Nr. 297, Februar 2022

# Nationale Ansätze zum Schutz vor Ransomware

Regierungen entwickeln derzeit verschiedene Strategien zum Schutz gegen die wachsende Bedrohung durch *Ransomware*. Nur wenige Länder haben bislang einen ganzheitlichen Ansatz formuliert. Eine politische Richtlinie, die sich ausdrücklich mit *Ransomware* befasst, kann die behördenübergreifende Koordination unterstützen und die internationale Kooperation fördern.

Von Nele Achten

*Ransomware*-Angriffe beginnen in der Regel mit der Infiltration eines Computersystems und der Verschlüsselung von Daten mithilfe einer Schadsoftware. *Ransomware* (auch bekannt als «Erpressersoftware») ist eine Software, die von Staaten, politisch motivierten Hackergruppen und sonstigen Kriminellen eingesetzt wird. Das Motiv ist meist finanzieller Natur. Das Opfer wird in diesem Fall nach der Verschlüsselung aufgefordert, Lösegeld *(Ransom)* zu zahlen. Nach getätigter Zahlung wird ein Code zur Entschlüsselung übermittelt, mit dem der Zugriff auf die eigenen Daten wiederhergestellt wird. Mit *Ransomware* können jedoch auch andere Beweggründe rein zerstörerischer oder politischer Art verfolgt werden.

Lösegeldforderungen für zuvor verschlüsselte Daten gibt es bereits seit den 1980ern. Seitdem haben sich *Ransomware*-Gruppen immer professioneller organisiert, und die Anzahl der *Ransomware*-Vorfälle hat im letzten Jahrzehnt stetig zugenommen. In den letzten zwei bis drei Jahren hat sich der Einsatz von *Ransomware* von allein handelnden Personen zu einem System entwickelt, in dem mehrere auf jeweils einzelne Schritte des Angriffs spezialisierte Akteure zusammenarbeiten. Aufgrund dieser Entwicklung und den damit zusammenhängenden wachsenden wirtschaftlichen Folgen der Angriffe müssen politische Lösungen entwickelt werden, die das Problem von *Ransomware* gezielt angehen.


Mitarbeiter des *US Cyber Command* im Fort George G. Meade in Maryland im Oktober 2020.
*Joseph Cole / US Cyber Command*

Die meisten Staaten verfügen bereits über nationale Cybersicherheitsstrategien, die die Verantwortlichkeiten nationaler Behörden in Bezug auf Cyberbedrohungen regeln. Explizite nationale Ansätze gegen *Ransomware* würden jedoch die Koordination zwischen nationalen Akteuren verbessern und auf internationaler Ebene signalisieren, wie Staaten gegen *Ransomware* vorgehen wollen.

## Die Entwicklung von Ransomware

Aufgrund der folgenden drei Faktoren fällt es Strafverfolgungsbehörden schwer, dem Anstieg an *Ransomware*-Vorfällen entgegenzuwirken: Erstens wurde der Einsatz von *Ransomware* durch die wachsende Verbreitung von Kryptowährungen massiv erleichtert. Zwar können Strafverfolgungsbehörden Lösegeldzahlungen in Kryptowährungen bis zu einem gewissen Grad

### Die Bedeutung von Kryptowährungen für Ransomware

**Eine Kryptowährung** ist eine dezentrale digitale Währung, die durch Verschlüsselung gesichert ist. Dies bedeutet, dass sie nicht von einer zentralen Behörde ausgegeben wird und ohne eine vermittelnde Institution zwischen Nutzern übertragen werden kann. Bitcoin, die erste dezentrale Digitalwährung, befindet sich seit 2009 im Umlauf und wurde von einer unbekannten Person oder Gruppe erfunden.

**Alle digitalen Währungstransaktionen sind öffentlich,** da sie in einem dezentral geführten Kontobuch *(distributed ledger)* namens *Blockchain* erfasst werden. Dies ist ein entscheidender Unterschied zum herkömmlichen Bankensystem. Digitale Währungen können somit bis zu einem bestimmten Grad zurückverfolgt werden. Kryptowährungs-Mischdienste (auch *Tumbler* genannt) bieten jedoch an, «schmutzige» Gelder mit anderen zu mischen, wodurch die Rückverfolgung von Geldflüssen erschwert wird.

