Kann Russlands SORM den Sanktionssturm überstehen?

Wilde, Gavin

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Wilde, G. (2023). Kann Russlands SORM den Sanktionssturm überstehen? *Russland-Analysen*, 439, 6-10. https://doi.org/10.31205/RA.439.02

- J. Byrne, Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine, London: Royal United Services Institute, 8. August 2022, https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine.
- S. Tolkachev, A. Teplyakov, Import Substitution in Russia. The Need for a System-Strategic Approach, Problems of Economic Transition, 60:7, 2018, S. 545–577,https://www.tandfonline.com/doi/abs/10.1080/10611428.2022.2111162.

ANALYSE

Kann Russlands SORM den Sanktionssturm überstehen?

Gavin Wilde (Carnegie Endowment for International Peace, Washington D.C.)

DOI: 10.31205/RA.439.02

Zusammenfassung

Russlands digitaler Telekommunikationssektor und das elektronische Überwachungssystem SORM waren vor dem Angriffskrieg gegen die Ukraine in hohem Maße auf westliche Technologien angewiesen. Nach der Invasion haben westliche Sanktionen und Exportkontrollen den Zugang zu Hard- und Software massiv erschwert. Russlands repressiver Überwachungsstaat steht nun vor ungewissen Aussichten, da sich im Inland oder in China hergestellte Technologien als unzureichend erweisen könnten, um westliche Importe zu ersetzen.

Fünfzehn Jahre bevor Edward Snowden die elektronischen Überwachungsmöglichkeiten der USA offenlegte, gelangte eine junge russische Journalistin namens Wiktorija Jegorowa in den Besitz eines Dokuments, in dem Russlands eigene Bemühungen zur Überwachung von Telefon- und zunehmend auch digitalen Netzwerken beschrieben wurden. Im Laufe der nächsten zwei Jahrzehnte lüfteten investigative Journalist:innen wie Irina Borogan und Andrej Soldatow den Schleier der Geheimhaltung um Russlands System für Fahndungs- und Ermittlungsmaßnahmen (Sistema operatiwno-rosysknych meroprijatij, SORM) (https://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet). Diese Erkenntnisse, insbesondere vor dem Hintergrund des erneuten Einmarsches Moskaus in die Ukraine im Jahr 2022 und der anschließenden technologischen und wirtschaftlichen Isolierung vom Westen, werfen nun Fragen hinsichtlich der langfristigen Überlebensfähigkeit von SORM auf.

Moskaus erste Forschungs- und Entwicklungsanstrengungen (F&E) für ein umfangreiches System der Telefonüberwachung begannen Mitte der 1980er Jahre in der damals ältesten F&E-Einrichtung der Sowjetunion im Moskauer Vorort Kutschino. Zu dieser Zeit war die 12. Abteilung des KGB für die technischen Details des Abhörens und der Überwachung der inländischen Telefonzentralen zuständig. Nach dem Zusammenbruch der Sowjetunion übernahm die wichtigste Nachfolgebehörde des KGB, der Föderale Sicherheitsdienst (FSB), das Programm, wobei das ähnlich benannte sogenannte 12. Zentrum die Leitung innehatte.

Mitte der 1990er Jahre wurden die analogen Festnetz-Telekommunikationssysteme allmählich durch digitale Systeme und Mobilfunk ersetzt. Parallel dazu entwickelten sich auch die Funktionen von SORM weiter. Als beispielsweise 1998 die E-Mail schlagartig Verbreitung fand, schlugen die russischen Kommunikationsbehörden vor, dass alle Internetdienstanbieter (Internet Service Providers, ISP) auf eigene Kosten SORM-fähige »Black Boxes« installieren sollten. Dabei handelte es sich um Komponenten, die es dem FSB ermöglichten, den Internetverkehr abzuhören. Um bestimmte Inhalte abzuhören, waren gerichtliche Anordnungen erforderlich, allerdings war der FSB nicht verpflichtet, Dritte, einschließlich Internetanbieter, über diese Anordnungen zu informieren (https://www.themoscowtimes.com/2013/06/18/nsa-is-no-match-for-the-fsb-a25059). Der FSB fungierte auch als alleinige Lizenzierungsbehörde für die von den russischen Anbietern verwendeten kryptografischen Mechanismen, wodurch der meiste Webverkehr leicht zu entschlüsseln war. Die russischen Behörden konkurrierten später mit der Ende-zu-Ende-Verschlüsselung seitens der Nutzer:innen, was die Überwachung erschwerte (https://www.bbc.com/news/technology-43668537). Zur Jahrtausendwende trat die verschärfte Regulierung der staat-

