auch mögliche Konsequenzen und eine Beschreibung des geltenden geographischen Gebiets. Die

---

[133] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 86, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 31.08.2021.

[134] JD (2020), *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, S. 86, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 31.08.2021.

[135] Regjeringen.no, 03.12.2019, *Cybersikkerhetsforordningen*, https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2017/nov/cybersecurity-act/id2590048/, 31.08.2021.

[136] FFI (2020), *Samfunnssikkerhet mot 2030*, S. 35, https://publications.ffi.no/nb/item/asset/dspace:6641/20-00530.pdf, 31.08.2021.

[137] NSM, o. J., *Rammeverk for håndtering av IKT-hendelser*, https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/, 31.08.2021.

Gefahrenwarnungen des MET unterscheiden auch zwischen Sturzregen und Regen, da dies oft für die Sicherheit der Prognosen und die Schäden entscheidend sein kann.[138]

Standard Norge

Norwegen ist, vertreten durch die Organisation „Standard Norge", Mitglied im Europäischen Komitee für Normung (CEN) und der internationalen Organisation für Normung (ISO). „Standard Norge" ist als Interessensorganisation für Bildung, Wissenschaft und Forschung registriert. Es ist eine Mitgliedsorganisation, der Forschungsinstitute, Interessensorganisationen, Behörden, Verbraucherorganisationen und Wirtschaftsvertreter angehören. Aufgrund der CEN-Mitgliedschaft, die Norwegen zur Umsetzung der CEN-Normen verpflichtet, haben fast 95 Prozent der in Norwegen geltenden Normen einen europäischen Ursprung. ISO-Normen werden lediglich nach Bedarf umgesetzt.

Die in Norwegen geltenden Normen werden als „Norsk Standard" (Deutsch: Norwegischer Standard) bezeichnet und haben unterschiedliche Klassifizierungen.[139]

Standards für die digitale Sicherheit

Standard Norge verfügt über ein eigenes Komitee für IT-Sicherheit, Cybersicherheit und dem Schutz von Personendaten. Dieses hat eine große Auswahl an internationalen Standards in Betracht gezogen, priorisiert und schließlich in drei „Pakete" kategorisiert. Das Paket 1-2-3 wurde geschnürt, um Unternehmen dabei zu unterstützen, ihre Aktivitäten im Bereich der Cybersicherheit zu systematisieren und angebrachte Maßnahmen zu implementieren, sobald Risiken identifiziert werden. Die Verantwortung für Cybersicherheit und den Schutz von Personendaten liegt bei der Unternehmensführung und den Vorständen der Firmen.[140]

Grundpaket 1 sind die gesammelten Standards von Standard Norge zum Thema IT-Sicherheit. Dieses enthält Standards, welche alle Unternehmen kennen sollten, um eine grundlegende IT-Sicherheit gewährleisten zu können. Die zwei wichtigsten Standards sind:

- NS-ISO/IEC 27001 Informationstechnologie – Sicherungstechniken – Managementsysteme für IT-Sicherheit – Anforderungen (*enthält Anforderungen, nach denen das Managementsystem der Unternehmen zur Informationssicherheit zertifiziert werden können)*
- NS-ISO/IEC 27001 Informationstechnologie – Sicherungstechniken – Maßnahmen zur Informationssicherung *(enthält Ratschläge und Maßnahmen zur Einführung eines Steuerungssystems im Hinblick auf die Anforderungen aus NS-ISO/IEC 27001)*

Die Standards in **Grundpaket 2** haben eine erweiterte Funktion, welche weiter reichen und Unterstützung zur Implementierung von Kontrollfunktionen beinhalten, um Risiken für die Cybersicherheit vorzubeugen. Teil dieses Pakets sind Standards für Clouds, der Umgang mit sensiblen personenbezogenen Informationen (GDPR) sowie Information security governance.

Die Standards in **Grundpaket 3** beinhalten u.a. sektorenspezifische Standards, aber auch verschiedene Standards zu den Themen Speicherung sowie die Beweissicherung bei konkreten Vorfällen.[141]

---

[138] DSB (2019), *Analyser av krisescenarioer 2019*, S. 36, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 31.08.2021.

[139] Standard Norge, 25.06.2019, *Norsk Standard*, https://www.standard.no/standardisering/norsk-standard/, 23.03.2021.

[140] Standard Norge, 14.09.2020, *Grunnpakke 1-2-3 for cybersikkerhet*, https://www.standard.no/fagomrader/ikt/it-sikkerhet/grunnpakke-1-2-3-for-cybersikkerhet/, 01.09.2021.

[141] Standard Norge, 14.09.2020, *Grunnpakke 1-2-3 for cybersikkerhet*, https://www.standard.no/fagomrader/ikt/it-sikkerhet/grunnpakke-1-2-3-for-cybersikkerhet/, 01.09.2021.

Standardisierung in den Bereichen Elektrotechnik und elektronische Kommunikation

NEK (*Norsk Elektroteknisk Komitee*) ist eine unabhängige Mitgliederorganisation, welche die Arbeit mit Standardisierung im elektrotechnischen Bereich vorantreibt und für die Ausarbeitung und Genehmigung der elektrotechnischen Normen verantwortlich ist. NEK deckt die Fachbereiche für u.a. Alarmsysteme, Cybersicherheit, Telekommunikation, Verteidigung sowie Notfallbereitschaft und Verkehr ab. Das übergeordnete Ziel der Organisation ist es, dort Normen und Standards zu verfassen, wo in der Wirtschaft, der Stromversorgung und im privaten Sektor ein Bedarf für Sicherheit-, Funktions- und Umweltnormen entsteht. NEK ist, gemeinsam mit Standard Norge und der nationalen Kommunikationsbehörde Nkom, ein Teil des norwegischen Standardisierungsapparates.[142]

Qualitätssicherung für Dienstleistungen für den Umgang mit Cyberangriffen

Das NSM hat eine Genehmigungsverfahren für Unternehmen entwickelt, welche Dienstleistungen für den Umgang mit Cyberangriffen anbieten. Dessen Ziel ist es, dass Unternehmen, in denen IT-Sicherheitsvorfälle auftreten, Dienstleister für den Umgang mit diesen Vorfällen wählen können, der die Qualitätsanforderungen für diese Dienste erfüllt. Um eine solche Genehmigung zu erhalten, müssen Anbieter dem offenen Markt entsprechende Dienstleistungen anbieten.[143] Zum aktuellen Zeitpunkt gibt es in Norwegen fünf Unternehmen, welche die Anforderungen des NSM erfüllen, dies sind Defendable AS, mnemonic AS, Atea AS, Netsecurity AS und Sopra Steria.

IT-Sicherheit bei öffentlichen Ausschreibungen

Im November 2019 hat die norwegische Regierung einen Leitfaden zur Sicherheit bei öffentlichen Ausschreibungen veröffentlicht. Dieser stellt Zusammenhänge zwischen dem Sicherheitsgesetz und dem Regelwerk für öffentliche Beschaffungen her und gibt Hinweise, welche Sicherheitskriterien der öffentliche Sektor bei Anschaffungen beachten sollte. Der Leitfaden möchte den Handlungsspielraum im Regelwerk für Beschaffungen verdeutlichen und wie Sicherheitsinteressen bei solchen Prozessen bewahrt werden können. Er beinhaltet daher auch eine Aussage, wie dies auch bei Beschaffungen gewährleistet werden kann, welche nicht unter das Sicherheitsgesetz fallen, wo Sicherheit jedoch dennoch ein zentrales Element darstellt. Ferner enthält das Dokument Informationen zu Risikobewertungen, bevor eine Ausschreibung vorgenommen wird und wie Auftraggeber bei solchen Bewertungen vorgehen können.[144]

[142] Norsk Elektroteknisk Komite (NEK), o. J., *Kort om NEK*, https://www.nek.no/om-nek/kort-om-nek/, 18.10.2021.

[143] NSM, 17.06.2020, *Kvalitetsordning for leverandører som håndterer IKT-hendelser*, https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/handtering-av-dataangrep/kvalitetsordning-for-leverandorer-som-handterer-ikt-hendelser, 10.09.2021.

[144] Regjeringen.no, 21.11.2019, *Større fokus på sikkerhet i anskaffelser*, https://www.regjeringen.no/no/aktuelt/storre-fokus-pa-sikkerhet-i-anskaffelser/id2678449/, 01.09.2021.

5 Markteinstieg und Vertrieb

Dank der norwegischen EWR-Mitgliedschaft steht der norwegische Markt deutschen Unternehmen auf fast ähnliche Weise wie der EU-Markt offen. Für den Export von Waren und Dienstleistungen sowie auch für die Gründung einer Zweigniederlassung oder einer Tochtergesellschaft und für den Erwerb norwegischer Unternehmen gibt es keine rechtlichen Zugangsbeschränkungen. Die Mitglieder der Geschäftsführungsorgane müssen jedoch zur Hälfte aus EWR-Bürgern mit einem EWR-Wohnsitz bestehen.[145]

Waren und Dienstleistungen können entweder direkt oder über eine Zweigniederlassung oder eine Tochtergesellschaft vertrieben werden. Zu beachten ist, dass Zweigniederlassungen ausländischer Unternehmen in Norwegen als eigenständiges Steuersubjekt gelten. Der Vertrieb kann auch über einen Handelsvertreter oder einen Vertragshändler abgewickelt werden. Erstere unterliegen dem Handelsvertretergesetz, welches unter die europäische Handelsvertreterrichtlinie fällt und somit in vielen Teilen dem deutschen Handelsgesetzbuch entspricht.[146]

5.1 Öffentliches Vergabeverfahren und Ausschreibungen

Die Planung und Durchführung von Beschaffungen im öffentlichen Sektor ist durch ein Gesetz vom 17. Juni 2016 Nr. 73 geregelt. Organisationen der öffentlichen Hand müssen demnach einige grundlegende Prinzipien und Anforderungen bei der Planung und Durchführung von Beschaffungen befolgen. Die Durchführung von Einkaufs- und Beschaffungsprozessen im öffentlichen Sektor ist durch das Ausschreibungsgesetz (*Anskaffelsesloven*) geregelt.[147]