Vermögen in digitalen Währungen können **nicht mit realen Personen verbunden werden,** sondern sind mit digitalen Währungsadressen verknüpft. Diese Adressen werden benötigt, um das Ziel einer Transaktion in Kryptowährung zu identifizieren. Hierin liegt ein weiterer Unterschied zu physischen Währungen, durch den die Identifizierung von realen Personen hinter digitalem Vermögen stark erschwert wird. Gelingt es einer Behörde dennoch, digitales Vermögen mit illegalen Aktivitäten in Verbindung zu bringen, kann sie dem Unternehmen, welches die digitale Geldbörse führt, die Sperrung des Zugangs auferlegen.

zurückverfolgen – in den meisten Fällen können die Gelder jedoch nicht sichergestellt werden. Eine Sicherstellung der Gelder funktioniert nur, wenn die Behörden Zugriff auf das Passwort des entsprechenden Krypto-*Wallets* erhalten, an das die Zahlung erfolgte.

Zweitens gestaltet sich die Identifizierung einzelner Verdächtiger im Rahmen der Strafermittlungen schwierig (siehe Textbox). Und drittens ist für erfolgreiche Ermittlungen gegen den Einsatz von *Ransomware* grenzüberschreitende Zusammenarbeit erforderlich. *Ransomware*-Aktivitäten werden jedoch nicht in allen Ländern auf dieselbe systematische Art verfolgt.

Einige CybersicherheitsExpertenInnen sind der Ansicht, dass wir uns momentan in einer regelrechten *Ransomware*-Pandemie befinden. In der Tat weisen verschiedene Faktoren auf eine erhebliche Zunahme von *Ransomware* hin, darunter der Anstieg von *Ransomware*-Erkennungen durch automatisierte Software, häufigere Versicherungsfälle und zahlreichere Meldungen von Vorfällen an Behörden. Die steigende Zahl von *Ransomware*-Angriffen ist zum Teil auch auf die sinkenden Kosten für deren Durchführung zurückzuführen. Schadsoftware kann relativ leicht im *Darknet* erworben werden, um damit von einem vorher festgelegten Opfer Lösegeld zu erpressen.

Vor allem aber hat sich das Umfeld, welches *Ransomware*-Angriffe ermöglicht, in den letzten zwei bis drei Jahren deutlich weiterentwickelt. So werden *Ransomware*-Angriffe nicht mehr von einzelnen Personen, sondern von professionell organisierten Gruppen durchgeführt, die die Lösegelder untereinander aufteilen. Innerhalb dieser Gruppierungen sind verschiedene Teams für unterschiedliche Schritte des Angriffs zuständig, wie zum Beispiel das Ausspähen von Zugangsdaten, das Erweitern der Schadsoftware, das Infizieren der Systeme der Erpressungsopfer sowie die Monetarisierung der gestohlenen Daten. Die Aufteilung der Aufgaben ermöglicht eine stärkere Spezialisierung der Beteiligten und fördert die Entwicklung von neuen kreative Erpressungsmethoden.

## Ganzheitliche Ansätze

Nach den jüngsten *Ransomware*-Angriffen auf Gesundheitsunternehmen weltweit und ein US-Ölpipeline-Unternehmen im Mai 2021 wurde die Entwicklung angemessener Massnahmen zur Bekämpfung von *Ransomware* für viele Staaten eine Priorität. Die meisten Regierungen sind sich einig darüber, dass der Schutz vor *Ransomware*-Angriffen ein koordiniertes Vorgehen aller relevanter politischer Akteure erfordert. Die *Anti-Ransomware-Initiative* – ein im Oktober 2021 von der US-Regierung initiierter Zusammenschluss von über 30 Staaten – verdeutlicht dies. Die Initiative stellt einen ganzheitlichen handlungsorientierten internationalen Ansatz gegen Bedrohungen durch *Ransomware* dar. Aus zwei Gründen ist dieses Vorhaben im Vergleich zu anderen internationalen Initiativen im Bereich der Cybersicherheit neu und beachtenswert: Die Initiative schliesst explizit den Privatsektor mit ein und umfasst die internationale Kooperation unterschiedlicher staatlicher Behörden, anstatt sich nur auf diplomatische und militärische Massnahmen zu beschränken.