lichen Überwachung in Kraft, die insbesondere die großen russischen Telekommunikationsunternehmen und Internetanbietern in die Pflicht nahm.

Unter Präsident Wladimir Putin wurde Russland immer repressiver, und auch SORM hielt mit diesen Entwicklungen Schritt. Seit 2016 sind Telekommunikationsunternehmen und Internetdienstanbieter im Rahmen der als »Jarowaja-Gesetzgebung« bekannten Anti-Terror-Gesetzgebung verpflichtet, alle Inhalte – hierzu gehören Sprache, Text, Video und Bilder – sechs Monate lang aufzubewahren. Zugehörige Metadaten (Absender, Empfänger, Zeitstempel, Standort) müssen bis zu drei Jahre lang gespeichert werden. Diese Daten sind auf Anfrage den Behörden zur Verfügung zu stellen. Anfallende Infrastrukturkosten für die Einhaltung dieser Vorschriften müssen allein von den Dienstleistern getragen werden. Ab 2020 forderte der FSB ausnahmslos den uneingeschränkten Fernzugriff auf alle Nutzer:innendaten sowie die automatische Entschlüsselung der Kommunikation. Anfang 2021 zentralisierte das Innenministerium die eigenen Überwachungsprogramme, die wiederum dem 12. Zentrum des FSB unterstellt wurden.

Im Sommer 2022 ging das Digitalministerium dazu über, nicht nur Geldstrafen gegen Internet- und Telekommunikationsanbieter zu verhängen, die sich nicht an die SORM-Regulierung hielten, sondern verweigerte ihnen auch die Betriebslizenz oder entzog diese ganz. Die föderale Aufsichtsbehörde Roskomnadsor nutzte die SORM-Infrastruktur, um den Datenverkehr und den Zugang zu tausenden von westlichen Websites und Diensten zu sperren. Moskaus langjähriges Projekt, sein »souveränes Internet« (https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/) von allen Webinhalten abzuschotten, die den Interessen des Kremls zuwiderlaufen, wurde zusehends mit SORM integriert mit dem Ziel, ein weitgehend in sich geschlossenes, leicht zu überwachendes und regulierbares Informationsökosystem zu schaffen. Die Leitlinie, die sich daraus für die Praxis der digitalen Kommunikation ergab, lautet: »was nicht überwacht oder zensiert werden kann, wird nicht übertragen«. So deutet beispielsweise die Tatsache, dass Moskau zunächst versucht hat, die beliebte Messaging-App Telegram im Jahr 2018 vollständig zu blockieren, dann aber nach diesem gescheiterten Versuch dazu übergegangen ist, die App in vollem Umfang zu nutzen, auf eine gewisse Fähigkeit zur Entschlüsselung des Datenverkehrs hin (https://focus.ua/digital/525481-fsb-u-kursi-chomu-peresichnim-ukrajincyam-ta-mozhnovladcyam-ne-slid-koristuvatisya-telegram), entweder mit oder ohne Zustimmung von Telegram (https://www.themoscowtimes.com/2017/09/27/fsb-seeks-telegram-encryption-keys-founder-claims-a59085).