Die oben erwähnten rechtlichen Rahmen gelten sowohl für öffentliche Auftraggeber wie staatliche Organe oder Kommunen als auch für Konsortien mit diesen.[148]

Der geschätzte Wert des zu beschaffenden Objekts bzw. der zu beschaffenden Dienstleistung bestimmt, welche Teile des Beschaffungsrecht zur Anwendung kommen. Ab Überschreitung eines definierten Schwellenwertes muss ein Projekt bzw. eine Beschaffungsmaßnahme öffentlich ausgeschrieben werden. Diese Schwellenwerte werden alle zwei Jahre durch die EU-Kommission entsprechend der Währungskursentwicklung angepasst. Entsprechend dieser Änderungen definiert das norwegische Wirtschaftsministerium (*Nærings- og fiskeridepartementet*) neue **EWR-Schwellenwerte** in Norwegen. Die nationalen Schwellenwerte werden ebenfalls entsprechend angepasst. Derzeit (Stand März 2021) liegen die EWR-Schwellenwerte bei

- 1,3 Mio. NOK (ca. 121.000 €) für Güter- und Dienstleistungsbeschaffungen des öffentlichen Sektors 132.000 € (national)
- 2,05 Mio. NOK (ca. 191.000 €) für Güter- und Dienstleistungsbeschaffungen des privaten Sektors
- 51,5 Mio. NOK (ca. 4,8 Mio. €) für Verträge in den Bereichen Bau und Anlagenbau (öffentlicher und privater Sektor)[149]

Ferner gelten für spezifische Dienstleistungserbringungen weitere Schwellenwerte. Öffentliche Ausschreibungen, die über die verpflichtende Vergabe erfolgen, werden sowohl auf dem **nationalen Vergabeportal** www.doffin.no als auch auf dem **europäischen Ausschreibungsportal TED** (*Tenders Electronic Daily*) publiziert. Die Ausschreibungen müssen sowohl auf Norwegisch als auch

[145] IHK Schleswig-Holstein o. J., *Gesetze in Norwegen*, https://www.ihk-schleswig-holstein.de/international/laenderschwerpunkt-norwegen/wirtschaft-handel-steuer-recht-1360472, 22.03.2021.

[146] Ebd.

[147] Anskaffelser.no, 21.02.2021, *Lov og forskrifter om offentlege anskaffingar*, https://www.anskaffelser.no/avtaler-og-regelverk/lov-og-forskrifter, 22.03.2021.

[148] Regjeringen, 24.04.2018, *Veileder til reglene om offentlige anskaffelser (anskaffelsesforskriften)*, https://www.regjeringen.no/no/dokumenter/veileder-offentlige-anskaffelser/id2581234/, 22.03.2021.

[149] Regjeringen, 12.02.2020, *Nye terskelverdier i norske kroner av 12. februar 2020,* https://www.regjeringen.no/contentassets/48242c43007d4e4c95dec5d63b2df498/nye-terskelverdier-av-12-februar-2020.pdf, 23.03.2021

auf einer der offiziellen EU-Sprachen ausgearbeitet werden.[150] Norwegische Auftraggeber veröffentlichen entsprechend dem geltenden Regelwerk Bekanntmachungen und Ausschreibungen. Ausschreibungen, die über dem nationalen Schwellenwert (1,3 Mio. NOK), aber unter dem EWR-Schwellenwert liegen, müssen nur auf der nationalen Ausschreibungsplattform Doffin veröffentlicht werden.[151] Diese Datenbank ist somit durchaus eine wichtige Quelle für Dienstleister und Lieferanten, die nach Aufträgen suchen. Zu beachten bei diesen Ausschreibungen ist jedoch, dass sie meist in norwegischer Sprache veröffentlicht werden und auch die Angebotsabgabe in dieser Sprache erfolgen muss. Im Portal sind die Ausschreibungen nach Branchen sortiert, des Weiteren kann nach Kriterien wie Auftraggeber, Kommune, Ausschreibungstyp oder Datum gesucht werden. Betreiber des Portals ist die staatliche Behörde für öffentliche Verwaltung und Finanzen (*Direktoratet for Forvaltning og Økonomistyring*, DFØ). Die dort veröffentlichten Ausschreibungen sind für fünf Jahre, teilweise auch in englischer Sprache, einsehbar. Die Registrierung auf doffin.no ist kostenlos.[152]

Beschaffungen zwischen 100.000 und 1,3 Mio. NOK unterliegen einem einfacheren Prozess. Hier erhalten die Auftraggeber eine größere Handlungsfreiheit, um die Ausschreibung bedarfsgerecht zu organisieren. Es besteht keine Ausschreibungspflicht, aber die Beschaffung muss gemäß den geltenden Wettbewerbsregeln erfolgen. In solchen Fällen ist es beispielsweise ausreichend, drei potenzielle Lieferanten zu kontaktieren und Angebote von diesen einzuholen.[153]

Die Beschaffung von Objekten und Dienstleistungen unter 100.000 NOK ist vom Beschaffungsregelwerk befreit, sodass die Aufträge direkt vergeben werden können.[154]

5.2 Vertriebswege

Im Bereich des **Schutzes vor Naturereignissen** gibt es nur wenige Privatkunden, hauptsächlich aufgrund der zweigeteilten Ordnung für Erstattung nach Naturschäden, wonach ein Versicherungs- bzw. Erstattungsanspruch durch die staatliche Ordnung oder die Versicherungsgesellschaft besteht. Grundstücksbesitzer sind eigenverantwortlich für ihren Besitz, aber nach dem Gesetz über die Naturschadensversicherung sind Gebäude und Einrichtungen, die gegen Brandschäden versichert sind, auch gegen Naturschäden versichert. Eine Hausratsversicherung deckt also automatisch auch Naturschäden (siehe auch Kapitel 4.2.4). [171]

Wie in Kapitel 3.2.2 beschrieben, ist ein großer Anteil der **kritischen Infrastrukturen** Norwegens im Besitz von privaten Unternehmen oder wird durch diese betrieben, was natürlich eine enge Kooperation zwischen öffentlichen und privaten Akteuren erfordert. Es ist auch eine steigende Tendenz zu erkennen, dass öffentliche Instanzen und Behörden eigens **digitale Dienste** entwickeln, welche im Wettbewerb zum Privatmarkt stehen, und dass diese immer mehr Fachkräfte und Kompetenz im Arbeitsmarkt anziehen. Die Gründung des nationalen Cybersicherheitszentrums hat das Ziel, die Kooperation zwischen den verschiedenen IT-Sicherheitsmilieus zu stärken, sodass verschiedene Akteure mit Blick auf gemeinsame Risiken und dem gleichen Situationsverständnis operieren. Die Gründung des Zentrums ist ein wichtiger Schritt in der Weiterentwicklung der **öffentlich-privaten Kooperation** im Bereich der IT-Sicherheit.

Sowohl die öffentlichen als auch die privaten Eigentümer kritischer Infrastrukturen verschiedener Sektoren sind potenzielle Käufer von **IT-Sicherheitsdiensten** (siehe Kapitel 5.1 zu öffentlichen Ausschreibungen und folgend in diesem Kapitel). Es sollte darauf geachtet werden, dass bei gewissen Ausschreibungen, bei denen der Anbieter Zugang zu Informationen erhält, welche als „vertraulich“ (*KONFIDENSIELT*) oder höher eingestuft werden, der Anbieter eine gültige Deklaration für den angegebenen

[150] Regjeringen, 11.12.2017, *Kunngjøringer*, https://www.regjeringen.no/no/tema/naringsliv/konkurransepolitikk/offentlige-anskaffelser-/andre-kolonne/kunngjoringer/id2522857/, 10.10.2021.

[151] Regjeringen, *Veileder til reglene om offentlige anskaffelser (anskaffelsesforskriften)*, https://www.regjeringen.no/no/dokumenter/veileder-offentlige-anskaffelser/id2581234/sec7, 10.10.2021.

[152] Doffin.no, o. J., *About Doffin*, https://doffin.no/en/Home/About, 22.03.2021.

[153] Samfunnsbedriftene, 06.04.2018, *Terskelverdiene for offentlige anskaffelser er oppjustert*, https://www.samfunnsbedriftene.no/aktuelt/advokattjenester/terskelverdiene-for-offentlige-anskaffelser-er-oppjustert/, 26.03.2021.

[154] Ebd.

Sicherheitsgrad vorweisen können muss. Das gleiche gilt bei Ausschreibungen für Objekte oder Infrastrukturen, die als „kritisch" oder höher eingestuft werden. [172]

Ausländische Akteure, welche den norwegischen Markt überwachen und ggf. Angebote für öffentliche Ausschreibungen einreichen möchten, die über dem nationalen Schwellenwert von 1,3 Mio. NOK (ca. 121.000 €), jedoch unter dem EWR-Schwellenwert liegen, sollten darauf achten, dass diese nur auf der norwegischen Ausschreibungsplattform www.doffin.no ausgeschrieben werden. Da diese meist in norwegischer Sprache veröffentlicht werden und auch die Angebotsabgabe in dieser Sprache erfolgen muss, ist es sinnvoll, die ersten öffentlichen Ausschreibungen gemeinsam mit einem norwegischen Partner zu bewältigen, um so das System besser kennenzulernen. Es gibt auch Anbieter im Markt, wie die Firma Mercell, die eine Reihe exklusiver Ausschreibungen aus z.B. den nordischen Ländern, auch unter dem EU-Schwellenwert, ermittelt. Das Unternehmen bietet u.a. auch Übersetzungsdienste an. Darüber hinaus besteht die Möglichkeit nach Bedarf selbständige Berater im Markt zu engagieren, die Ihr Unternehmen in diesem Prozess begleitet und betreut.