Die *Anti-Ransomware-Initiative* benennt zudem richtigerweise die verschiedenen staatlichen Behörden, die an der Umsetzung der Massnahmen gegen *Ransomware* beteiligt sind. Unabhängig davon muss jede Regierung für sich selbst entscheiden, ob ihr Militär und ihre Nachrichtendienste eine aktive Rolle bei der Bekämpfung von *Ransomware* spielen sollen – und wenn ja, welche. Diese Entscheidung erfordert eine sorgfältige Beurteilung aller zur Verfügung stehenden Massnahmen. Mögliche Massnahmen reichen von der Abschreckung von *Ransomware*-Angreifen, zur Prävention von *Ransomware*-Vorfällen bis hin zu öffentlichen Empfehlungen, um einen Schaden infolge eines Vorfalles möglichst klein zu halten.

## Eine nationale Sicherheitsbedrohung?

Einige Staaten haben *Ransomware* als Bedrohung ihrer nationalen Sicherheit eingestuft. Entsprechend ist in diesen Ländern auch das Militär an der Bekämpfung von *Ransomware*-Angriffen beteiligt. Dieser nationale Sicherheitsansatz zur Bekämpfung von *Ransomware* beinhaltet den Einsatz von offensiven Cyberaktivitäten gegen bestimmte organisierte *Ransomware*-Gruppen, die besonders schwerwiegende Angriffe zu verantworten haben. Australien, die USA und Kanada haben öffentlich bekanntgemacht, dass ihre Streitkräfte offensive Operationen durchgeführt haben, unter anderem um cyberkriminelle Infrastrukturen im Ausland zu zerstören. General Paul Nakasone, Oberbefehlshaber des *US Cyber Command* und Direktor der *National Security Agency,* bestätigte im Dezember 2021 zum ersten Mal Offensivmassnahmen des US-Militärs gegen *Ransomware*-Gruppen. Die Beteiligung des *US Cyber Command* rechtfertigte der General mit Verweis auf die jüngsten *Ransomware*-Angriffe gegen kritische Infrastrukturen in den USA.

An einer Veranstaltung des in den USA ansässigen *Institute for Technology and Security* erwähnten ExpertenInnen auch geringere Voraussetzungen, die den Einsatz von offensiven Cyberoperationen gegen die hinter *Ransomware* stehenden Akteure bereits rechtfertigen könnten. Dazu gehören der Umfang, die Zunahme und der Schweregrad des Angriffes sowie das Kriterium, ob sich die *Ransomware*-Gruppen physisch in Gebieten aufhalten, wo keine direkte Zusammenarbeit mit den lokalen Strafverfolgungsbehörden besteht.

Regierungen, die einen nationalen Sicherheitsansatz zur Bekämpfung bestimmter Arten von Cyberkriminalität verfolgen, könnten mit den Massnahmen zur Bekämpfung von *Ransomware* anderer Staaten in Konflikt geraten. So können zum Beispiel eingreifende Massnahmen gegen Kriminelle, Krypto-Handelsplattformen und *Ransomware*-Gruppen eines bestimmten Landes mit laufenden Ermittlungen zur Beweismittelbeschaffung eines anderen Landes kollidieren. Die europäischen Regierungen scheinen den Einsatz offensiver Cybermassnahmen gegen Cyberkriminelle durch andere Staaten zu akzeptieren – ihre eigenen Herangehensweisen gegen *Ransomware* müssen sie jedoch erst noch bekanntgeben.

Aus Sicht des internationalen Rechts hängt die Entscheidung, ob, wann und wie offensive Cybermassnahmen gegen *Ransomware* ergriffen werden dürfen, davon ab, welche rechtliche Position das jeweilige Land in Bezug auf das Vorhandensein und den Umfang einer generell rechtlichen Norm der staatlichen Souveränität hat. Staaten, die sich nicht für die Existenz einer generellen rechtlichen Norm der staatlichen Souveränität ausgesprochen haben, besitzen mehr Spielraum bezüglich der Durchführung offensiver Cybermassnahmen. Sobald diese jedoch Infrastrukturen in Drittländern betreffen, hängt die Frage nach der Souveränitätsverletzung auch von der rechtlichen Position des Drittstaates in Bezug auf die Existenz einer generellen rechtlichen Norm der staatlichen Souveränität ab.

Unternehmen, die Opfer von *Ransomware*-Angriffen werden, sind zunehmend bereit, Informationen an die Strafverfolgungsbehörden weiterzugeben.