Derzeit nutzt Moskau SORM zudem wahrscheinlich für einige rudimentäre Überwachungsmaßnahmen in ehemaligen Sowjetrepubliken (https://privacyinternational.org/blog/1296/lawful-interception-russian-approach) und vermarktet SORM-Fähigkeiten an befreundete Staaten in Lateinamerika und anderen Regionen. Westliche Technologie wiederum scheint eine Schlüsselrolle bei der Entwicklung von SORM gespielt zu haben. Die Entwicklung über das bloße Abhören von Telefongesprächen hin zur Überwachung des Internetverkehrs (auch Deep Packet Inspection, kurz DPI genannt) erforderte einen massiven Datenvernetzungs- und Speicherbedarf (Storage Area Network, SAN). Amerikanische, japanische, südkoreanische und europäische Firmen sind die Hauptakteure auf dem globalen SAN-Markt. Aus Dokumenten, die TechCrunch (https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/) und der New York Times (https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html) zwischen 2019 und 2022 zugespielt wurden, geht hervor, dass Geräte des finnischen Unternehmens Nokia und der US-amerikanischen multinationalen Unternehmen Cisco und Procera für die Funktionsfähigkeit von SORM unentbehrlich waren. Dies ist nicht unbedingt ungewöhnlich, da Regierungen auf der ganzen Welt, auch in Demokratien mit transparenterer Rechtsprechung, digitale Netzwerkprodukte benötigen, um Abhörprogramme für Strafverfolgungsbehörden zu erleichtern. Diese Enthüllungen ermöglichten jedoch einen Einblick in die offensichtliche Abhängigkeit von ausländischer Technologie, was in krassem Gegensatz zu Russlands Rhetorik steht, »Importsubstitutionen« voranzutreiben und Russland technologische Autarkie zu garantieren.

Gleichzeitig besteht ein inländisches Ökosystem von Auftragnehmern und Zulieferern, die SORM ermöglichen. Durch eine Reihe von Fusionen und Übernahmen in den letzten zehn Jahren wurden viele dieser Unternehmen zeitweise unter der direkten und indirekten Aufsicht einer einzigen Person konsolidiert: dem in Usbekistan geborenen russischen Tycoon Alischer Usmanow. Usmanow, der zu den 100 reichsten Personen der Welt gehörte, unterhält Berichten zufolge enge Beziehungen zu hochrangigen Kreml- und FSB-Beamten und besitzt große Anteile an der größten russischen Telekommunikationsgesellschaft Megafon. Er war auch ein wichtiger Partner für das Zitadel-Konglomerat, das schätzungsweise 60–80 Prozent (https://thebell.io/partner-usmanova-monopoliziroval-rynok-proslushki-dlya-zakona-yarovoj) der Unternehmen kontrolliert, die SORM landesweit ausstatten. Hierzu gehören MFI Soft, Norsi-Trans und Special Technologies, die auch ehemalige Offiziere des 12. Zentrums des FSB als Mitarbeitende beschäftigen

sind. Das Unternehmen Zitadel hat somit am meisten von der »Jarowaja-Gesetzgebung« profitiert.

Russlands erneuter Einmarsch in die Ukraine Ende Februar 2022 stellte einen Wendepunkt dar. Innerhalb weniger Wochen stellten zahlreiche westliche Technologieunternehmen ihre Tätigkeit auf dem russischen Markt freiwillig ein oder begannen damit, Vorbereitungen für den Rückzug zu treffen. Zu den Unternehmen, die Russland den Rücken kehrten, gehörten Nokia, Cisco und Procera, aber auch andere wichtige Konzerne wie Intel, Adobe, Hewlett-Packard, Microsoft, Dell, Eriksson, LG, Nvidia, Kyocera, Siemens, SAP, Oracle, Juniper Networks und Samsung (https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain). Nach einigen Einschätzungen entfiel fast ein Fünftel des gesamten Rückzugs vom russischen Markt auf Technologieunternehmen. Durch diese Abwanderung wurden die Pläne des Digitalministeriums für die Einführung von 5G zunichte gemacht, was viele Brancheninsider:innen die Sorge äußern ließ, dass der durch den Rückzug bedingte Mangel an Ausrüstung die Mobilfunknetze des Landes langfristig lähmen könnte. So bedienten Geräte von Ericsson und Nokia (beispielsweise Antennen oder Glasfaserkabel) fast die Hälfte aller Mobilfunkbasisstationen in Russland. Umgekehrt machte der russische Markt wiederum nur zwei bis drei Prozent der globalen Einnahmen dieser Unternehmen aus.

