Ein Vergleich aktueller kritischer Infrastrukturansätze

Russische Angriffe auf kritische Infrastrukturen in der Ukraine und andere Krisen in den letzten Jahren haben zu bedeutenden politischen Entwicklungen im Zusammenhang mit kritischen Infrastrukturen innerhalb der EU, der NATO und der Schweiz geführt. Im Umgang mit der herausfordernden Risikolandschaft stehen Resilienz und Kooperation im Fokus, um die Auswirkungen disruptiver Ereignisse abzufedern.

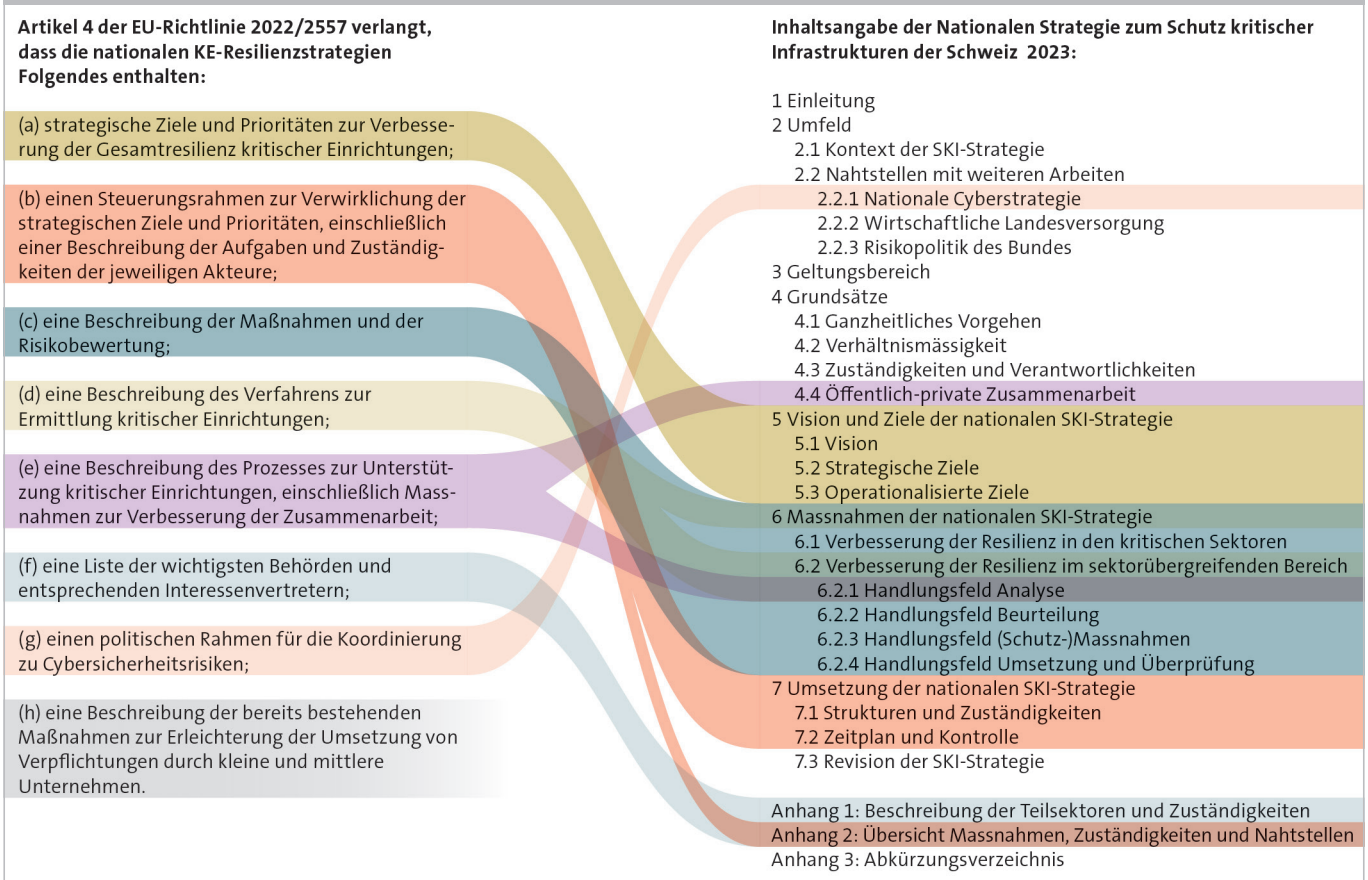
Von Simon Aebi

Russlands Vorgehen in der Ukraine seit 2014 einschliesslich seiner gross angelegten Invasion im Jahr 2022 haben die Bedeutung kritischer Infrastrukturen (KI) und ihrer Verwundbarkeiten aufgezeigt. So hat Russland beispielsweise gezielt Energie- und Kommunikationsinfrastrukturen angegriffen, um durch die Unterbrechung wichtiger Dienstleistungen einen militärischen Vorteil zu erlangen. Gezielte Angriffe auf KI bestehen jedoch bereits unter der Kriegsschwelle und werden oft als «hybride Bedrohungen» bezeichnet. Diese Bedrohungen können unter anderem in Form von Cyberattacken oder Spionage auftreten. Die Sabotage der Nord-Stream-Pipeline in der Ostsee im Jahr 2022 hat beispielsweise die Anfälligkeit der europäischen Energieinfrastruktur aufgezeigt.

Eine Präsentation u.a. der EU-NATO Task Force zur Resilienz kritischer Infrastruktur am 11. Januar 2023. *Johanna Geron / Reuters*

Unter KI versteht man Einrichtungen, Systeme, Netzwerke und Betreiber, die Dienste ermöglichen und bereitstellen, die für das Funktionieren von Regierungen, Volkswirtschaften und Gesellschaften erforderlich sind. Zwar können verschiedene Länder und Organisationen eine leicht voneinander abweichende Definition und Abgrenzung von KI haben, doch begegnet man ihnen