Das Ministerium für Erdöl- und Energie (OED) hat die administrative Verantwortung für **Hochwasser und Erdrutsche.** Die operative Verantwortung wird an die staatliche Behörde NVE delegiert. NVE unterstützt die Kommunen und die Gesellschaft in der Präventionsarbeit für solche Naturereignisse. Sie sind für den nationalen Hochwasserwarndienst, welcher den hydrologischen Zustand in den landesweiten Gewässern überwacht, zuständig, und bewerten die Hochwassergefahr auf lokalem Niveau. [173] Besonders im Bereich der Naturereignisse sind zumeist staatliche Einrichtungen die Auftraggeber. Für die Hochwasser- und Erosionssicherung werden Projekte u.a. von NVE oder den Kommunen ausgeschrieben. Laut NVE gibt es verschiedene Arten, wie solche Sicherungsprojekte ausgeschrieben werden: Die Kommunen können Unterstützung von NVE beantragen, die Ausschreibungen zu formulieren oder zu spezifizieren. In diesem Fall wird nach beratenden Ingenieurunternehmen gesucht, welche den weiteren Prozess mit u.a. Zustandsbeschreibungen und der Auswahl von Lieferanten und Technologien übernehmen. Die Kommunen können auch beantragen, dass NVE die Maßnahme im Auftrag der Kommune durchführt, oder finanzielle Zuschüsse von NVE beantragen – dann führt die Kommune den Rest selbst aus. Die meisten Kommunen haben jedoch keine ausreichende Einkaufskompetenz- Ferner verfügt NVE über ein staatlich finanziertes Budget für Hochwasser- und Erdrutschsicherung – hier basiert sich NVE auf eigene Messungen und wählt kritische Gebiete, welche gesichert werden müssen, selbst aus.[155]

Das **NGI** ist auch ein Beispiel für ein Unternehmen, welches häufig als Totallieferant auftritt und den gesamten Prozess von Vorstudien über Konzeptentwicklung, Design, Produktion, Installation, Datensammlung, -übertragung und Analyse übernimmt. NGI hat sich ein Netzwerk an nationalen und internationalen Unterlieferanten aufgeteilt. Die Projekte variieren stark von größeren Entwicklungs- und Lieferprojekten mit vielen Unterlieferanten bis hin zu Studien, Modelltests und direkten Messaufträgen.

Es kann ein sinnvoller Ansatz sein, sich um die Kooperation mit verschiedenen F&E- oder privaten Akteuren zu bemühen, welche strategisch komplementäre Produkte oder Lösungen anbieten. Die Erfahrungen der Deutsch-Norwegischen Handelskammer und Gespräche mit Branchenexperten verschiedener Sektoren haben gezeigt, dass es viele norwegische Unternehmen präferieren, Lösungen aus dem Ausland über einen lokalen oder skandinavischen Partner zu beziehen. Vorteile eines lokalen Partners sind die direkte Kommunikation mit norwegischen Endkunden in der gleichen Sprache, er kennt häufig die Branche und die relevanten Akteure sehr gut, genießt daher ein gewisses Vertrauen und ist natürlich auch geografisch näher am Kunden. Besonders kleinere Unternehmen empfinden häufig die Zusammenarbeit mit einem norwegischen Partner bzw. Importeur als komfortabler. In größeren Unternehmen gehört in der Regel auch die direkte Zusammenarbeit mit ausländischen Lieferanten zum Tagesgeschäft. Lieferanten aus dem Ausland, die ihre Lösungen auf dem norwegischen Markt vertreiben wollen, sollten sich als Vorbereitung folgende Fragen stellen:

- Wie einfach ist es, mit uns Kontakt aufzunehmen?
- Wie einfach ist es, für fremdsprachlichen Unternehmen mit uns zu kommunizieren?
- Wie einfach ist es, von uns ein Angebot zu erhalten?

[155] Gespräch mit Norges Vassdrags- og Energidirektorat (NVE), Siss-May Edvardsen, Regionsjef Vest, 21.10.2021.

- Wie einfach ist es, von uns beliefert zu werden?
- Wie einfach ist die Inbetriebnahme unserer Lösung?
- Wie einfach ist die Verfügbarkeit von technischem Support und Ersatzteilen?

5.3 Eintrittschancen und Hemmnisse

5.3.1 Schutz vor Naturereignissen

Kapitel 3.1.2 zeigt, dass die bestehenden Hochwassermodelle im Markt sehr allgemein sind, während die norwegische Topographie jedoch sehr komplex ist. Voraussagen für die Zukunft zu treffen ist unter diesen Umständen schwierig, da die Situation zum selben Zeitpunkt z.B. in zwei benachbarten Tälern komplett verschieden sein kann. Zum jetzigen Zeitpunkt gibt es **kein gutes Hochwasserwarnungssystem auf detailliertem Niveau** in Norwegen. Die aktuellen Warnungen beziehen sich häufig auf größere Gebiete. Diese zu verwerten ist schwierig für die lokalen Behörden, welche häufig auch keine ausreichenden Kompetenzen auf diesem Feld besitzen.

Das NGI unterstreicht, dass eine **unzureichende Einkaufskompetenz unter den staatlichen Auftraggebern** eine durchgehende Herausforderung bei Ausschreibungen zum Schutz vor Naturereignissen darstellt. Ein wichtiger Vorteil ist jedoch, dass die norwegischen Auftraggeber in hohem Maße an **forschungsbasierten Lösungen** interessiert sind. Sie sind **sehr offen gegenüber Innovationen** und dafür, neue Ideen im Markt zu testen.[156]

Wie an früherer Stelle in dieser Analyse bereits erwähnt, werden **Satellitendaten** künftig ein wichtiges Werkzeug für die Prävention von Unglücken und Schäden durch Erdrutsche, Felsstürze, Lawinen, Hochwasser und weiteren Naturereignissen sein. Satellitendaten sind besonders bedeutend für die Entwicklung neuer Dienstleistungen und Methoden im Zusammenspiel mit anderen Datenquellen und der innovativen Nutzung von IT. **Maschinelles Lernen, die Aggregation von Satellitendaten in Modellen und die Automation manueller Arbeitsprozesse** sind Fokusbereiche für effektivere Dienstleistungen und Produkte mit höherer Qualität undd einer besseren geographischen und zeitbasierten Abdeckung.[157]

Warnsysteme für potenzielle Quickton-Erdrutsche sind besonders aktuell und nachgefragt, da z.B. der InSAR-Dienst dafür leider nicht genutzt werden kann.

Das NGI hebt auch die Entwicklung und die **wachsende Nutzung naturbasierter Lösungen** als wichtigen Trend in Norwegen hervor, um das Risiko für klimabedingte Naturschäden zu minimieren. Der Hintergrundgedanke hierbei ist, dass die Natur selbst die Idee für Ideen und Lösungen ist, welche flexible Alternativen zu traditionellen Ingenieurslösungen sein können.

Der schnelle Ausbau des 5G-Netzes in Norwegen bringt viele Möglichkeiten, auch im Bereich der Naturereignisse, mit sich. 5G wird die Möglichkeiten der Nutzung von Sensoren für Hochwasserwarnungen oder die Überwachung von Wasserständen oder erdrutschgefährdeten Gebieten deutlich ausweiten. Es wird erwartet, dass 5G kontinuierlich in immer mehr kritische Gesellschaftfunktionen integriert wird.

5.3.2 Digitale Sicherheit: Steigende Nachfrage vor allem durch die Pandemie

IT-Sicherheit war nie zuvor ein aktuelleres Thema. Unternehmen, welche Sicherheitsdienstleistungen, -berater, -infrastruktur und -software anbieten, haben durchgehend ein solides Wachstum durch die gesamte Coronapandemie vermeldet. Mobiles Arbeiten, kombiniert mit einer schnellen Digitalisierung haben zu einem „Cocktail verschiedener Herausforderungen“ für die Sicherheit in der privaten Wirtschaft und im öffentlichen Sektor geführt. Im vergangenen Jahr hat sich die Anzahl digitaler Angriffe vervielfacht,

[156] Gespräch mit NGI, Dominik Lang, Director Natural Hazards, 02.09.2021.

[157] Regjeringen.no (2019-2020), *6.3.2 Overvåking av flom, skred og is*, https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20192020/id2682361/?ch=6, 20.10.2021

somit ist auch der Bedarf für IT-Sicherheit gestiegen. Mehrere Unternehmen konnten ein prozentuales Umsatzwachstum im zweistelligen Bereich verzeichnen. Das Krisenteam des IT-Unternehmens Atea (*Incident Response Team*) hat im vergangenen Jahr besonders die gesteigerten Hacking-Aktivitäten gespürt. Das Team besteht aus 120 Sicherheitsexperten und ist eines von fünf Unternehmen, welches auf die Reaktion auf cyberkriminelle Vorfälle spezialisiert ist und durch die nationale Sicherheitsbehörde (*Nasjonal Sikkerhetsmyndighet*) in diesem Bereich zugelassen ist. So z.B. haben sich die Anfragen an das Krisenteam von Atea verdreifacht. Die Nachfrage nach sog. „Managed Security Services» ist ebenfalls stark gestiegen. Das Krisenteam bietet dann u.a. **virtuelle Überwachungsdienstleistungen, Analyse und Unterstützung, wenn Hacker und Cyberkriminelle auf die Dateninfrastruktur der Kunden zugreifen**. Andere Anbieter, wie Netsecurity und Palo Alto Networks, vermelden auch ein starkes Aktivitäts- und Umsatzwachstum. Palo Alto Networks hat seine Aktivitäten in Norwegen in den vergangenen zwölf Monaten mehr als verdoppelt und erwartet ein weiteres Wachstum (Stand Mai 2021).[158]

Wie in Kapitel 3.2 beschrieben, ist die Ausbreitung des *Internet of Things* (IoT) ein zentraler Faktor in der weiteren Digitalisierung der Gesellschaft. So z.B. hat Oslo Sporveier, Betreiber des Straßenbahnnetzes in der norwegischen Hauptstadt, entschieden, seine alten **Signalanlagen** mit einer Lösung auszurüsten, welche auf das Mobilnetz von Telia zurückgreift (siehe 3.2.3). Außerdem gibt es auch immer mehr **Lösungen, die auf freie Frequenzen basieren.** Als Kommunikationsprotokoll für IoT-Anwendungen wird gern auf LoRaWAN zurückgegriffen. Mittelfristig wird erwartet, dass die verschiedenen IoT-Lösungen in zentrale Teile der Wertschöpfungsketten mehrerer kritischer Funktionen integriert werden.[159] Der Bedarf für **gute Sicherheitslösungen**, welche spezifisch zum Schutz der neuen, komplexeren Netzwerkstrukturen entwickelt werden, wird steigen. Künstliche Intelligenz und maschinelles Lernen werden künftig für die schnellere Aufdeckung verdächtiger Aktivitäten in solchen software-definierten Netzwerken entscheidend sein.