Ein weiterer wichtiger Faktor sind die westlichen Sanktionen und Exportkontrollen. Diese Beschränkungen durch die Vereinigten Staaten und 37 andere Länder, die in mehreren komplexen und koordinierten Runden erlassen wurden, zielen darauf ab, die Lieferung strategischer Technologien, vor allem Halbleiter und andere mikroelektronische Komponenten, an das russische Militär zu unterbinden. Dazu gehörte auch die erstmalige Anwendung der *Foreign Direct Product Rule* (https://www.atlanticcouncil.org/blogs/econographics/foreign-direct-product-rule-is-russia-the-next-huawei/) durch die Vereinigten Staaten gegen ein ganzes Land, um dessen Zugang zu Erzeugnissen, die in den USA hergestellte Software und Hardware verwenden, erheblich einzuschränken. Auch wenn der russische Telekommunikationssektor (noch) nicht in großem Umfang von solchen Beschränkungen betroffen ist, besteht der begründete Verdacht, dass Moskau wichtige Komponenten zur Deckung des unmittelbaren militärischen Bedarfs abzweigt. So haben ukrainische staatliche Sprecher:innen berichtet, dass Chips aus Haushaltsgeräten in erbeuteten russischen Panzern und abgeschossenen Drohnen gefunden wurden. In diesem Zusammenhang sind auch Berichte zu sehen, dass der US-Gigant Cisco, nicht verkaufte Lagerbestände und Ersatzteile im Wert von über 23 Millionen Dollar vernichtete, als er seinen Rückzug aus Russland im Frühjahr 2023 vollzog, damit diese nicht in die Hände eines immer repressiveren Regimes fallen, das einen brutalen Krieg gegen seinen Nachbarn führt.

Die Ausweitung des Wirkungsbereichs von SORM auf besetzte ukrainische Gebiet veranlasste die Vereinigten Staaten dazu, die Zitadel-Holding und anderer Lieferanten Anfang 2022 zu erfassen. Auch Usmanow und sein Geschäftsimperium befinden sich im Fadenkreuz. Nachdem die Vereinigten Staaten bereits kurz nach Ausbruch des Krieges sein persönliches Vermögen eingefroren hatten, blockierten sie im April 2022 jegliche Transaktionen mit Wirtschaftsunternehmen, die ihm direkt oder indirekt zu 50 Prozent oder mehr gehören, darunter Megafon. Die Europäische Union folgte diesem Beispiel. Dies könnte möglicherweise der Hintergrund sein, warum Usmanow Anfang 2023 seinen »Rückzug« aus dem Geschäftsleben ankündigte (https://www.svoboda.org/a/usmanov-soobschil-rspp-ob-othode-ot-aktivnoy-deyateljnosti-/32235558.html) und Anteile an Unternehmen, die für den Betrieb von SORM unerlässlich sind, zu veräußern (https://www.vedomosti.ru/business/news/2022/03/02/911731-usm-prodaet-iks-holding). Der Kreml wirkte zudem hinter den Kulissen darauf hin (https://interfax.com/newsroom/top-stories/87391/), dass die staatlich kontrollierte Rostelekom Megafon übernimmt. Der russische Minister für digitale Entwicklung, Maxut Schadajew, teilte Interfax im Februar 2023 mit, dass eine solche Übernahme die territoriale Abdeckung durch eine optimierte Verteilung des knappen technischen Inventars erweitern würde, anstatt dass jeder Anbieter nur sein eigenes Netz und seinen eigenen Kundenstamm bediene. Zu möglichen kartellrechtlichen Bedenken äußerte er sich nur flüchtig.

Mangelnde Konsolidierung auf dem Mobilfunkmarkt stellte bisher ein Hindernis für SORM dar, und das schon vor den westlichen Sanktionen und der daraus resultierenden Knappheit an technischer Ausrüstung. In Ermangelung eines einheitlichen, staatlich geführten Telekommunikationsunternehmens erfüllten unabhängige Anbieter lange Zeit nur schleppend das absolute Minimum an SORM-bezogenen Anforderungen. Branchenkenner:innen weisen darauf hin, dass dafür technologische Interoperabilität und Langlebigkeit eine notwendige Voraussetzung ist, die in der Praxis oft nicht gegeben sind.

