

### Die Sanktionen machen sich bemerkbar: Trübe Aussichten für die russische Chipindustrie

Nocetti, Julien

Veröffentlichungsversion / Published Version

Zeitschriftenartikel / journal article

**Empfohlene Zitierung / Suggested Citation:**

Nocetti, J. (2023). Die Sanktionen machen sich bemerkbar: Trübe Aussichten für die russische Chipindustrie. *Russland-Analysen*, 439, 3-6. <https://doi.org/10.31205/RA.439.01>

**Nutzungsbedingungen:**

Dieser Text wird unter einer CC BY-NC-ND Lizenz (Namensnennung-Nicht-kommerziell-Keine Bearbeitung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:

<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>

**Terms of use:**

This document is made available under a CC BY-NC-ND Licence (Attribution-Non Commercial-NoDerivatives). For more information see:

<https://creativecommons.org/licenses/by-nc-nd/4.0>

## Die Sanktionen machen sich bemerkbar: Trübe Aussichten für die russische Chipindustrie

Julien Nocetti (Französisches Institut für internationale Beziehungen – IFRI, Paris)

DOI: 10.31205/RA.439.01

### Zusammenfassung

Integrierte Schaltkreise oder Halbleiter sind Dual-Use-Technologien, die in weiten Bereichen Anwendung finden können, angefangen bei Smartphones bis hin zu Raketensystemen. Sukzessive Krisen – die Konkurrenz zwischen China und den USA, die Coronapandemie, der Krieg gegen die Ukraine – haben ihre strategische Bedeutung deutlich gemacht. Russlands Lage ist fragil, weil sich die Verfügbarkeit dieser Hardware merklich verschlechtert hat, denn internationalen Sanktionen zielen insbesondere auf die russische Halbleiterindustrie ab. Eine technologische Souveränität über eine Lokalisierung der Halbleiterindustrie erscheint höchst unwahrscheinlich. Dies hängt auch damit zusammen, dass der Verteidigungssektor als großer Abnehmer der Chips besonders heftig unter den Sanktionen leidet.

### Hardware-Schwächen: Die russische Halbleiterindustrie und der Markt

Die Halbleiterproduktion in Russland ist den industriellen Standards des Westens um Jahre hinterher. Nach dem Zusammenbruch der Sowjetunion erlebte die Industrie für elektronische Komponenten, die vor allem für die Verteidigungs-, Weltraum- und Atomindustrie produzierte, eine erhebliche Talfahrt.

Der Anteil elektronischer Geräte, die in Russland produziert und verkauft werden, ist auf rund 12 Prozent zurückgegangen. In den Ländern der OECD liegt die einheimische Produktion im Schnitt bei 70–80 Prozent des Inlandsbedarfs. In den 2000er Jahren nahm der Rückgang in Russland weiter an Fahrt auf, die technologische Kluft zu den USA und China vergrößerte sich. 2016 wurden Berichten zufolge 80 Prozent der IT-Produkte in Russland importiert. Das verstärkte die Vorstellung, dass Russland in diesen Bereichen eine Revolution verpasst hat. Auf Russland entfielen 2009 nur 0,44 Prozent der weltweiten Chipproduktion, und dieser Anteil wuchs danach nur langsam, wobei er in den 2010er Jahren niemals die Schwelle von drei Prozent überschritt und zudem ab 2014 nach der Verhängung der westlichen Sanktionen wieder zurückging. 2013 beschrieb der Vizepräsident des Russischen Ingenieursverbandes den Zustand der russischen Elektronikindustrie mit dem Prädikat »fortgeschrittene Veralterung«. In der Folge nahm sich die russische Führung des Problems an: 2016 rief Präsident Putin das Ziel aus, die Produktion komplexer ziviler und Dual-Use-Elektronikkomponenten in Russland zu steigern. Russische Komponenten konnten 2018 gleichwohl nur 27 Prozent des innerrussischen Bedarfs decken.

Vor allem ab 2020 bemühte sich Russland, technologisch aufzuholen und den Hochtechnologiesektor »souverän« zu machen. Fortschrittliche Halbleiter

spielen dabei angesichts der Intensivierung des technologischen Wettbewerbs zwischen China und den USA eine entscheidende Rolle. Eigene Komponenten herzustellen ist eine der Voraussetzungen für digitale Souveränität (<https://iz.ru/667647/andrei-bezrukov/mirovye-pole-boia>).