im Allgemeinen aus einer sektorbezogenen Perspektive. So unterscheidet man zum Beispiel zwischen Energieinfrastruktur, Kommunikationsdienstleistungen oder Transportnetzen. Die sektorbezogene Betrachtung bietet einen Ansatz um KI zu erkennen, abzugrenzen und zu organisieren. Allerdings kennzeichnen sich die heutigen KI durch starke gegenseitige Abhängigkeiten, die auf die Globalisierung, Urbanisierung, Digitalisierung und einen allgegenwärtigen Cyberraum zurückzuführen sind. Dadurch verschwimmen diese Sektorgrenzen und KI werden noch verwundbarer. Beispielsweise hängen moderne Energieinfrastrukturen von Telekommunikationsnetzen ab und umgekehrt. Potenzielle Störungen von KI sind jedoch nicht nur auf absichtliche Bedrohungen zurückzuführen, sondern können das Ergebnis unterschiedlicher Gefahren sein. Dazu zählen unter anderem Naturgefahren und geophysikalische Ereignisse wie Überschwemmungen oder Erdbeben sowie Zwischenfälle, die durch technisches Versagen und menschliches Handeln verursacht werden. So hat beispielsweise die Entgleisung eines Güterzugs im Gotthard-Tunnel im August 2023 die Folgen einer Störung innerhalb

Überschneidungen zwischen den EU-Anforderungen an nationale CER-Strategien und der SKI-Strategie der Schweiz



Quelle: EU-Richtlinie 2022/2557 und Schweizer Strategie zum Schutz kritischer Infrastrukturen 2023 (angepasst durch Autor)

des Schweizer Güterschienennetzes aufgezeigt. Darüber hinaus hatte die Liberalisierung von KI im Westen – vor allem in den 1990er Jahren – zur Folge, dass häufig private Akteure Besitzer oder Betreiber von KI sind. Das kann die Regierungsaufsicht, die Kontrolle und die Vereinheitlichung von Sicherheitsmassnahmen erschweren, wenn diese kostenoptimierten Geschäftsmodellen gegenüberstehen.