Dabei ist die vollständige Einhaltung aller gesetzlichen Regelungen kostspielig. Eine Untersuchung (https://www.rbc.ru/technology_and_media/09/11/2017/5a03187e9a7947d88f988f53) von Russia Business Consulting aus den Jahren 2016–2017 ergab, dass Roskomnadsor in diesem Zeitraum über 450 SORM-bezogene Strafen für administrative Verstöße gegen mehr als 200 Anbieter und Einzelpersonen verhängte. Zu

bedenken ist dabei, dass die finanzielle Belastung, die die Umsetzung von SORM mit sich bringt, insbesondere für kleinere Unternehmen nahezu unerschwinglich war. Der FSB und das Digitalministerium schätzten 2017 die durch SORM verursachten Kosten für die Branche auf bis zu 4,5 Billionen Rubel (https://tjournal.ru/tech/72992-v-rossii-vstupila-v-silu-samaya-zhestkaya-chast-zakona-yarovoy-operatory-potratyat-rekordnye-summy-a-ceny-vyrastut), während die Russische Union der Industriellen und Unternehmer in seiner eigenen Schätzung von mehr als dem Dreifachen dieser Summe ausging. Mit anderen Worten: Sowohl die politischen als auch die wirtschaftlichen Aspekte von SORM schaffen Anreize für die Konsolidierung unter den größten Internet- und Telekommunikationsanbietern (https://www.reuters.com/markets/deals/russia-approves-veons-sale-vimpelcom-management-rbc-cites-sources-2023-02-01/), da für kleinere Unternehmen die Kosten für die Einhaltung und Nichteinhaltung von SORM gleichermaßen unerschwinglich sind (https://dgap.org/en/research/publications/security-first-technology-second) und ihnen der politische Einfluss großer Konkurrenten wie Rostelekom, MTS und Megafon fehlt. Sollte das bisher von Usmanow-kontrollierte Megafon tatsächlich in Staatseigentum übergehen, wäre dies ein weiteres Anzeichen, dass der Kreml weniger an Förderung des Technologiesektors interessiert ist als an dessen bloßer Unterwerfung.

Ironischerweise würde eine größere staatliche Kontrolle über die Telekommunikationsbranche das SORM-Programm für westliche Sanktionen und technologische Isolation anfälliger denn je machen. Je länger Russland auf Hardware- und Softwarelösungen angewiesen ist, für die keine Updates oder Dienstleistungen in Aussicht gestellt werden, desto größer wird die technologische Bürde, die SORM in der Zukunft generieren wird. Wie der Branchenanalyst Roger Entner im April 2022 gegenüber der Moscow Times erklärte, »wird Russland im Jahr 2022 stehen bleiben, während sich der Rest der Welt weiterentwickelt. Das Land könnte sich in ein gescheitertes Technologiemuseum verwandeln« (https://www.themoscowtimes.com/2022/04/22/failing-technology-museum-uncertain-future-for-russian-telecoms-as-foreign-firms-flee-a77464). Es gibt weitere Anzeichen, dass sich diese Prognose erfüllen könnte, da sowohl das Ministerium für digitale Entwicklung als auch Brancheninsider:innen im Frühjahr 2023 einräumten, dass eine groß angelegte Einführung der 5G-Mobilfunktechnologie in ganz Russland bis mindestens 2030 (https://www.kommersant.ru/doc/5988542) unwahrscheinlich bleibt. Verantwortlich dafür sei sowohl einen Mangel an ausländischen Komponenten als auch an inländischen Produktionskapazitäten. Ob Unternehmen wie Ericsson bereit sind, Lizenzen für in Russland hergestellte Versionen ihrer Geräte zu vergeben, bleibt offen (https://www.kommersant.ru/doc/5967047). Gleichzeitig sind die sogenannten »Parallelimporte« (der Import von Gütern über Drittländer ohne Genehmigung der Hersteller, Anm. d. Red.) mit Engpässen und Strafmaßnahmen verbunden sind (https://www.macobserver.com/news/russia-legalizes-shady-gray-market-for-tech-products-in-effort-to-skirt-sanctions/; https://eurasianet.org/russias-parallel-imports-hindered-by-central-asia-bottleneck).