Im Januar 2020 wurde unter dem neuen Ministerpräsidenten Michail Mischustin die »Strategie für die Entwicklung der russischen Elektronikindustrie bis 2030« verabschiedet. Die Strategie umfasst drei Phasen: eine erste Phase der Substitution von Importen, gefolgt von einer zweiten Phase zur Förderung russischer Technologien auf den internationalen Märkten und schließlich eine dritte Phase mit dem Versuch, eine technologische Dominanz zu erreichen. Die Strategie ist höchst ambitioniert und ein Beispiel für den weltweiten Trend hin zu einem Protektionismus bei Technologie, der vor dem Hintergrund geoökonomischer Realitäten wie etwa der Destabilisierung von Lieferketten. Gleiches gilt für technologische Anforderungen wie etwa die Entwicklung immer kleinerer, immer komplexerer und leistungsfähigerer Chips.

Wie in China besteht in Russland das Problem weniger in der Frage, ob die entsprechenden Fähigkeiten vorhanden sind, sondern vielmehr in der Fähigkeit, das notwendige Umfeld und die erforderlichen Lieferketten für die Halbleiterproduktion zu schaffen. Gleichwohl deuten einige Schritte aus dem Jahr 2019 auf einen proaktiven Ansatz hin, etwa mit dem Erwerb eines kontrollierenden Anteils an dem russischen Privatunternehmen »Yadro« an dem ebenfalls russischen Unternehmen »Syntacore«. »Syntacore« hat ein internationales Konsortium begründet, das eine Open-Source-Prozessorarchitektur (RISC-V) entwickelt, die Weltmarktführern wie »Intel« Konkurrenz machen will.

Die beiden wichtigsten einheimischen Produzenten (»Baikal Electronics« und MCST) weisen zudem

einige Schwächen auf: Ersteres kann nicht auf russischen Lösungen zurückgreifen, da es Prozessoren verarbeitet, die auf der Architektur des in Großbritannien entstandenen Unternehmens ARM basieren. MCST wiederum entwickelt keine Produkte, die für den Massenmarkt geeignet wären. Beide Akteure sind bis zur Verhängung der Sanktionen gegen Russland von den Produktionskapazitäten der »Taiwan Semiconductor Manufacturing Company« (TSMC) abhängig gewesen.

### **Chips und Sanktionen: Auswirkungen auf die Importe nach Russland**

Nach dem Beginn des russischen Angriffskrieges gegen die Ukraine haben die westlichen Länder mit raschen und koordinierten Schritten eine Reihe von Maßnahmen getroffen, um Russland von den wichtigsten globalen technologischen Lieferketten abzuschneiden. Diese erfolgten in unterschiedlicher Form: Zunächst zielten die Kontrollmaßnahmen auf westliche Exporte bestimmter Technologien, insbesondere auf Dual-Use-Güter – also auf Produkte, die sowohl für den zivilen als auch den militärischen Sektor gebraucht werden.

In dem Wissen, dass Russland diese Technologien für seine Kriegsanstrengungen benötigt, haben die Vereinigten Staaten sowie ihre europäischen und asiatischen Verbündeten bei den Exportkontrollen früh die Halbleiterexporte in den Blick genommen. Die russischen Importe integrierter Schaltkreise sind nach Verabschiedung der Exportkontrollen und dem Rückzug multinationaler Unternehmen vom russischen Markt erheblich zurückgegangen. Die Importe bleiben auch deutlich geringer als vor dem Einmarsch in die Ukraine. Russland hat allerdings beträchtliche Anstrengungen unternommen, ein Netz von Zulieferern in Ländern aufzubauen, die sich nicht den Sanktionen angeschlossen haben. Mit Blick auf ihre potenzielle Nutzung für militärische Zwecke sollen die Halbleiter nun von dort kommen.

Russland ist also weiterhin in der Lage, Lieferanten für eine Reihe integrierter Schaltkreise zu finden, hauptsächlich aus China und Hong Kong, wenn auch in erheblich geringerem Umfang als vor dem Krieg. Wie im Falle anderer Güter wird ein kleiner Umfang über andere Länder verfrachtet. Die Exporte integrierter Schaltkreise aus China und Hong Kong belaufen sich auf 55 Prozent des Medianwerts der Exporte nach Russland in Bezug auf alle Länder im Vergleich zu Vorkriegszeiten (Die Exporte aus China und Hong Kong beliefen sich auf 45 Prozent der russischen Importe im Jahr 2019 und 33 Prozent der Importe von 2021). Es gab allerdings Berichte, dass die Mängelraten bei Halbleitern aus China hoch waren.