Die kontinuierliche Verschlechterung der internationalen Sicherheitslage hat in zunehmendem Masse die Bedeutung von KI und ihres Schutzes innerhalb der westlichen Länder und Institutionen erhöht. Der Zusatzbericht zum Sicherheitspolitischen Bericht der Schweiz 2021, der 2022 veröffentlicht wurde, unterstrich die Überprüfung und Anpassung seiner Strategien in Bezug auf Resilienz und Kooperation beim Schutz kritischer Infrastrukturen, um auf künftige Herausforderungen vorbereitet zu sein. Ausserdem zeigt der Bericht auf, dass eine verstärkte internationale Zusammenarbeit, insbesondere mit der NATO und der EU, neue Möglichkeiten zur Stärkung des Bevölkerungsschutzes schaffen könnte. Das wiederum schliesst die Bereiche der KI und Resilienz mit ein. Folglich bieten Überlegungen zu den jüngsten Veränderungen innerhalb der NATO und der EU sowie über das derzeitige Verständnis der Resilienz von KI wertvolle Anhaltspunkte für mögliche oder bestehende Zusammenarbeit. Die Überprüfung der aktualisierten nationalen Strategie zum Schutz kritischer Infrastrukturen der Schweiz bietet eine Chance, Überschneidungen und Abweichungen in den Überlegungen zur Resilienz von KI zwischen der Schweiz, der EU und der NATO festzustellen.

Vom Schutz zur Resilienz

Die Resilienz von KI hat sich aus Schutzkonzepten für KI entwickelt und stellt einen Paradigmenwechsel in den letzten Jahrzehnten dar. Der Schutz von KI entwickelte sich zu einem grundlegenden Konzept in der Sicherheitspolitik und beschrieb den angemessenen Schutz von KI vor Naturgefahren, technologischen Problemen, vom Menschen verursachten Unfällen und vorsätzlichen Angriffen während der Nachkriegsära und in der Zeit des Kalten Kriegs. Häufig verfolgten solche Schutzkonzepte einen All-Gefahren-Ansatz (engl. All-Hazards Approach) und versuchten, alle möglichen Gefährdungen und Bedrohungen für KI zu kennen und zu entschärfen. Jedoch hat der All-Gefahren-Ansatz seine Grenzen, da es unrealistisch und in manchen Fällen ökonomisch ineffizient wäre, alle Gefahrenquellen zu ermitteln und sich gegen sie zu schützen.

Im Vergleich dazu hat die Resilienz von KI den Fokus hin zum Erkennen und Reduzieren der Vulnerabilitäten von KI verlagert. Entsprechend sind resiliente KI in der Lage, Disruptionen zu verhindern, auszuhalten und sich davon zu erholen. Idealerweise stellen sie dabei den kontinuierlichen Betrieb bei Zwischenfällen und Krisen sicher. Des Weiteren hat der Wechsel vom Schutz hin zur Resilienz von KI auch den Fokus von einem überwiegend physischen Verständnis von KI hin zu einer Sichtweise

gelenkt, die KI als Systeme und Netzwerke erkennt, welche essenzielle Dienstleistungen erbringen. Heute konzentrieren sich die Schweiz, die EU und die NATO in ihrer Haltung zur Sicherheit von KI auf Resilienz.

NATO

Als zwischenstaatliche Allianz, die zur gemeinsamen Verteidigung gegründet wurde, konzentriert sich die NATO in erster Linie auf gegenseitige Sicherheit und die Zusammenarbeit zwischen ihren Mitgliedsstaaten. Die langjährigen Ziele der NATO – Abschreckung und Verteidigung, Krisenprävention und kooperative Sicherheit – wurden im Laufe der Zeit immer stärker verbunden mit der zivilen Bereitschaft und der nationalen Resilienz ihrer Mitgliedstaaten. So einigten sich die Mitgliedstaaten auf dem NATO-Gipfel 2016 in Warschau auf sieben grundlegende Anforderungen für Resilienz. Dazu zählen unter anderem robuste Regierungsfunktionen, Energieversorgung, Kommunikationssysteme und Transportinfrastrukturen.

Da 21 der NATO-Mitgliedstaaten auch Teil der EU sind, wurde im Januar 2023 die EU-NATO-Taskforce zur Resilienz kritischer Infrastruktur eingerichtet. Der Fokus der Taskforce liegt auf der Verbesserung der institutionsübergreifenden Resilienz in den Bereichen Transport, Energie, digitale Infrastruktur und Weltraum durch verstärkte Zusammenarbeit, das Teilen von Informationen und Frühwarnsysteme. Ihr abschliessender Bewertungsbericht, der im Juni 2023 veröffentlicht wurde, gibt 14 Empfehlungen, die dazu beitragen sollen, die Ansätze der EU und der NATO für die Resilienz von KI anzugleichen. Da man die hohe Vernetzung von KI erkannt hat, umfassen die Empfehlungen die Entwicklung schneller Reaktionen gegen Bedrohungen auf höchster politischer Ebene, die Durchführung regelmässiger Risiko- und Bedrohungsanalysen, die Einbindung der Resilienzthematik in Übungen und die Förderung des strategischen Engagements der Bündnispartner, Mitgliedstaaten und dem privaten Sektor.