Telekommunikationsunternehmen und Internetanbieter sind nicht die einzigen Akteure, auf die sich die russischen Behörden stützen, um ihre umfassenden Überwachungsmaßnahmen zu ermöglichen. Im Jahr 2017 richtete die Zentralbank das »Einheitliche Biometrische System« (Jedinaja Biometritscheskaja Sistema, JeBS) ein, um die Millionen Proben von Stimmen und Gesichter der Kund:innen russischer Banken zu speichern. Innerhalb von vier Jahren wurde die Anbindung an das JeBS und die Eingabe von Daten in das System für die Finanzbranche verpflichtend. Ende letzten Jahres erklärte Präsident Wladimir Putin das JeBS zum einzigen Speicherort für biometrische Daten, das per Gesetz nun Daten erfasst, die von Fingerabdrücken bis hin zu Überwachungskameraaufnahmen von Straßen reichen. Außerdem übertrug Putin die gesamte Aufsicht und operative Kontrolle über das JeBS an den FSB, der mit ziemlicher Sicherheit beabsichtigt, das JeBS und SORM zu integrieren. Eine solche Interoperabilität, die eine ausreichende Infrastruktur an Datenbanken notwendig macht (https://www.kommersant.ru/doc/5258236), erscheint kurzfristig allerdings als unwahrscheinlich.

Selbst wenn der Kreml beschließen würde, die Milliardenkosten für den Austausch veralteter westlicher Technik in Russlands digitaler Kommunikations- und Überwachungsinfrastruktur zu übernehmen, ist es ebenso unwahrscheinlich, dass im Inland oder in China hergestellte Geräte Ersatz schaffen können. So berichtet beispielsweise die staatlich kontrollierte Zeitung *Kommersant* (https://www.kommersant.ru/doc/3670738), dass die Hälfte des russischen Marktes für Computerserver aus ausländischer Produktion stammt. Einer aktuellen Studie des *Bank of Finland Institute for Emerging Economies* (BOFIT) zufolge ist jedoch der Wert der weltweiten Technologieeinfuhren nach Russland zwischen Dezember 2021 und Dezember 2022 um 30 Prozent gesunken. Dieser Wert umfasst auch Importe aus China, die um 10 Prozent zurückgingen.

Die Abhängigkeit von China würde eigene Risiken mit sich bringen, wie in einem kürzlich durchgesickerten Schreiben des russischen Ministeriums für digitale Entwicklung an nationale Sicherheitsbeamte vom Sommer 2022 dargelegt wird (https://www.themoscowtimes.com/2023/04/19/sanctions-hit-russia-weary-of-over-

reliance-on-chinese-tech-bloomberg-a80875). In dem Dokument wird nicht nur vor Gefahren für die Funktionsfähigkeit kritischer Informationsinfrastrukturen gewarnt, sondern auch für die Überlebensfähigkeit einheimischer Technologieunternehmen. Als Maßnahme schlug das Ministerium Einfuhrbeschränkungen für Huawei und andere chinesische Produkte vor. Außerdem räumte das Ministerium ein Zeitrahmen von bis zu 24 Monaten ein, um eine vollständige Abhängigkeit von Peking abzuwenden. Diese Periode könnte wiederum ein Hinweis auf die schwindenden Lagerbestände der wichtigsten Ersatzteile sein. Eine neuere Analyse der Handelsdaten zeigt jedoch, dass China seit Beginn des Krieges zwar ein Rettungsanker für einige wichtige Technologieexporte nach Russland war, aber gleichzeitig nicht in der Lage ist, jegliche benötigte Technologie zu ersetzen.