Wie ebenfalls an vorangegangener Stelle in dieser Analyse zitiert, stellt auch der **Fachkräftemangel eine Herausforderung in der Branche dar, da somit der Bedarf des Marktes für IT-Sicherheitsdienstleistungen nicht gedeckt werden kann**. Laut der Branchenverbände Abelia und IKT Norge bauen öffentliche Organisationen ihre IT-Strukturen intern auf und bieten den stark nachgefragten IT-Beratern Bedingungen, mit denen private Akteure kaum mithalten können. Damit verstärkt sich der Fachkräftemangel im privaten Sektor. Somit wird auch die Entwicklung neuer Technologien für den privaten Sektor behindert. Eine Herausforderung dabei ist, dass die IT-Unternehmen in den vergangenen Jahren **in stärkeren Wettbewerb mit öffentlichen Unternehmen und Behörden getreten sind, welche eigene digitale Dienstleistungen entwickeln**. Diese Praxis hemmt laut IKT Norge Vorausschaubarkeit, Innovation und Wachstum bei kleinen, privatwirktschaftlichen Akteuren. [160]

Der neue Leitfaden für IT-Sicherheit im öffentlichen Sektor (siehe Kapitel 4.3.3) bedeutet, dass die öffentliche Hand in höherem Maße professionelle IT-Sicherheitsanbieter nutzen könnte und sollte, um einen Beitrag zur Definition von Sicherheitsanforderungen im Vorfeld von öffentlichen Ausschreibungen zu leisten. Sowohl NSM als auch NorSis haben wiederholt geäußert, dass Unternehmen ohne eigene IT-Sicherheitsabteilung diese Kompetenz extern beschaffen sollten. Daraus ergeben sich sowohl direkte **Möglichkeiten für Anbieter auf dem Feld der IT-Sicherheit** als auch für Lieferanten von Lösungen für den öffentlichen Sektor, welche die **Anforderungen hinsichtlich Sicherheit, GDPR und/oder internen Kompetenzen erfüllen**. [161]

---

[158] Finansavisen, 30.05.2021, *Brennhett marked for IT-sikkerhet*, https://finansavisen.no/nyheter/teknologi/2021/05/30/7681237/brennhett-marked-for-it-sikkerhet?, 20.10.2021.

[159] Nasjonal Kommunikasjonsmyndighet (Nkom) (2020), *EKOMROS 2020: Den digitale grunnmuren satt på prøve,* S. 24, https://issuu.com/nasjonalkommunikasjonsmyndighet/docs/ekomros_2020?fr=sZTZjZDE1Mjg1NjA, 13.10.2021.

[160] IKT Norge, o. J., *Offentlig utvikling av tjenester*, https://www.ikt-norge.no/tema/offentlig-utvikling-av-tjenester/, 10.09.2021.

[161] Computerworld, 25.09.2020, Slik ivaretar du it-sikkerheten i offentlige anskaffelser, https://www.cw.no/artikkel/debatt/slik-ivaretar-du-it-sikkerheten-offentlige-anskaffelser, 09.09.2021.

Führende Akteure in der IT-Branche heben hervor, dass es, bevor es den Sicherheitsleitfaden gab, die **Verantwortlichkeiten**, in welchen Abteilungen der öffentlichen Institutionen die Entscheidungen getroffen werden und welche Argumente bei Beschaffungen im Hinblick auf IT-Sicherheit am schwersten gewichtet werden, **ungeklärt blieben.**

Dies liegt vor allem daran, dass die IT-Abteilungen Zeit investiert haben und Lösungen getestet haben, um die optimalsten Lösungen für ihre eigenen Infrastrukturen zu finden, dennoch aber zumeist die **Einkaufsabteilungen die letztlichen Entscheidungen treffen und Anbieter mit dem niedrigsten Preis** wählen. Wie oben beschrieben, wird erwartet, dass der neue Leitfaden diesen Trend etwas umkehren kann, dennoch ist das starke Preisbewusstsein, welches das Qualitätsbewusstsein dominiert, ein reales Hemmnis für professionelle und sicherheitsorientierte Anbieter bei öffentlichen Ausschreibungen.[162] Ein Gespräch mit der Branchenorganisation Abelia bestätigt diese Problematik, sowie die fehlende Einkaufskompetenz der Fachverantwortlichen.[163]

Neben dem niedrigen Investitionswillen hebt IKT Norge auch hervor, dass sowohl im öffentlichen als auch im privaten Sektor das **fehlende Wissen und die fehlende Bereitschaft, dem Thema Sicherheit einen ausreichenden Fokus einzuräumen**, ein durchgängiges Problem ist. Der Verband unterstreicht, dass eine genügende Sicherheit, kontinuierliche Follow-ups, Bereitschafts- und Backup-Pläne sowie die Sicherheitskultur in der Unternehmensführung, Entscheidungsprozessen und Betrieb eine Prämisse sind, Prozesse erfolgreich zu digitalisieren.[164]

Neue Anbieter im Markt für **Dienstleistungen im Umgang mit Angriffen auf die IT-Sicherheit**, kann die Qualitätsordnung des NSM eine Barriere darstellen, norwegische Kunden zu erreichen. Das Ziel dieser Ordnung ist, dass Unternehmen, welche IT-Sicherheitsvorfällen ausgesetzt sind, einen Dienstleister wählen können sollen, der den Qualitätskriterien des NSM entspricht.[165] Nur sehr wenige Unternehmen erfüllen diese Kriterien und die Qualifikationen zu erfüllen, erfordert Investitionen in zeitliche und personelle Investitionen. Bisher erfüllen die fünf Unternehmen Defendable AS, mnemonic AS, Atea AS, Netsecurity AS und Sopra Steria diese Anforderungen (siehe Kapitel 4.3.5).

5.4 Handlungsempfehlungen für einen Markteinstieg

Generell ist Unternehmen, die erste Aktivitäten auf dem norwegischen Markt planen, zu empfehlen, **die Strukturen des norwegischen Marktes kennenzulernen und sich mit den lokalen Verhältnissen auseinander zu setzen.** In diesem Zusammenhang kann ein lokaler Partner ein Vorteil sein, der mit den kulturellen, sprachlichen und möglichst auch branchenspezifischen Besonderheiten vertraut ist und potenzielle Risiken kennt. Das Vertrauen potenzieller Endkunden kann oft schneller erlangt werden, wenn das ausländische Unternehmen bereits über einen lokalen Ansprechpartner verfügt.

Darüber hinaus sollte sich jedes Unternehmen mit den marktypischen **Standards und Normen** auseinandersetzen. Norwegische Kunden, die Produkte von ausländischen Lieferanten beziehen, setzen in der Regel voraus, dass diese an die Bedürfnisse und gesetzlichen und branchentypischen Anforderungen im Zielmarkt angepasst sind. Es ist wichtig, die relevanten Akteure und deren **Einkaufsstrukturen** und **Vertriebswege** in den einzelnen Sektoren genau zu recherchieren.

Eine **Konkurrenzanalyse** ist unabdingbar, um eventuelle Wettbewerber und Marktführer zu identifizieren und um ihre Marktmacht beurteilen zu können. Auch wenn der Markt grundsätzlich sehr offen gegenüber neuen Technologien aus dem Ausland ist, sind eventuell bereits vertretene Anbieter natürlich sehr wachsam gegenüber neuem Wettbewerb. Bei Fragen zu diesen Themen steht die die für den Markteintritt verantwortliche Abteilung der AHK Norwegen gern zur Verfügung.

---

[162] Computerworld, 25.09.2020, Slik ivaretar du it-sikkerheten i offentlige anskaffelser, https://www.cw.no/artikkel/debatt/slik-ivaretar-du-it-sikkerheten-offentlige-anskaffelser, 09.09.2021.

[163] Gespräch mit Abelia, Kjetil Thorvik Brun, Leiter Technologie und Digitalisierung, 17.09.2021.

[164] IKT Norge, o. J., *Sikkerhet og beredskap*, https://www.ikt-norge.no/tema/sikkerhet-og-beredskap/, 10.09.2021.

[165] NSM, 17.06.2020, *Kvalitetsordning for leverandører som håndterer IKT-hendelser*, https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/handtering-av-dataangrep/kvalitetsordning-for-leverandorer-som-handterer-ikt-hendelser, 10.09.2021.

Bei der Teilnahme an Ausschreibungen norwegischer Auftraggeber sollten Lieferanten darauf achten, dass sie die angegebenen **Ausschreibungskriterien zu 100 % erfüllen**. Nicht zu unterschätzen ist außerdem die Tatsache, dass die Erfahrungen und die Kompetenz einzelner Schlüsselpersonen eines Lieferanten oftmals in der Bewertung des Angebots höher in die Gewichtung eingehen als die Kompetenz und die Referenzen des gesamten Unternehmens. Außerdem sollte aus den Angebotsunterlagen hervorgehen, wie das Risiko verteilt ist. Norwegische Auftraggeber bzw. Einkäufer weisen auch häufig darauf hin, dass es unbedingt notwendig ist, die Ausschreibungsunterlagen genau zu studieren, um ein vollständiges Verständnis über den Umfang der ausgeschriebenen Leistung zu erlangen. Die Auftraggeber schätzen **eine gesunde und seriöse Vertragspartnerschaft**. Aus dem Angebotspreis sollten, als Resultat des vollständigen Verständnisses des Auftragsumfangs, transparente und angemessene Profite hervorgehen. Darüber hinaus wird hervorgehoben, dass Anbieter deutlich zeigen sollen, dass sie in der Lage sind, die angebotene Leistung auszuführen, z. B. durch die Darstellung von Organisations- und Ressourcenplänen.

Unternehmen, die im Rahmen von Bau- oder Installationsaufträgen in Norwegen tätig werden, müssen sich unbedingt mit den **rechtlichen und steuerlichen Rahmenbedingungen** vertraut machen (siehe Kapitel 4). Diese weichen teilweise von den üblichen EU-Modellen ab und können bei Nichteinhaltung unnötigen bürokratischen Aufwand erfordern. Nicht selten ist auch der norwegische Auftraggeber nicht komplett über all diese Pflichten informiert. Das Team der Abteilungen Recht & Steuern sowie Fiskal & Personal der AHK Norwegen unterstützt hier gern.