Wenn der betreffende Drittstaat eine solche rechtliche Norm öffentlich bestätigt hat, wird eine Verletzung dennoch wahrscheinlich nur festgestellt, wenn die offensive Cybermassnahme gegen die von Cyberkriminellen genutzte Infrastruktur eine Mindestschwelle erreicht. Dies könnte beispielsweise der Fall sein, wenn eine offensive Cybermassnahme gegen eine *Ransomware*-Gruppe in einem Drittland durchgeführt wird, in dem die Strafverfolgung selbst über ausreichende Kapazitäten verfügt, um den Server der Gruppe vom Netz zu nehmen.

Schliesslich hängt die Entscheidung für oder gegen den Einsatz offensiver Cybermassnahmen gegen *Ransomware* auch von der Bewertung anderer Vorgehensweisen ab, auf die ein Staat zurückgreifen kann. So stehen einem Staat eine Reihe nicht militärischer Massnahmen zur Verfügung, wie beispielsweise diplomatische Schritte, eine strafrechtliche Verfolgung sowie grenzüberschreitende Massnahmen der Strafverfolgungsbehörden zur Zerstörung krimineller Netzwerke. Diplomatische Schritte reichen von der Ermahnung eines Staates, der *Ransomware*-Gruppen einen sicheren Hafen bietet, bis hin zur Auferlegung von Sanktionen gegen spezifische digitale Geldbörsen oder gegen Kryptobörsen, die Transaktionen ermöglichen, welche mit kriminellen Aktivitäten in Zusammenhang gebracht werden können. Derartige nicht offensive Massnahmen stellen ein geringeres Risiko der Eskalation dar und bieten daher eine vorteilhaftere Grundlage zur Verbesserung grenzüberschreitender Ermittlungen, unter anderem auch mit demjenigen Staat, der beschuldigt wird, Cyberkriminellen einen Unterschlupf zu gewähren.

## Strafrechtliche Verfolgung

Regierungen, die nur durch Strafverfolgung und multilaterale Zusammenarbeit gegen *Ransomware* vorgehen, können verschiedene kriminelle Akteure ins Visier nehmen. So können sich strafrechtliche Ermittlungen gegen *Ransomware*-Gruppen selbst sowie in einigen Rechtsordnungen gegen juristische Personen richten, die *Ransomware*-Aktivitäten ermöglichen. Dazu gehören unter anderem Kryptobörsen, die Geldwäsche ermöglichen.

Kryptobörsen sind Unternehmen, die ihren Kunden den Tausch von Kryptowährungen gegen andere Vermögenswerte wie herkömmliches Geld oder andere digitale Währungen ermöglichen. In einigen Ländern sind diese Unternehmen verpflichtet, die Behörden über verdächtige Aktivitäten zu informieren. Wenn sie dieser Meldepflicht nicht nachkommen und somit finanzielle Transaktionen aus nachweislich illegalen Quellen unterstützen, können sie strafrechtlich haftbar gemacht werden. In der Schweiz sind Kryptobörsen ähnlich wie Banken zusätzlich verpflichtet, die Identität aller Kunden zu kennen, die grössere Transaktionen durchführen.

Ferner müssen Regierungen, die im Kampf gegen *Ransomware* vor allem auf ihre Strafverfolgung setzen, möglichst gute Beziehungen zum Privatsektor entwickeln. Andreas Popow, ein auf *Ransomware* spezialisierter Schweizer Staatsanwalt, führte in einem Interview aus, dass sich die Kooperation mit dem Privatsektor in den letzten Jahren gewandelt hat und gereift ist. Unternehmen, die Opfer von *Ransomware*-Angriffen werden, sind zunehmend bereit, Informationen an die Strafverfolgungsbehörden weiterzugeben. Darüber hinaus werden *Ransomware*-Opfer immer häufiger von spezialisierten Anbietern für den Schutz gegen Cybersicherheitsvorfälle unterstützt, sodass die Strafverfolgung digitale Beweise im direkten Austausch mit diesen Unternehmen sichern kann. Für die Strafverfolgungsbehörden bedeutet dies oft einen geringeren Arbeitsaufwand, wenn es um die Beweissicherung geht.