Einigen Berichten zufolge umfassten die Exporte nach Russland im Jahr 2022 Waren von großen mul-

tinationalen Produzenten, die von dritter Seite geliefert werden (<https://brief.kharon.com/updates/russian-import-network-acquired-electronics-through-companies-that-supply-chinese-military-and-western-manufacturers>). Darunter fallen auch Exporte an russische Unternehmen, die das inländische Militär beliefern. Der wichtigste Typ integrierter Schaltkreise, die seit dem Einmarsch in die Ukraine von Hong Kong und China nach Russland exportiert werden, sind Prozessoren und Mikrocontroller.

### **Auswirkungen der Sanktionen auf Chips: Soll zuerst Druck auf die russische Verteidigungsindustrie ausgeübt werden?**

Die Schwächen der einheimischen Industrie bei der Herstellung von russischen Waffen, Kommunikationsmitteln und elektronischer Systeme zur Kriegsführung sind in hohem Maße von im Westen produzierten Mikrochips abhängig, die derzeit unter die Regeln durch die Exportbeschränkungen der westlichen Allianz fallen (<https://www.electronicweekly.com/blogs/mannerisms/dilemmas/russias-backward-chip-industry-2022-04/>). Dem im Vereinigten Königreich angesiedelten »Royal United Services Institute« (RUSI) zufolge enthält zum Beispiel die russische Drohne »Orlan-10« (dt.: »Adler 10«) Chips, die von den Unternehmen »Texas Instruments« und »Honeywell« hergestellt werden. Des Weiteren hat eine Untersuchung der Rechercheplattform »Conflict Armament Research« gezeigt, dass die satellitengesteuerten Steuerungselemente mehrerer russischer Raketentypen (z. B. der Typen 3M14 [Code der NATO bzw. des US-Verteidigungsministeriums: SS-NX-30], 9M544, Ch-59 [NATO-Code: AS-13 Kingbolt] und Ch-101 [NATO-Code: AS-23 Kodiak]) mehrere im Ausland hergestellte Mikrokomponenten enthalten, die zwischen 2012 und 2020 hergestellt wurden (<https://storymaps.arcgis.com/stories/239f756e2e6b49a5bec78f5c5248bf3d>). Die russischen Raketensysteme der Typen »Iskander« und »Kalibr« sind mit modernsten Halbleitern ausgestattet, welche auch westliche Technologien miteinschließen.

Russlands neu entwickelte Systeme für die Funkkommunikation (u. a. das tragbare Funksystem »Asart«, das auf taktischer Ebene Kommunikation einerseits lahmlegen und andererseits sicherer machen soll) scheinen ebenfalls auf einer Vielzahl im Westen produzierter Komponenten zu beruhen. Den Daten des ukrainischen Think Tanks »Center for Army, Conversion, and Disarmament Studies« (CACDS) zufolge enthält »Asart« sechs Komponenten ausländischer Herkunft, unter anderem den Chip »Spartan 6«, der Kommunikation verschlüsselt und von dem US-amerikanischen Unternehmen »Xilinx« in Taiwan hergestellt wird. »Spartan 6« ist als Dual-Use-Produkt kommerziell verfügbar und kann über das chi-

nesische Portal »AliExpress« erworben werden. Ebenso beruht das russische Aufklärungs-, Kommando- und Kommunikationssystem »Strelez-M« auf sieben Komponenten ausländischer Herkunft, unter anderem auf einem Chip, der vom in den USA ansässigen Unternehmen »Microchip Technology« hergestellt wird.

Die Abhängigkeit des russischen Militärisch-Industriellen Komplexes (MIK) von im Ausland produzierten Mikrochips lässt sich durch mindestens zwei Faktoren erklären.