5.5 SWOT- Analyse

Untenstehend werden verschiedene unternehmensbeeinflussende, externe Faktoren in einer SWOT-Analyse zusammengefasst. Hierbei liegt der Fokus auf landesspezifische Indikatoren sowie allgemeingültige Bedarfe und Trends auf dem Markt, jedoch nicht auf konkret nachgefragte Lösungen und Technologien.

Abbildung 6: SWOT-Analyse - Interne und externe Faktoren des norwegischen Marktes für zivile Sicherheitstechnologien

Strengths (Stärken)	Weaknesses (Schwächen)
• Politische und wirtschaftliche Stabilität • Flache Organisationsstrukturen und Hierarchien • Gute digitale Infrastruktur. Fortschrittlicher Ausbau von 5G • Hohes digitales Kompetenzniveau • Starker Fokus auf Public-Private-Partnerships • Hohe Offenheit für Innovationen und neue Ideen im Markt (gilt in dieser Analyse insbesondere für Naturereignisse) • Enge Verknüpfung vom privaten Sektor, Bildungsinstitutionen und Forschung	• Norwegen kein EU-Mitglied • Bisher sehr allgemeine Hochwassermodelle, während Topographie sehr komplex ist. • Eingeschränkte Einkäuferkompetenz bei zuständigen Akteuren (wie z.B. Kommunen) • Mangel an qualifiziertem Fachpersonal, sowohl im Bereich der Naturereignisse als auch IT • Nahezu jegliche elektronische Kommunikation ist von der Infrastruktur von Telenor abhängig • Hohe Abhängigkeit von elektrischem Strom in allen Lebens- und Gesellschaftsbereichen als potenzielle Anfälligkeit • Teilweise unklare Abgrenzung der Verantwortlichkeiten, in welchen Abteilungen der öffentlichen Organisationen Einkaufsentscheidungen getroffen werden.

Opportunities (Chancen)	Threats (Risiken)
• Verstärkter Einsatz gegen Schäden durch Hochwasser und Erdrutsche durch höheres Gefahrenniveau • Der Markt bietet keine ausreichend guten Warnsysteme für potenzielle Quickton-Erdrutsche • Steigende Nachfrage durch zunehmende, zielgerichtete Cyberangriffe auf norwegische Behörden und Unternehmen • Nachfrage nach neuen Dienstleistungen: 5G-Netz führt zu höherem Risiko für verschiedene digitale Bedrohungen • 5G: Neue Möglichkeiten für Sicherheitstechnologien im Bereich der Naturereignisse • Gute Chancen für innovative Lösungen im Bereich IT-Security – norwegische private Unternehmen nicht besonders stark in Forschung und Entwicklung • Steigende Nutzung von IoT-Anwendungen und Lösungen, die auf freien Frequenzen basieren, z.B. LoRaWAN • Bewilligingen zur Stärkung der Kapazitäten im Notfall-Kommunikationsnetz *Nødnett*	• Niedriger Investitionswille im Bereich der IT-Sicherheit • Behörden/Organisationen der öffentlichen Hand entwickeln eigene digitale Dienstleistungen • Teilweise starker Fokus auf Kosten vor Qualität bei Ausschreibungen, oft aufgrund von fehlender Kompetenz und unklar verteilten Rollen in öffentlichen Einrichtungen • Hohe Forschungs- und Entwicklungsintensität in öffentlichen Organisationen • Herausfordernd, als Lieferant von Dienstleistungen für den Umgang mit Cyberangriffen die Anforderungen der nationalen Sicherheitsbehörde (NSM) zu erfüllen.

Quelle: AHK Norwegen/Eigene Darstellung

6 Profile zentraler Marktakteure

6.1 Ministerien und Behörden

Unternehmen	Kurzprofil	Kontaktdaten
Justizministerium (Justis- og beredskapsdepartementet, JD) Postboks 8005 Dep 0030 Oslo	• Koordinierung der digitalen Sicherheit im zivilen Sektor und allgemeine Verantwortung für die Koordinierung der zivilen Sicherheit der Gesellschaft • Administrative Verantwortung für das Gesetz zur nationalen Sicherheit (Sikkerheitsloven)	www.regjeringen.no/no/dep/jd/id463/ postmottak@jd.dep.no
Öl- und Energieministerium (*Olje- og energidepartementet,* OED)	• Verantwortung für das Regelwerk zur Nutzung der Wasserressourcen • Übergeordnete Verantwortung für die staatlichen Verwaltungsaufgaben zur Vorbeugung von Hochwasserschäden und Lawinen- oder Erdrutschkatastrophen	www.regjeringen.no/no/dep/oed/id750/ postmottak@oed.dep.no
Staatliche Behörde für zivile Sicherheit und Bereitschaft (*Direktoratet for samfunnssikkerhet og beredskap,* DSB)	• Behält Übersicht über Risiko und Anfälligkeit in der Gesellschaft und treibt die Prävention von Krisen, Katastrophen und anderen unerwünschten Ereignissen voran • Stellt Bereitschaftskräfte zur Verfügung, effektives Katastrophen- und Krisenmanagement • Leiter der Zivilverteidigung	www.dsb.no postmottak@dsb.no

	• Nationale Brandschutzbehörde sowie verantwortliche Behörde für Elektro-, Chemikalien und Produktsicherheit	
	• Systemverantwortung für das Kommunikationsnetz der öffentlichen Sicherheit (*Nødnett*)	
Staatliche Behörde für Wasserläufe und Energie (Norges vassdrags- og energidirektoratet, NVE)	• Operative Verantwortung für die Vorbeugung von Schäden durch Überschwemmungen und Erdrutsche	www.nve.no nve@nve.no
	• Beinhaltet u.a. die Vermittlung von Kompetenz und Ressourcen zur Untersuchung, Flächenplanung, Sicherung, Überwachung und Warnung sowie Unterstützung bei Ereignissen	
	• 24/7-Bereitschaftstelefon	
	• Verantwortlich für den nationalen Hochwasserwarndienst (in Zusammenarbeit mit dem MET und der Straßenbaubehörde *Statens Vegvesen*)	
	• Nationaler Hochwasser- und Lawinenwarndienst warnt auf regionalem Niveau – lokale Akteure überwachen die jeweiligen Areale. In Krisensituationen (bei Hochwasser und Erdrutschen) sind mehrere Bereitschaftsbehörden involviert, u.a. die Kommunen, die Polizei oder die Zivilverteidigung	
Norwegisches Institut für geologische Untersuchungen (*Norges Geologiske Undersøkelse*, NGU)	• Untersuchung der norwegischen Geologie zum Nutzen von Wirtschaftsentwicklung, Verkehr, ziviler Sicherheit, Umweltfragen sowie der Flächen- und Naturverwaltung	www.ngu.no ngu@ngu.no
	• Führt Arbeiten u.a. im Auftrag von NVE bei Felsrutschen aus	
Nationale Sicherheitsbehörde (*Nasjonal Sikkerhetsmyndighet*, NSM)	• Expertenorgan für Informations- und Objektsicherheit	www.nsm.no postmottak@nsm.no
	• Nationales Expertenumfeld für digitale Sicherheit	
	• Warn- und Koordinationsinstanz für Cyberangriffe gegenüber der systemkritischen Infrastruktur und anderen wichtigen gesellschaftlichen Funktionen	
	• Betreibt die nationale Gegenwehrfunktion für Cyberangriffe gegenüber kritischen Infrastrukturen (NorCERT) und das nationale Warnsystem für digitale Infrastruktur	
	• Leitet die Arbeit im Koordinationsgremium *Felles Cyberkoordineringssenter*, NCSC)	
	• Geleitet vom NSM	

Nationales Zentrum für Cyber Security (*Nasjonalt cybersikkerhetssenter*, NCSC)	• Nationale Abwehrinstanz für ernsthafte digitale Angriffe • Betreibt das nationale Warnsystem für die digitale Infrastruktur • Knotenpunkt für nationale und internationale Kooperation mit Detektion, Management, Analyse und Beratung von bzw. zu digitalen Angriffen • Fördert intersektorale Zusammenarbeit und zwischen zentralen Dienstleistern, IT-Dienstleistern und Interessenorganisationen im Bereich der digitalen Sicherheit	https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/ ncsc@nsm.no
Nationale Kommunikationsbehörde (*Nasjonal kommunikasjonsmyndighet*, Nkom)	• Sicherheit im Telekommunikationsnetz und für Telekommunikationsdienstleistungen	www.nkom.no firmapost@nkom.no
Nationale Behörde für Digitalisierung (*Digitaliseringsdirektoratet, Digdir*)	• Staatliches Expertenumfeld für IT-Sicherheit • Setzt sich für gestärkte und ganzheitlichere Ansätze im Bereich der IT-Sicherheit in der staatlichen Verwaltung ein	www.digdir.no postmottak@digdir.no

6.2 Verbände, Cluster und Netzwerke

Unternehmen	Kurzprofil	Kontaktdaten
Abelia Postboks 5490, Majorstuen N-0305 Oslo	Landesweiter Verband für Kompetenz- und Technologieunternehmen. Organisiert ca. 2.500 Unternehmen aus den Bereichen IKT, Telekommunikation, Lehre, Forschung, Beratung/Consulting, Kreativwirtschaft und ideellen Organisationen. Eigenes Forum für digitale Sicherheit.	www.abelia.no post@abelia.no
IKT-Norge Oscars gate 20 0352 Oslo	Unabhängige Interessens- und Mitgliederorganisation. Ziel: Stärkung der Rahmenbedingungen für die Digitalwirtschaft.	www.ikt-norge.no post@ikt-norge.no
NCE Finance Innovation Media City Bergen (T2/F11) Lars Hilles Gate 30 5008 Bergen	FinTech-Cluster (Non-Profit) mit ca. 80 Mitgliedern.	https://financeinnovation.no/ info@financeinnovation.no
Nasjonalt cybersikkerhetssenter (NCSC) (Nationales Zentrum für Cybersicherheit)	Kooperation aus 40 öffentlichen und privaten Unternehmen und Organisationen. Knotenpunkt für nationale und internationale Kooperation mit Detektion, Management, Analyse und Beratung von bzw. zu digitalen Angriffen.	https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/ ncsc@nsm.no