## Prävention und Schadensminderung

Zusätzlich zu den verschiedenen reaktiven Massnahmen können nationale Herangehensweisen zum Schutz gegen *Ransomware* durch Massnahmen der Prävention und Schadensminderung ergänzt werden. Die meisten Länder verfügen über sogenannte staatliche *Computer Emergency Response Teams* (CERT), die dafür zuständig sind Erkenntnisse über Bedrohungen zu verbreiten und Empfehlungen zur Eindämmung spezifischer Gefahren der Cybersicherheit auszusprechen. Bezüglich der Bedrohung durch *Ransomware* unterstüt-

### «Zahlen Sie kein Lösegeld!»

So lautet der gängige Ratschlag von Behörden an *Ransomware*-Betroffene. Die Begründung ist, dass Lösegeldzahlungen aus gesamtgesellschaftlicher Perspektive eine negative Wirkung haben, da sie Angreifer ermutigen ihre Machenschaften fortzusetzen. Darüber hinaus riskieren *Ransomware*-Opfer, die Lösegeld zahlen, erneut ins Visier zu geraten, da die Hacker deren niedrigen Sicherheitsstandards und ihre Zahlungsbereitschaft nun kennen. Letztlich liegt die Entscheidung für oder gegen die Lösegeldzahlung beim Opfer.

Die staatliche Empfehlung gegen die Zahlung ist allerdings nur ernst zu nehmen, wenn staatliche Stellen die Opfer auf andere Art und Weise unterstützen. So können Behörden beispielsweise andere Lösungen aufzeigen, um verschlüsselter Daten wiederherzustellen. Das von Europol, der dänischen Polizei und den Cybersicherheitsunternehmen Kaspersky und McAfee initiierte Projekt #NoMoreRansom bietet zum Beispiel Entschlüsselungstools für bestimmte Schadsoftware, die bei *Ransomware*-Angriffen eingesetzt wird.

**Weitere Artikel zum Thema**

Bernard Barbier / Jean-Louis Gergorin / Edouard Guillaud, "Il faut se demander si la France peut continuer à se passer d'une forte coordination stratégique de la cybersécurité auprès du président," *Le Monde,* 14.01.2022.

White House Press Release, "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting", 04.20.2021.

Institute for Security and Technology, *Combatting Ransomware – A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force,* September 2021.

Stefan Soesanto, "Wrong Turn or Right Lane? Defending Forward Against Cybercriminals Abroad," *Real Clear Defense,* 09.05.2020.

zen die staatlichen CERTs Unternehmen, indem sie Informationen über Schwachstellen teilen und dadurch die Infiltration von Systemen erschweren. Bei der Schadensminderung spielt letztlich auch die Strafverfolgung eine Rolle. So können *Ransomware*-Opfer bei der Entschlüsselung ihrer Daten durch Strafverfolgungsbehörden unterstützt oder bezüglich Lösegeldzahlungen beraten werden.

Ein Problem kann im Bereich präventiver staatlicher Massnahmen entstehen, wenn Regierungen die Betreiber kritische Infrastruktur und sonstige Unternehmen in unterschiedlichem Ausmass unterstützen. Betreiber von kritischer Infrastruktur profitieren häufig vom Informationsaustausch zu Bedrohungen in staatlich koordinierten Gruppen und mitunter zudem von technischer Unterstützung im Falle eines Angriffs. Die Einstufung nur bestimmter Einrichtungen eines Sektors als «kritisch» provozierte in der Vergangenheit Kritik. Ein wichtiges Beispiel in diesem Zusammenhang ist der Gesundheitssektor, in dem bereits die Stilllegung kleinerer Einrichtungen die Destabilisierung der gesamten Gesellschaft zur Folge haben kann (siehe CSS-Analyse Nr. 296). Deswegen unterstützt das staatliche CERT der Schweiz alle Einrichtungen des Gesundheitswesens und Energiesektors, unabhängig von ihrer Einstufung als kritisch.

## Resilienz

Letztlich gibt es eine wachsende Zahl von Richtlinien und Gesetzen zur Stärkung der Resilienz von Produkten. Massnahmen zur Stärkung der Resilienz beinhaltet die Förderung von Sicherheitspraktiken in Unternehmen, die über den reinen Informationsaustausch zu spezifischen Schwachstellen hinausgehen. Das besondere Augenmerk auf die Stärkung der Resilienz ist nicht überraschend. Eine Analyse der grössten *Ransomware*-Schadensfälle in Europa hat gezeigt, dass die meisten Angriffe hätten vermieden werden können.