Europäische Union

Im Dezember 2022 ersetzte die Europäische Kommission ihre Richtlinie zu KI aus dem Jahr 2008 durch ihre neue «Richtlinie über die Resilienz kritischer Einrichtungen» (CER). Mit der CER-Richtlinie hat die beachtenswerte Terminologie der «kritischen Einrichtungen» (KE) die Bezeichnung KI ersetzt. Zusammen mit der ergänzenden, nicht abschliessenden Liste wesentlicher Dienste, die 2023 veröffentlicht wurde, fokussiert sich die CER-Richtlinie mehr auf die Betreiber von KI und deren Dienstleistungen als auf die allgemeinen KI-Sektoren. Die CER-Richtlinie spiegelt die Bemühungen der EU wider, die Resilienz der KE und ihrer Dienste als wesentliche Elemente für die Sicherheit und Verteidigung, den EU-Binnenmarkt und die Existenzgrundlage der EU-Bevölkerung zu stärken. Hierfür ist eine Harmonisierung der nationalen sektorübergreifenden Vorschriften erforderlich. Daher macht die Richtlinie den EU-Mitgliedstaaten Vorgaben, die letztendlich zu einer stärkeren Regulierung für KE führen werden.

Der relativ enge Zeitrahmen, der den EU-Mitgliedstaaten bleibt, um diese Richtlinie einzuführen und umzusetzen, macht deutlich, wie dringlich diese Angelegenheit ist. Vor dem Hintergrund der Verschlechterung der internationalen Sicherheitslandschaft unterstreicht die CER-Richtlinie auch die Anfälligkeit der KE gegenüber hybriden Bedrohungen. Zusätzlich hebt die Richtlinie die Bedeutung und Risiken des digitalen und des Cyberraums hervor und impliziert, dass KE über die rein physischen Eigenschaften hinausgehen. Abschliessend schreibt die CER-Richtlinie Massnahmen vor, um die Resilienz der KE zu stärken. Dazu zählen die Entwicklung nationaler Strategien, regelmässige Risikobewertungen, Notfallplanungen, die Berichterstattung in Ereignisfällen sowie unterstützende Massnahmen seitens der Behörden. Darüber hinaus müssen die Zusammenarbeit und der Austausch von Informationen zwischen den Staaten, Behörden und KE koordiniert werden.

> Heutige KI kennzeichnen sich durch starke gegenseitige Abhängigkeiten.

Schweiz

Im Juni 2023 veröffentlichte der Bundesrat die dritte Ausgabe der Nationalen Strategie zum Schutz kritischer Infrastrukturen der Schweiz. Ziel der Strategie ist es, alle relevanten Akteure von der Bundesebene bis hin zur Kantonsebene und dem privaten Sektor in Einklang zu bringen, indem sie übergreifende Ziele und Grundsätze definiert. Obwohl der Titel «Schutz kritischer Infrastrukturen» lautet, folgt die Strategie – einschliesslich ihrer Vorgängerversion aus 2017 – dem Konzept der Resilienz von KI. So lautet die Vision: «Die Schweiz ist in Bezug auf kritische Infrastrukturen resilient, sodass grossflächige und schwerwiegende Ausfälle möglichst verhindert werden beziehungsweise im Ereignisfall das Schadensausmass möglichst gering gehalten wird.» Um dieses Ziel zu erreichen, schlägt die Strategie acht Massnahmen – darunter sieben sektorübergreifende – vor, um die Resilienz zu stärken und die Zusammenarbeit zwischen den verschiedenen Ebenen, Sektoren und Bereichen der Akteure zu fördern.