Næringslivets Sikkerhetsråd (NSR) **(Sicherheitsrat der Wirtschaft)** Middelthunsgt 27 0368 Oslo	Eine Mitgliedsorganisation, die Unternehmen hilft, die Beratung und Unterstützung in Bezug auf Industriespionage, Sabotage, Drogen, Diebstahl, Terrorismus, organisierte Kriminalität, Betrug, Erpressung, Korruption, Computerkriminalität und mehr benötigen.	www.nsr-org.no post@nsr-org.no
Den Norske Dataforening (DND) x **(Norwegischer IT-Verband)** Rebel Universitetsgata 2 0164 Oslo	Norwegens größtes Netzwerk für IT- und Digitalisierungsfachkräfte.	www.dataforeningen.no kontakt@dataforeningen.no
Norsk Informasjonssikkerhetsforum (ISF) **(Norwegisches Informationssicherheitsforum)** Postboks 250 St. Olavs plass 0164 Oslo	Ideelle Organisation, welche sich für die IT-Sicherheit ihrer Mitglieder einsetzt.	www.isf.no service@isf.no
Nettverket naturfareforum **(Forum/Netzwerk für Naturgefahren)**	Das Branchennetzwerk wurde gegründet, um die Kooperation zwischen nationalen, regionalen und lokalen Akteuren zu stärken, um die Anfälligkeit gegenüber unerwünschten Naturereignissen zu reduzieren.	https://naturfareforum.com/
Forsvars- og sikkerhetsindustriens forening **(Verband der Verteidigungs- und Sicherheitsindustrie)** Postboks 5250 Majorstuen 0303 Oslo	Unabhängige und selbstständige Interessensorganisation für Industrie-, Zulieferer- und Kompetenzunternehmen mit Geschäftsinteressen hinsichtlich Produkten und Dienstleistungen für Sicherheit, Verteidigung und Notfallbereitschaft auf nationalen und internationalen Märkten.	www.fsi.no fsi@nho.no
Nasjonal rassikringsgruppe **(Nationale Gruppe zur Erdrutschsicherung)** Postboks 701 9815 Vadsø	Ziel: Erdrutschsicherung auf die politische Tagesordnung setzen und die öffentlichen Mittel für Maßnahmen zur Erdrutschsicherung erhöhen.	www.nasjonalrassikringsgruppe.no
Finans Norge Postboks 2473 0202 Oslo	Hauptorganisation der norwegischen Finanzwirtschaft. Vertritt ca. 240 Unternehmen.	www.finansnorge.no Firmapost@finansnorge.no

6.3 Forschung und Entwicklung

Eine detailliertere Übersicht über Akteure im Bereich Forschung und Entwicklung für zivile Sicherheitstechnologien kann Anhang 4 entnommen werden.

6.3.1 Natur und Klima

Unternehmen	Kurzprofil	Kontaktdaten

NGI: Norwegian Geotechnical Institute P.O. Box. 3930 Ullevål Stadion N-0806 Oslo	NGI ist ein unabhängiges internationales Zentrum für angewandte Forschung und Beratung in dem Bereich der ingenieurwissenschaftlichen Geowissenschaften. Das Zentrum beschäftigt geotechnische, geologische und geophysikalische Experten.	www.ngi.no ngi@ngi.no
Nina: Norwegian Institute for Nature Research P.O. Box 5685 Torgarden 7485 Trondheim	NINA erforscht seit mehreren Jahrzehnten die Auswirkungen des Klimawandels auf alle Arten in der Natur – vom Hochgebirge bis zum Meeresboden und von der Arktis bis zur Antarktis.	www.nina.no firmapost@nina.no
NORCE: Norwegian Research Centre AS Postboks 22 Nygårdstangen 5838 Bergen	NORCE spielt eine führende Rolle im Bereich Klimaanpassung. Mit der "Seasonal Forecasting Engine" entwickeln sie saisonale Vorhersagen für den öffentlichen und privaten Sektor. Diese Informationen sind für viele Branchen relevant (u.a. Stromlieferanten, Versicherungen und Landwirtschaft). Sie sind zudem Experten im Bereich der avansierten Klimamodellierung.	www.norceresearch.no post@norceresearch.no
SINTEF AS Postboks 4760 Torgarden 7465 TRONDHEIM	SINTEF ist Norwegens größtes Forschungsinstitut für Energie- und Klimatechnologie.	www.sintef.no

6.3.2 Digitale Sicherheit

Unternehmen	Kurzprofil	Kontaktdaten
Big Data Research Group by Western Norway Research Institute Vestlandsforsking Postboks 163 NO-6851 Sogndal	Forschung im Bereich Big Data und Emerging Technologies, einschließlich Blockchain, künstlicher Intelligenz und IoT. Das Ziel ist es Probleme von regionaler, nationaler und globaler Bedeutung im Bereich Notfallmanagement, kritische Infrastrukturen, Verkehr und Mobilität, Energie, eGovernment und Cybersicherheit zu lösen.	www.bigdata.vestforsk.no rak@vestforsk.no
CIEM: Centre for Integrated Emergency Management CIEM University of Agder Post Box 422 NO-4604 Kristiansand	Multidisziplinäres Forschungszentrum an der Universität Agder, Norwegen. Das Zentrum beschäftigt sich damit wie technologische Innovationen der Notfallvorsorge und das Notfallmanagement verbessern können. Die Forschung findet u.a. in den Bereichen Cyber Security, resiliente Gemeinschaften, Situationsbewusstsein, Social Media Analytics, humanitäre Logistik, Augmented Reality und Sensortechnologien statt.	https://ciem.uia.no/

FFI: Norwegian Defence Research Establishment Postboks 25 2027 Kjeller, Norway	Die eigene Forschungseinrichtung des Verteidigungssektors. Das FFI forscht bereits seit langer Zeit im Bereich der Cyber Security. Die Projekte umfassen das gesamte Spektrum: von der Prävention über die Erkennung bis hin zum Incident Management.	www.ffi.no firmapost@ffi.no
NORCICS: Norwegian Centre for Cybersecurity in Critical Sectors	Das forschungsbasierte Innovationszentrum (SFI) NORCICS ist an der Norwegischen Universität für Wissenschaft und Technologie (NTNU) angesiedelt und bindet Forschungs- und Industriepartner aus dem öffentlichen und privaten Sektor ein. Die Vision von NORCICS besteht darin, Norwegen zum sichersten digitalisierten Land der Welt zu machen, indem es die Cyber Security und Widerstandsfähigkeit seiner kritischen Sektoren verbessert und forschungsbasierte Innovationen unterstützt.	www.ntnu.edu/norcics/contact
NTNU CCIS: Center for Cyber and Information Security	Nationales Zentrum für Forschung, Bildung, Tests, Training und Kompetenzentwicklung im Bereich Cyber- und Information Security an der NTNU Gjøvik und NTNU Trondheim. NTNU CCIS hat eine öffentlich-private, zivil-militärische und internationale Partnerschaft mit mehr als 40 nationalen und internationalen Partnern. Derzeit sind am CCIS 120 Forscher und rund 800 NTNU-Studenten.	www.ntnu.edu/ccis/ post@ccis.no
NUPI's Centre for Digitalization and Cyber Security Studies PB 7024 St. Olavs Plass 0130 OSLO	Arbeitet mit Forschungsprojekten zu politischen und gesellschaftlichen Aspekten im Cyberspace. In den verschiedenen Forschungsprojekten geht u.a. um globale Herausforderungen in Bezug auf das Managen des Cyberspace, Macht und Abhängigkeit, digitale Kriegsführung und die Nutzung digitaler Technologien zur Einflussnahme.	www.nupi.no/en/About-NUPI/Projects-centers/NUPI-s-Centre-for-Digitalization-and-Cyber-Security-Studies post@nupi.no
Simula UiB Thormøhlens gate 53D N-5006 Bergen	Ein Forschungszentrum, welches zu dem Simula Research Laboratory und der Universität Bergen gehört. Fokusiert sich auf das Erlangen von Wissen im Bereich der Sicherung der ICT-Infrastruktur.	https://simula-uib.com/

6.4 Messen und Fachveranstaltungen

Titel der Veranstaltung	Kurzprofil	Kontaktdaten

Digitalkonferansen 2021	Kristiansand, 11.11.2021. Fachkonferenz, deckt u.a. die Themen Systementwicklung, Coding und künstliche Intelligenz ab.	www.digitalkonferansen.no post@digin.no
Interpraevent	Internationale Konferenz zum Umgang mit Naturgefahren. Treffpunkt für Forscher und Verwaltungsakteure in diesem Bereich.	www.interpraevent2020.no interpraevent@gyro.no
NorSIS-konferansen 2021	Oslo, 23.-24. November 2021 Konferenz zu Sicherheitskultur, Gefahren im Internet und der neuen Gefährdungslage durch Cyberkriminalität.	https://norsis.no/norsis-konferansen-2021/
PARANOIA 2021 Langkaia 1 0150 Oslo	Oslo, 18.-19. November 2021. Führende Cyber-Security-Konferenz in den nordischen Ländern, viele internationale Akteure beteiligt.	www.paranoia.watchcom.no/ paranoia@watchcom.no
Posisjonskonferansen	Kartverket, Norsk Romsenter und Nkom veranstalten diese Fachkonferenz. Thema: Nutzung globaler Satellitennavigationssysteme. arrangerer fagkonferansen som omhandler bruk av globale satellittnavigasjonssystemer.	www.nkom.no/aktuelt/invitasjon-til-posisjonskonferansen-om-gnss-sarbarheter firmapost@nkom.no
Sikkerhetskonferansen	Größte Veranstaltung im Bereich der präventiven Sicherheit in Norwegen.	https://nsm.no/kurs-og-konferanser/sikkerhetskonferansen/2021/
Totalforsvarets Cybersikkerhetskonferanse	Zielgruppe: Akteure aus öffentlichen Instanzen, Wissenschaft und der Privatwirtschaft, welche im Bereich der Cyber- und Informationssicherheit in der zivilen und militärischen Verteidigung arbeiten.	www.cyberkonf.no