Zum einen scheinen die Mikroprozessoren, die innerhalb Russlands von einer kleinen Anzahl Unternehmen hergestellt werden, im Vergleich zu westlichen Lösungen an mangelhafter Qualität und übermäßiger Komplexität zu leiden. Nach Verhängung der westlichen Sanktionen waren die russischen Firmen nicht in der Lage, Technologien aus den USA oder deren Verbündeten, die sich den Sanktionen angeschlossen haben, legal zu erwerben. Hierzu zählte auch die »Taiwan Semiconductor Manufacturing Company« (TSMC), auf deren Produkte die russischen Chiphersteller in großem Maße zurückgriffen (<https://www.washingtonpost.com/technology/2022/02/25/ukraine-russia-chips-sanctions-tsmc/>). Ein Ersatz dieser Komponenten durch chinesische Versionen erfordert in einigen Fällen eine Neugestaltung der elektronischen Ausrüstung und eine Umstrukturierung der Unternehmensketten, was mehrere Jahre in Anspruch nehmen könnte (<https://secretmag.ru/technologies/chipy-pod-sankciyami-sposobna-li-rossiya-obespechit-sebja-mikroelektronikoi.htm>). Darüber hinaus hinken chinesische Chips in ihrem Aufbau den westlichen Chips hinterher. Bestimmte Chips (wie etwa »Spartan 6«, »TSOP 66« oder »LQFP64«), die im Kommunikationssystem »Asart« oder den Präzisionsraketen vom Typ 9M544 zu finden sind, können zwar über »AliExpress« bezogen werden, doch könnte die Nutzung solcher kommerziell verfügbaren Komponenten dazu führen, dass die russischen Waffensysteme weniger zuverlässig und stör anfälliger sind ([https://defence-ua.com/weapon\\_and\\_tech/na\\_mikroshemah\\_z\\_%20aliexpress\\_analogovnjeta\\_sistema\\_navedennja\\_tornado\\_s\\_z\\_rf\\_foto-8418.html](https://defence-ua.com/weapon_and_tech/na_mikroshemah_z_%20aliexpress_analogovnjeta_sistema_navedennja_tornado_s_z_rf_foto-8418.html)). So war Wally Adeyemo, der stellvertretende Finanzminister der USA, der Ansicht, dass »nahezu 40 Prozent der weniger fortschrittlichen Mikrochips, die

Russland aus China bezieht, mit Mängeln behaftet sind« (<https://home.treasury.gov/news/press-releases/jy1286>).

Zweitens kann die russische Halbleiterindustrie die große Nachfrage nach diesen Elementen nicht befriedigen. Daten von Ende 2022 zufolge benötigt das Land pro Monat bis zu 30.000 Platinen einfacher Mikrochips. Innerhalb Russlands können allerdings nur 8.000 Platinen produziert werden (<https://www.kommersant.ru/doc/5667792>). Im Januar 2023 verkündete die Regierung den Start eines neuen Technologieparks in der russischen Region Uljanowsk mit der Absicht, die dortige Halbleiterproduktion anzukurbeln (<https://www.kommersant.ru/doc/5759442>). Angesichts der Exportbeschränkungen ist es allerdings schwierig, die Produktionsraten und die Qualität der dort gefertigten Produkte abzuschätzen.

### Schlussfolgerungen

Russland sieht sich bei der Produktion und der Lieferung von Halbleitern einer Reihe ungeheurer Herausforderungen gegenüber. Seit dem Einmarsch in die Ukraine sind beträchtliche Schwächen der Lieferketten von Halbleitern nach Russland zu Tage getreten. Diese Lieferketten sind nicht völlig unabhängig, es besteht hier also keine technologische Souveränität. Dass die internationalen Sanktionen gezielt den Chip-Sektor ins Visier nahmen, ist dabei kein Zufall: Dadurch, dass die zivile Industrie getroffen wird, hat der Militärisch-Industrielle Komplex damit zu kämpfen, sich nachhaltigen Zugang zu hochwertigen Mikrochips für seine Waffensysteme zu sichern. In diesem Bereich spielen Strategien zur Umgehung der Sanktionen eine Rolle, etwa die Errichtung illegaler Lieferketten. Eine genaue Nachverfolgung dieser Ketten ist aber nur schwer möglich. Auf dem Schlachtfeld in der Ukraine wird es wohl langfristig zu Problemen für die Leistungsfähigkeit der russischen Streitkräfte geben. Diese Entwicklung dürfte auch ein Licht darauf werden, wie es tatsächlich um die Substanz der russisch-chinesischen Beziehungen bestellt ist, da Moskau beträchtliche technologische Unterstützung von Peking erwartet. Dieses Bedürfnis Russlands steht allerdings in einem Spannungsfeld mit Chinas Befürchtungen, selbst Opfer sekundärer US-Sanktionen zu werden.

*Übersetzung aus dem Englischen: Hartmut Schröder*

#### Über den Autor

Dr. *Julien Nocetti* ist Associate Fellow am Französischen Institut für Internationale Beziehungen (IFRI), Forscher am Zentrum GEODE (Geopolitics of the datasphere, Université Paris 8) und leitet den Lehrstuhl für den Umgang mit Cyberrisiken an der School of Business in Rennes.

#### Lesetipps

- J. Byrne et al., The Orlan Complex: Tracking the Supply Chains of Russia's Most Successful UAV, London: Royal United Services Institute, Dezember 2022, <https://rusi.org/explore-our-research/publications/special-resources/orlan-complex-tracking-supply-chains-russias-most-successful-uav>.

- 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 operativno-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 Nachfolge-

behörde 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 Internetdiensteanbieter (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-