Unterschiede bei Mandat und Ebene

Ein Vergleich der nationalen Strategie zum Schutz kritischer Infrastrukturen (SKI) der Schweiz mit den Empfehlungen der NATO als internationale Verteidigungsallianz und der verbindlichen Regelung der EU für Mitgliedstaaten ist in Anbetracht der unterschiedlichen Ebenen der Gouvernanz, Durchsetzung und Mandate sicherlich schwierig. Jedoch erlaubt es Differenzen und Gemeinsamkeiten zu erkennen und trägt zu einem umfassenderen Bild der Positionen und Prioritäten dieser Institutionen bei. Erstens: Die Konzeption der NATO von Resilienz kann man nur begrenzt mit der SKI-Strategie der Schweiz vergleichen, da sich die grundlegenden Anforderungen der NATO auf die gemeinsamen Verteidigungsfähigkeiten der Allianz fokussieren. Darüber hinaus scheinen die Anforderungen, die im Abschlussbericht der EU-NATO-Taskforce ausgeführt werden, lediglich den KE-Ansatz der EU zu wiederholen – jedoch beschränkt auf die für die Ambitionen der NATO relevanten Bereiche. Dennoch gibt es Gemeinsamkeiten: Auch die SKI-Strategie der Schweiz betont die Bedeutung resilienter Energieversorgungsinfrastrukturen, Lebensmittel- und Wasserressourcen sowie ziviler Kommunikations- und Transportsysteme.

Zweitens: Während die NATO eine resiliente Infrastruktur als einen Faktor versteht, der es Regierungen ermöglicht, zu handeln und zu kommunizieren, hebt die Schweizer Strategie die Rolle von resilienten Behörden hervor, welche KI-Betreiber im Falle disruptiver Ereignisse unterstützen können. Drittens: Während die NATO und die EU die Zusammenarbeit über Landesgrenzen hinweg priorisieren, geht die Schweizer Strategie nur kurz auf grenzüberschreitende Abhängigkeiten von KI ein. Stattdessen zielt sie darauf ab, die Bemühungen im Zusammenhang mit resilienter KI innerhalb der Schweiz zu stärken. Darüber hinaus betont die Rhetorik der NATO und der EU stark die «hybriden Bedrohungen». Im Vergleich dazu ist die

Schweizer Strategie eher vage, was die Definition relevanter Bedrohungen und Risiken angeht, und bezieht sich stattdessen Bewertungen auf nationaler sowie Sektor-, Behörden- und Betreiberebene.

Viertens: Die EU hat eine Sprache übernommen, die einen klaren Wandel vom Schutz der KI hin zur Resilienz der KE sowie deren wesentlichen Dienstleistungen, die sie erbringen, darstellt. Zwar beschreibt die Schweizer Strategie Resilienz und strebt diese an, doch sie verwendet weiterhin die Bezeichnung KI und KI-Betreiber und die Betonung der Dienstleistungen ist weniger dominant als in der CER-Richtlinie. Fünftens: Die CER-Richtlinie ist für Mitgliedstaaten verbindlich und enthält Vorgaben, die von identifizierten KE umgesetzt werden müssen. Im Gegensatz dazu handelt es sich bei der Schweiz um eine nationale Strategie welche Ziele und Lösungsansätze formuliert. Anforderungen und Vorschriften für Schweizer KI-Betreiber entstehen aus spezifischen Gesetzgebungen für die unterschiedlichen Sektoren (Energie, Transport, Finanzen).

Die Zusammenarbeit zwischen allen Akteuren ist von höchster Bedeutung.

Gemeinsames Verständnis

Wie oben beschrieben, gibt es eine Reihe von Unterschieden zwischen den NATO-Empfehlungen, der EU-Richtlinie und der Strategie der Schweiz. Dennoch besteht ein gemeinsames Verständnis über die Bedeutung von KI und ihrer Resilienz. So verfolgt die Schweiz beispielsweise unabhängig Ansätze und Massnahmen für KI-Resilienz, die denen der NATO und der EU entsprechen. Die Kongruenz wird sogar noch deutlicher, wenn man die EU-Anforderungen für Mitgliedstaaten und die Schweizer SKI-Strategie vergleicht. Zum Beispiel fordert Artikel 4 der CER-Richtlinie die EU-Mitglieder auf, eine nationale Strategie zu besitzen. Die Schweiz hat nicht nur seit 2012 eine eigene Strategie, sondern die Elemente, die von der CER-Richtlinie vorgegeben werden, sind auch in der Schweizer Strategie enthalten (siehe Grafik). Die Überlappungen gehen aber über das reine Vorhandensein einer nationalen Strategie hinaus.