6.5 Fachmedien

Unternehmen	Kurzprofil	Kontaktdaten
Aktuell Sikkerhet P.b. 130 N-2261 Kirkenær	Fachzeitschrift und Onlineportal zu Sicherheitsrisiken und -bedarfen, informiert zu Sicherheitslösungen in der Privatwirtschaft und im öffentlichen Sektor.	www.aktuellsikkerhet.no redaksjonen@aktuellsikkerhet.no
Brann & Sikkerhet Pb 6754 Etterstad 0609 Oslo	Norwegens älteste Zeitschrift zu Brandschutz und Sicherheit.	https://brannvernforeningen.no/brann-og-sikkerhet/ post@brannvernforeningen.no
Computerworld PB 171, Sentrum 0102 Oslo	Landesweit einizge Fachzeitschrift für den norwegischen IT-Sektor. Erscheint seit 1983 zehn Mal jährlich.	www.cw.no cw@cw.no
Geo365.no GeoPublishing AS Trollkleiva 23 1389 Heggedal	News und Wissen zu geowissenschaftlichen Themen mit besonderer Relevanz für die norwegische Wirtschaft und Gesellschaft.	https://geo365.no/ ingvild@geonova.no

Kommunalteknikk Norsk Kommunalteknisk Forening C/O Spaces Tollbugata 8A 0152 Oslo	Fachzeitschrift des kommunaltechnischen Verbands Norwegens mit dem Ziel, als vermittelnder Kanal zwischen Kommunen, Behörden, Expertenmilieus, Organisationen und der Wirtschaft fungieren.	www.kommunalteknikk.no/utgivelser-i-pdf.76800.no.html
Samferdsel & Infrastruktur Value Publishing AS Kristian Augusts gate 12, 0164 Oslo	Größtes norwegisches Fachmagazin für den Verkehrs- und Infrastruktursektor.	www.samferdselinfra.no redaksjon@samferdselinfro.no
Teknisk Ukeblad Media AS Grensen 3 0158 Oslo	Erscheint wöchentlich; Fokus auf Technologie und Technologieunternehmen. Deckt folgende Themenbereiche ab: Energie, Schifffahrt, Bauwesen, Industrie, Gesundheit, Elektroautos, Flugverkehr und Transport.	www.tu.no nettdesk@tu.no

7 Quellenverzeichnis

7.1 Telefoninterviews mit Branchenexperten

Gespräch mit NGI, Dominik Lang, Director Natural Hazards, 02.09.2021.

Gespräch mit Abelia, Mikal Kvamsdal, wirtschaftspolitischer Sprecher Technologie und Digitalisierung, 17.09.2021.

Gespräch mit Abelia, Kjetil Thorvik Brun, Leiter Technologie und Digitalisierung, 17.09.2021.

Gespräch mit Norwegian Center for Cybersecurity in Critical Sectors, Prof. Sokratis K. Katsikas, Director, 01.02.2020.

Gespräch mit Norges Vassdrags- og Energidirektorat (NVE), Siss-May Edvardsen, Regionsjef Vest, 21.10.2021.

7.2 Schriftliche Quellen

Abelia, 11.01.2016, *Sikkerhet*, https://www.abelia.no/bransjer/teknologi-og-digitalisering/sikkerhet/, 09.09.2021.

Alt om samfunnssikkerhet, 09.03.2021, *Sikkerhet i Neste Generasjon Nødnett*, https://www.altomsamfunnssikkerhet.no/samfunnssikkerhet-og-beredskap/sikkerhet-i-neste-generasjon-nodnett/, 30.08.2021.

Anskaffelser.no, 21.02.2021, *Lov og forskrifter om offentlege anskaffingar*, https://www.anskaffelser.no/avtaler-og-regelverk/lov-og-forskrifter, 22.03.2021.

Atea, 25.02.2021, *Når kompetanse, vekst og sikkerhetsmarkedet går hånd i hånd,* https://www.atea.no/siste-nytt/kompetanse-vekst-og-sikkerhetsmarkedet/, 18.10.2021.

Auswärtiges Amt, *Norwegen: Wirtschaft*, 03.06.2019, https://www.auswaertiges-amt.de/de/aussenpolitik/laender/norwegen-node/-/205866, 12.04.2019.

Cautos Geo AS, o. J., *Om oss*, https://cautusgeo.com/om-oss/, 13.09.2021.

CIA WorldFactbook, 2019, *NORWAY*, S. 1, https://www.cia.gov/the-world-factbook/static/0ae463d06343fbf4c546ca0393f2ef19/NO-summary.pdf, 09.03.2021.

Computerworld, 05.03.2020, *Hvor bekymret bør vi være for 5G-sikkerheten?*, https://www.cw.no/artikkel/debatt/hvor-bekymret-bor-vi-vaere-5g-sikkerheten, 31.08.2021.

Computerworld, 25.09.2020, Slik ivaretar du it-sikkerheten i offentlige anskaffelser, https://www.cw.no/artikkel/debatt/slik-ivaretar-du-it-sikkerheten-offentlige-anskaffelser, 09.09.2021.

Departementene (2019), *Nasjonal strategi for digital sikkerhet*, S. 15, https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf, 23.08.2021.

Departementene (2019), Tiltaksoversikt til nasjonal strategi for digital sikkerhet, S. 9-10, https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt--nasjonal-strategi-for-digital-sikkerhet.pdf, 11.10.2021.

Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning (2015), *NOU Digital sårbarhet – sikkert samfunn*, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf, 23.08.2021.

Doffin.no, o. J., *About Doffin*, https://doffin.no/en/Home/About, 22.03.2021.

DSB (2021), *DSB årsrapport 2020*, https://www.dsb.no/globalassets/dokumenter/rapporter/dsbs-arsrapport-2020.pdf, 19.08.2021.

DSB (2021), *Analyser av krisescenarioer 2019*, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, 19.08.2021.

E24.no, 14.08.2021, *Bedriftene står i kø for IT-ekspertise: – Udekket behov som bare øker,* https://e24.no/naeringsliv/i/Ep6yoa/bedriftene-staar-i-koe-for-it-ekspertise-udekket-behov-som-bare-oeker, 15.10.2021.

Energifakta Norge, 20.08.2021, *Energibruken i ulike sektorer*, https://energifaktanorge.no/norsk-energibruk/energibruken-i-ulike-sektorer/. 23.08.2021.

FFI (2020), *Samfunnssikkerhet mot 2030*, https://publications.ffi.no/nb/item/asset/dspace:6641/20-00530.pdf, 31.08.2021.

Finans Norge, o. J., *Naturskadeforsikring*, https://www.finansnorge.no/tema/skadeforsikring/naturskadeforsikring/, 13.09.2021.

Finansavisen, 30.05.2021, *Brennhett marked for IT-sikkerhet*, https://finansavisen.no/nyheter/teknologi/2021/05/30/7681237/brennhett-marked-for-it-sikkerhet?, 20.10.2021.

flomrespons.no, o. J., *Fremtidens lokale verktøy for flomvarsling*, https://www.flomrespons.no/, 13.10.2021.

Forskning.no, 10.09.2019, *Hva skjer med resten av Mannen nå?*, https://forskning.no/geologi/hva-skjer-med-resten-av-mannen-na/1560028, 20.08.2021.

Forskning.no, 04.03.2021, *Hva er egentlig 5G?*, https://forskning.no/internett-mobiltelefon/hva-er-egentlig-5g/1813874, 30.08.2021.

Gemini.no, 02.03.2021, *Vi trenger flere eksperter på skred og flom*, https://gemini.no/2021/03/vi-trenger-flere-eksperter-pa-skred-og-flom/, 19.10.2021.

Germany Trade & Invest, 18.01.2021, *Unsicherheit drückt Investitionslust*, https://www.gtai.de/gtai-de/trade/specials/special/norwegen/unsicherheit-drueckt-investitionslust-236502, 11.03.2021.

IHK Schleswig-Holstein o. J., *Gesetze in Norwegen*, https://www.ihk-schleswig-holstein.de/international/laenderschwerpunkt-norwegen/wirtschaft-handel-steuer-recht-1360472, 22.03.2021.

IKT Norge, o. J., FinTech, https://www.ikt-norge.no/tema/fintech/, 09.09.2021.

IKT Norge, o. J., *Offentlig utvikling av tjenester*, https://www.ikt-norge.no/tema/offentlig-utvikling-av-tjenester/, 10.09.2021.

IKT Norge, o. J., *Sikkerhet og beredskap*, https://www.ikt-norge.no/tema/sikkerhet-og-beredskap/, 10.09.2021.

Justis- og Beredskapsdepartementet, *Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden*, https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf, 19.08.2021.

Mediaplanet, 27.09.2021, *Alt om samfunnssikkerhet: Setter Norge på kartet som verdensledende på digitalisering og digital sikkerhet*, https://www.altomsamfunnssikkerhet.no/samfunnssikkerhet-og-beredskap/setter-norge-pa-kartet-som-verdensledende-pa-digitalisering-og-digital-sikkerhet/, 14.10.2021.

Menon Economics, NINA & SWECO (2017), *Naturbaserte løsninger for klimatilpasning*, https://www.miljodirektoratet.no/globalassets/publikasjoner/m830/m830.pdf, 13.09.2021.

Nasjonal Kommunikasjonsmyndighet, o. J., *Om Nkom,* https://www.nkom.no/om-nkom, 13.10.2021.

Nasjonal Kommunikasjonsmyndighet (2020), *EKOMROS 2020: Den digitale grunnmuren satt på prøve,* S. 19, https://issuu.com/nasjonalkommunikasjonsmyndighet/docs/ekomros_2020?fr=sZTZjZDE1Mjg1NjA, 13.10.2021.

Nasjonal Kommunikasjonsmyndighet, o. J., *Håndtering av cyberhendelser - Nkom EkomCERT*, https://www.nkom.no/sikkerhet-og-beredskap/nkom-ekomcert, 13.10.2021.

NGI, o. J., *Kvikkleireskred i Norge*, https://www.ngi.no/Tjenester/Fagekspertise/Kvikkleireskred/Kvikkleireskred-i-Norge, 20.08.2021

NGI, *Digital Services,* https://www.ngi.no/eng/Services/Technical-expertise/Digital-services, 12.10.2021.