So aufrichtig Peking Moskau beruhigen mag, wie innig doch die Freundschaft zwischen den beiden Ländern ist, so hindern dennoch die westlichen Sanktionen chinesische Technologiegiganten wie Huawei und ZTE daran, der schwächelnden russischen Technologiebranche zu Hilfe zu kommen. Huawei wartet zwar weiterhin in Russland installierten Geräte und rüstet diese nach (ganz im Gegensatz zu Ericsson und Nokia). Der chinesische Konzern hat aber seine Aktivitäten in Russland merklich eingeschränkt und neue Aufträge eingestampft. Die Unternehmen beider Länder sind weitgehend von global agierenden Halbleiterherstellern wie Taiwan Semiconductor Manufacturing Company (TSMC) mit Sitz in Taiwan, Intel mit Sitz in den USA und Samsung mit Sitz in Südkorea abhängig, welche sich bisher an die vom Westen verabschiedeten Sanktionen halten. Mit diesen Einschränkungen begrenzt der Westen somit auch das Ausmaß, in dem Russlands wachsende Defizite in der Spitzentechnologie ausgleichen kann.

Letztendlich ist der vom FSB geführte Überwachungsstaat, den der Kreml vor dem Krieg gegen die Ukraine (und der KGB in der Blütezeit des Kalten Krieges) im Sinne hatte, nun mit vielen, durch den Krieg entstandenen Abhängigkeiten konfrontiert, die den Ausbau hemmen könnten. Viele Aspekte des Programms unterliegen der Geheimhaltung. Die vorliegenden Erkenntnisse deuten jedoch darauf hin, dass das Schicksal von SORM weitgehend mit dem des russischen Technologiesektors verwoben ist. In dem Maße, wie die Kosten steigen, die Komponenten knapper werden und westliche Regierungen Unternehmen wie Zitadel ins Visier nehmen, werden wahrscheinlich auch die Überwachungsmöglichkeiten und -kapazitäten des FSB leiden.

Über den Autor

Gavin Wilde ist Senior Fellow im Programm für Technologie und internationale Angelegenheiten beim Carnegie Endowment for International Peace, wo er sich mit Cyber- und Informationskonflikten beschäftigt. Zuvor war er als Direktor für Russland, das Baltikum und den Südkaukasus beim Nationalen Sicherheitsrat der USA und als leitender Analyst bei den US-Geheimdiensten tätig. Er ist ein Absolvent des National War College (mit Auszeichnung), wo er sich auf Informationskriegsführung spezialisiert hat.

Lesetipps

- Byrne, James, Gary Somerville, Joe Byrne, Jack Watling, Nick Reynolds, and Jane Baker. 2022. "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine." RUSI, August 2022. https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_0.pdf.
- Epifanova, Alena und Philipp Dietrich. 2022. "Russia's Quest for Digital Sovereignty: Ambitions, Realities, and Its Place in the World." DGAP Analysis 1, Februar 2022. https://dgap.org/sites/default/files/article_pdfs/DGAP-Analyse-2022-01-EN_0.pdf.
- Farah, Douglas und Marianne Richardson. 2022. "Dangerous Alliances: Russia's Strategic Inroads in Latin America." INSS Strategic Perspectives 41 (Dezember 2022). https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/strategic-perspectives-41.pdf.
- Wilde, Gavin; Sherman, Justin. 2023. "No Water's Edge: Russia's information War and Regime Security." Carnegie Endowment for International Peace, 04. Januar 2023. https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644
- Wilde, Gavin; Sherman Justin. 2022. "Putin's internet plan: Dependency with a veneer of sovereignty." Brookings, 11. Mai 2022. https://www.brookings.edu/techstream/putins-internet-plan-dependency-with-a-veneer-of-sovereignty/
- Simola, Heli. 2023. "The Shift in Russian Trade during a Year of War." BOFIT Policy Brief 9/2023. https://publications.bof.fi/handle/10024/52738
- Simola, Heli und Aino Röyskö. 2023. "Russia's Technology Imports from East Asia." Asian Economic Papers 22 (1): 1–10. https://direct.mit.edu/asep/article/22/1/1/114932/Russia-s-Technology-Imports-from-East-Asia
- Soldatov, Andrei und Irina Borogan. 2022. "Russia's Surveillance State." Center for European Policy Analysis, 26. Oktober 2022. https://cepa.org/article/russias-surveillance-state/