Ansätze zur Implementierung von *Best Practices* hängen vom jeweiligen nationalen Kontext ab. Oftmals bestehen staatliche Massnahmen aus einer Kombination von gesetzlich vorgeschriebenen und freiwilligen Mechanismen. Zwingende gesetzliche Bestimmungen gelten in der Regel nur für die Betreiber von kritischer Infrastruktur. Jedoch haben grössere Cyberangriffe in jüngerer Zeit zu einem Kurswechsel in einigen Ländern geführt, in denen zuvor keine verbindlichen Anforderungen galten. So erliess die US-Behörde für Transportsicherheit beispielsweise zwingende Sicherheitsanforderungen für Betreiber kritischer Ölpipelines, darunter auch die Voraussetzung «unmittelbare Schutzmassnahmen gegen Cyberangriffe» zu ergreifen.

Für alle anderen Unternehmen werden *Best Practices* üblicherweise nur durch freiwillige Empfehlungen der Cybersicherheits-Behörden gefördert. Darüber hinaus beeinflussen Versicherungsunternehmen die Bereiche Risikomanagement und Schadensprävention von Unternehmen, indem sie Mindestanforderungen für das Abschliessen eines Versicherungsvertrages definieren. Laut einem Bericht der Allianz von 2021 erfüllen drei von vier Unternehmen nicht die Cybersicherheitsanforderungen, die für den Abschluss eines entsprechenden Versicherungsvertrages erforderlich wären und müssen zunächst ihre Sicherheitspraktiken anpassen, um sich für einen entsprechenden Versicherungsschutz zu qualifizieren.

## Künftige Zusammenarbeit

Die globalen Bedrohungen durch *Ransomware* können nicht im Alleingang bewältigt werden. Meistens befinden sich die Angreifer im Ausland, was sowohl bei der Prävention als auch bei der Reaktion eine internationale Zusammenarbeit erforderlich macht. Die Entwicklung einer umfassenden internationalen Strategie ist komplex und erfordert die Einbeziehung der verschiedensten Akteure. Die internationale Kooperation zu Themen der Cybersicherheit hat sich nicht nur innerhalb bestehender Sicherheitsbündnisse weiterentwickelt, sondern auch zwischen neuen Gruppierungen von Staaten. Anstrengungen wie die *Anti-Ransomware-Initiative* oder das *Agile-Nations-Netzwerk* verkörpern beispielsweise oft eine Kooperation zwischen Staaten mit besonders weit entwickelten nationalen Cybersicherheitskonzepten.

In naher Zukunft anstehende Massnahmen werden sich wahrscheinlich auf die Operationalisierung bilateraler Kooperationen konzentrieren. Ein Beispiel könnte die Entwicklung gemeinsamer Kriterien für digitale Beweise sein, die im System von *Ransomware*-Opfern gesichert werden sollten. Dies könnte dabei helfen, ein Ökosystem des Informationsaustauschs zwischen Staaten und Unternehmen aufzubauen, die einem Bündnis zur Bekämpfung von *Ransomware* angehören.

Die Verbesserung des Schutzes vor *Ransomware* ist ein langer und schrittweise verlaufender Prozess. Auf nationaler Ebene könnte eine politische Richtlinie, die sich explizit dem Thema *Ransomware* widmet, den staatlichen Schutz vor Angriffen unterstützen. Auf internationaler Ebene kann die Definition von grundlegende praktischen Schritten die länderübergreifende Zusammenarbeit verbessern.

**Mehr Informationen über Cybersicherheitspolitik finden Sie auf der CSS Themenseite.**

**Nele Achten** ist Senior Researcher für Cybersicherheitspolitk im Team für schweizerische und euroatlantische Sicherheit 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
Sprachbearbeitung: Nele Achten, Fabien Merz
Layout und Grafiken: Miriam Dahinden-Ganzoni

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

Zuletzt erschienene CSS-Analysen:

**Cybersicherheit im Gesundheitswesen regulieren** Nr. 296
**Mikrochips: klein und gefragt** Nr. 295
**Die Taliban im Fokus Chinas und Russlands** Nr. 294
**Ukraine, Georgien und Moldau zwischen Ost und West** Nr. 293
**Kampfroboter: Realität oder Science-Fiction?** Nr. 292
**Europäische Kampfflugzeug-Programme** Nr. 291


ISSN: 2296-0236; DOI: 10.3929/ethz-b-000530183