Erstens: Die Sektoren, anhand welcher auch essentiellen Dienstleistungen und deren Dienstleister identifiziert werden, weisen grosse Ähnlichkeiten auf. Zweitens: Sowohl die CER-Richtlinie als auch die Schweizer SKI-Strategie fordern die regelmässige Überprüfung und Identifizierung von KE oder KI einschliesslich des Führens eines entsprechenden Inventars. Drittens: Wiederkehrende Risikobewertungen sollten sich auf eine potenzielle Disruption von Dienstleistungen und die wirksamsten Resilienzmassnahmen, die umgesetzt werden können, fokussieren. Viertens: Die CER-Richtline fordert, dass kompetente Behörden für die Umsetzung und Überwachung der nationalen Strategien definiert sein müssen. Deren Aufgabe sollte auch die Unterstützung der relevanten Akteure umfassen. Ausserdem sollte ein zentraler Ansprechpartner für grenzüberschreitende Probleme bezüglich KE definiert werden. Die Schweizer Strategie geht hier ähnlich vor: Sie definiert führende Behörden pro Sektor und erklärt das Bundesamt für Bevölkerungsschutz als koordinierender Ansprechpartner für KI. Fünftens: Grosse Bedeutung wird dem Teilen von Informationen und dem Melden von Zwischenfällen, die die Bereitstellung von Dienstleistungen durch KE oder KI unterbrechen (könnten) beigemessen. Die Zusammenarbeit zwischen allen Akteuren, vor allem in Bezug auf privat-öffentliche Beziehungen, ist von höchster Bedeutung und das Ermöglichen sektorübergreifender Plattformen scheint für dieses Ziel entscheidend zu sein. Zuletzt befürwortet die EU-Richtlinie national-gesetzliche Regulierungen, um die Resilienz zu stärken. Hier sieht die Schweizer SKI-Strategie vor, einen «Vorschlag für eine rechtliche Grundlage für den Erlass von sektorübergreifenden Vorgaben zu prüfen».

Ausblick

Ein gemeinsames Verständnis und ähnliche Prioritäten in Bezug auf KI kann als Ausgangspunkt für eine Vereinfachung und Verbesserung der Zusammenarbeit zwischen der Schweiz, der NATO und der EU dienen, wie im Zusatzbericht zum Sicherheitspolitischen Bericht der Schweiz 2021 beschrieben. Dies kann insbesondere beim Umgang mit grenzüberschreitenden Aufgaben hilfreich sein. Die Schweiz sollte mindestens die KI-relevanten Entwicklungen der NATO und der EU beobachten. Darüber hinaus kann man wertvolle Erkenntnisse aus den Erfahrungen dieser Organisationen gewinnen. So könnte die Schweiz auch von der vorgeschlagenen Empfehlung des EU-Rates für einen Konzeptentwurf für kritische Infrastrukturen zur Verbesserung koordinierter und grenzüberschreitender Reaktionen auf bedeutende Zwischenfälle lernen. Diese Empfehlung wird derzeit im EU-Rat diskutiert. Die Ziele dieses Konzeptes sollten die Stärkung eines gemeinsamen Lagebewusstseins, eine bessere Abstimmung der öffentlichen Kommunikation sowie das Ermöglichen effektiver Reaktionen auf schwerwiegende Zwischenfälle sein.

Für mehr zu Sozio-technischer Resilienz und Katastrophenvorsorge, siehe CSS Themenseite.

Simon Aebi ist Senior Researcher im Team Risiko und Resilienz am Center for Security Studies (CSS) der ETH Zürich.

Die **CSS Analysen zur Sicherheitspolitik** werden herausgegeben vom Center for Security Studies (CSS) der ETH Zürich. Das CSS ist ein Kompetenzzentrum für schweizerische und internationale Sicherheitspolitik. Jeden Monat erscheinen zwei Analysen auf Deutsch, Französisch und Englisch.

Herausgeberin: Névine Schepers
Lektorat: Simon Aebi
Layout und Grafiken: Miriam Dahinden-Ganzoni

Feedback und Kommentare: analysen@sipo.gess.ethz.ch
Weitere Ausgaben und Abonnement: www.css.ethz.ch/cssanalysen

ISSN: 2296-0236; DOI: 10.3929/ethz-b-000671523