Norges Bank, 09.03.2021, *Valutakurser*, https://www.norges-bank.no/tema/Statistikk/Valutakurser/?tab=currency&id=EUR, 09.03.2021.

Norges Geologiske Undersøkelse (NGU), 10.10.2018, *INSAR Norge*, https://www.ngu.no/emne/insar-norge, 20.10.2021.

Norsk Elektroteknisk Komite (NEK), o. J., *Kort om NEK*, https://www.nek.no/om-nek/kort-om-nek/, 18.10.2021.

Norsk Industri, 02.01.2021, *Brexit-avtale på plass – hva betyr dette for Norge og Norsk Industri?*, 11.03.2021.

Norsk Petroleum, 25.03.2021, *Eksport av olje og gas*, http://www.norskpetroleum.no/produksjon-og-eksport/eksport-av-olje-og-gass/, 07.04.2019.

NRK, o. J., *Leirskredet i Gjerdrum*, https://www.nrk.no/nyheter/leirskredet-i-gjerdrum-1.15307406, 20.08.2021

NRK, 13.06.2021, *Får mer nøyaktig flomvarsel: – Da kan vi forberede oss*, https://www.nrk.no/sorlandet/flomvarslingssystem-basert-pa-kunstig-intelligens-skal-gi-mer-presis-varsling-1.15511293, 15.09.2021.

NSM, 17.06.2020, *Kvalitetsordning for leverandører som håndterer IKT-hendelser*, https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/handtering-av-dataangrep/kvalitetsordning-for-leverandorer-som-handterer-ikt-hendelser, 10.09.2021.

Nodnett.no, o. J., *Hva er Nødnett?*, https://www.nodnett.no/om-nodnett/hva-er-nodnett/, 14.10.2021.

NTB, 15.12.2020, *Yr-appen er prisvinner*, https://kommunikasjon.ntb.no/pressemelding/yr-appen-er-prisvinner?publisherId=17846853&releaseId=17897837, 10.09.2021.

NTB, 06.09.2021, *Yr får betre nedbørvarsel*, https://kommunikasjon.ntb.no/pressemelding/yr-far-betre-nedborvarsel?publisherId=17846853&releaseId=17915030, 10.09.2021.

NSM, o. J., *Rammeverk for håndtering av IKT-hendelser*, https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/, 31.08.2021.

NTNU, o. J., *Norwegian Cyber Range*, https://www.ntnu.no/ncr, 11.10.2021.

NVE, o. J., *Kvikkleireskredet i Gjerdrum*, https://www.nve.no/naturfare/laer-om-naturfare/om-skred/kva-er-kvikkleire-og-kvikkleireskred/kvikkleireskredet-i-gjerdrum/, 26.08.2021.

PHUSICOS, o. J., *Solutions to reduce risk in mountain landscapes*, https://phusicos.eu/, 13.09.2021.

Regjeringen, 04.05.2018, *Gas exports from the Norwegian shelf*, https://www.regjeringen.no/en/topics/energy/oil-and-gas/Gas-exports-from-the-Norwegian-shelf/id766092/, 07.04.2019.

Regjeringen, 08.07.2021, *Undertegnet historisk frihandelsavtale med Storbritannia*, https://www.regjeringen.no/no/aktuelt/undertegnet-historisk-frihandelsavtale-med-storbritannia/id2866032/, 11.10.2021.

Regjeringen, 13.06.2019, *Die Deutschland-Strategie der norwegischen Regierung 2019,* https://www.regjeringen.no/en/dokumenter/deutschland_strategi/id2654427/, 11.03.2021.

Regjeringen, 10.06.2021, *Norge er elektrisk*, https://www.regjeringen.no/no/tema/transport-og-kommunikasjon/veg_og_vegtrafikk/faktaartikler-vei-og-ts/norge-er-elektrisk/id2677481/, 23.08.2021.

Regjeringen, *Prop. 100 S (2010–2011) Fullføring av utbygging og drift av Nødnett i hele Fastlands-Norge,* https://www.regjeringen.no/no/dokumenter/prop-100-s-20102011/id640914/?ch=5, 14.10.2021.

Regjeringen, 14.01.2021, *Naturfarer – hvem har ansvar for at nordmenn bor trygt?*, https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/oed/nyheter/2021/naturfarer-hvem-har-ansvar-for-at-nordmenn-bor-trygt/id2828628/, 15.10.2021.

Regjeringen, 16.10.2020, *Vår digitale sikkerhet styrkes*, https://www.regjeringen.no/no/aktuelt/var-digitale-sikkerhet-styrkes/id2771497/, 26.08.2021.

Regjeringen, 07.10.2019, *Statsbudsjettet 2020. Sikrere og mer effektiv kommunikasjon*, https://www.regjeringen.no/no/aktuelt/sikrere-og-mer-effektiv-kommunikasjon/id2672558/, 26.08.2020.

Regjeringen, (2019-2020), *6.3.2 Overvåking av flom, skred og is*, https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20192020/id2682361/?ch=6, 20.10.2021.

Regjeringen, 28.09.2018, *Statlige planretningslinjer for klima- og energiplanlegging og klimatilpasning*, https://www.regjeringen.no/no/dokumenter/statlige-planretningslinjer-for-klima--og-energiplanlegging-og-klimatilpasning/id2612821/, 31.08.2021.

Regjeringen, 19.04.2021, *NIS2-direktivet*, https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/, 31.08.2021.

Regjeringen, 03.12.2019, *Cybersikkerhetsforordningen*, https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2017/nov/cybersecurity-act/id2590048/, 31.08.2021.

Regjeringen, 21.11.2019, *Større fokus på sikkerhet i anskaffelser*, https://www.regjeringen.no/no/aktuelt/storre-fokus-pa-sikkerhet-i-anskaffelser/id2678449/, 01.09.2021.

Regjeringen, 24.04.2018, *Veileder til reglene om offentlige anskaffelser (anskaffelsesforskriften)*, https://www.regjeringen.no/no/dokumenter/veileder-offentlige-anskaffelser/id2581234/, 22.03.2021.

Regjeringen, 12.02.2020, *Nye terskelverdier i norske kroner av 12. februar 2020,* https://www.regjeringen.no/contentassets/48242c43007d4e4c95dec5d63b2df498/nye-terskelverdier-av-12-februar-2020.pdf, 23.03.2021

Regjeringen, 11.12.2017, *Kunngjøringer*, https://www.regjeringen.no/no/tema/naringsliv/konkurransepolitikk/offentlige-anskaffelser-/andre-kolonne/kunngjoringer/id2522857/, 10.10.2021.

Regjeringen (2019-2020), *6.3.2 Overvåking av flom, skred og is*, https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20192020/id2682361/?ch=6, 20.10.2021

Samferdsel & Infrastruktur, 19.01.2021, *Flomvarsling: digital verktøy for bedre beredskap,* https://www.samferdselinfra.no/flomvarsling-digitalt-verktoy-for-bedre-beredskap/, 13.10.2021.

Samfunnsbedriftene, 06.04.2018, *Terskelverdiene for offentlige anskaffelser er oppjustert*, https://www.samfunnsbedriftene.no/aktuelt/advokattjenester/terskelverdiene-for-offentlige-anskaffelser-er-oppjustert/, 26.03.2021.

SFI Norwegian Centre for Cybersecurity in Critical Sectors (2020), *SFI NORCICS Annual Report 2020*, https://www.ntnu.edu/documents/1294734959/1300988649/SFI+NORCICS+Annual+Report+2020.pdf/c2189003-5079-9646-4d3b-8dbc1c4a063c?t=1624015907570, 15.10.2021.

SSB, 23.02.2021, *Befolkning*, https://www.ssb.no/folkemengde, 09.03.2021.

SSB, 18.12.2018, *Befolkning*, https://www.ssb.no/befolkning/statistikker/folkemengde/aar-berekna, 09.03.2021
SSB, 09.03.2021, *Befolkning*, tabell 01222, https://www.ssb.no/statbank/table/01222, 09.03.2021.
SSB, 07.07.2021, *Nasjonalregnskap*, https://www.ssb.no/nasjonalregnskap-og-konjunkturer/nasjonalregnskap/statistikk/nasjonalregnskap, 22.07.2021
SSB, 04.06.2021, *Konjunkturtendensene,* https://www.ssb.no/nasjonalregnskap-og-konjunkturer/konjunkturer/statistikk/konjunkturtendensene, 22.07.2021
SSB, 27.01.2021, *Utenrikshandel med varer*, https://www.ssb.no/utenriksokonomi/statistikker/muh/aar, 10.03.2021.
SSB, 15.01.2021, *Handelsoverskuddet nesten utradert i 2020,* https://www.ssb.no/utenriksokonomi/artikler-og-publikasjoner/handelsoverskuddet-nesten-utradert-i-2020, 10.03.2021.
SSB, o. J., *Utenrikshandel med varer*, *tabell* 08809, https://www.ssb.no/statbank/table/08809/, 11.03.2021.
SSB, 20.01.2021, *Størst økning i utenlandske investeringer i eiendom og industri,* https://www.ssb.no/utenriksokonomi/artikler-og-publikasjoner/storst-okning-i-utenlandske-investeringer-i-eiendom-og-industri, 11.03.2021.

Standard Norge, 25.06.2019, *Norsk Standard*, https://www.standard.no/standardisering/norsk-standard/, 23.03.2021.
Standard Norge, 14.09.2020, *Grunnpakke 1-2-3 for cybersikkerhet*, https://www.standard.no/fagomrader/ikt/it-sikkerhet/grunnpakke-1-2-3-for-cybersikkerhet/, 01.09.2021.

Tu.no, 13.08.2021, *Norsk flomsikringstartup sikter mot Europa*, https://www.tu.no/artikler/norsk-flomsikringstartup-sikter-mot-europa/512412?utm_source=newsletter-tudaily&utm_medium=email&utm_campaign=newsletter-2021-08-14&key=gSOhW0ZF, 13.09.2021.
Tu.no, 08.11.2020, *Sensorteknologi skal verne mot villere vær lokalt*, ¨ https://www.tu.no/artikler/sensorteknologi-skal-verne-mot-villere-vaer-lokalt/501912, 19.10.2021.

www.ixpos.de/markterschliessung

www.bmwi.de