DGAP MEMO
Deutsche Gesellschaft für Auswärtige Politik e. V.

Nr. 25
Dezember 2024

# Spionagesoftware und Cyberangriffe: Die Gefahr durch nichtstaatliche Akteure steigt

Von Claudia Hofmann

**Die Verbreitung von Cyber-Intrusionstechnologien, einschließlich Spionagesoftware, stellt eine wachsende Bedrohung für die internationale Sicherheit dar. Während der Einsatz solcher Technologien einst staatlichen Akteuren vorbehalten war, setzen zunehmend auch nicht-staatliche Akteure diese Technologien ein – mit gravierenden Folgen für die globale Stabilität. Ein effektives internationales Exportkontrollsystem, flankiert von Sanktionen und weitreichenden rechtlichen Reformen, ist notwendig, um den Missbrauch einzudämmen.**

## EINE NEUE DIMENSION GLOBALER SICHERHEITSRISIKEN

Die Entwicklung von kommerziellen Cyber-Intrusionstechnologien und Spionagesoftware hat sich zu einer äußerst profitablen und schnellwachsenden Branche entwickelt, die allerdings zunehmend demokratischer Kontrolle und Regulierung entgleitet.

Laut einer Studie des Carnegie Endowment schlossen zwischen 2011 und 2023 mindestens 74 Regierungen Verträge mit kommerziellen Unternehmen ab, um Spionagesoftware oder digitale Forensiktechnologie zu erwerben. Während prominente Anbieter von Spionagesoftware wie die NSO Group und Intellexa Aufmerksamkeit erregen, tragen auch zahlreiche kleinere Unternehmen und Akteure im Bereich der Schwachstellen-Nutzung zur Entwicklung und Verbreitung dieser Technologien bei.

Von diesen 74 Regierungen nutzten 44 autokratische Regime Überwachungstechnologien, verglichen mit 30 liberalen Demokratien, die auf diese Technologie zurückgriffen. Russland beispielsweise nutzt die Pegasus-Software der NSO Group zur Überwachung unabhängiger Medien und zur Identifizierung von Reporter-Netzwerken. Auch das Umfeld des 2018 ermordeten Washington-Post-Reporters Jamal Khashoggi wurde gezielt mit Pegasus ausspioniert. Demokratische Regierungen haben solche Technologien ebenfalls gegen die Zivilgesellschaft eingesetzt, wie etwa Vorfälle in Polen zeigten.

**Cyber-Intrusionstechnologien** sind Werkzeuge und Techniken, die unbefugten Zugang zu Computersystemen, Netzwerken oder Geräten ermöglichen. Dazu zählt **Spionagesoftware**, die speziell zur Überwachung und Sammlung sensibler Daten entwickelt wurde, sowie **Malware**, eine Art Schadsoftware wie Viren oder Trojaner, die dazu dient, Systeme zu infiltrieren oder zu manipulieren. Ebenfalls wichtig sind **Exploits**, spezielle Codes, die gezielt Sicherheitslücken in Software ausnutzen, um Zugriff oder Kontrolle zu erlangen. Diese Technologien werden häufig unter dem Begriff „**Hacking-Tools**" zusammengefasst und können sowohl zu legitimen Zwecken als auch für missbräuchliche Aktivitäten eingesetzt werden.

## CYBEROPERATIONEN UND DIE VERBREITUNG VON SPIONAGESOFTWARE DURCH NICHT-STAATLICHE AKTEURE

Mit der zunehmenden Verbreitung kommerzieller und nicht-kommerzieller Technologien steigt zudem die Gefahr, dass sie in die Hände krimineller nicht-staatlicher Akteure gelangen.

Es braucht daher ein internationales Exportkontrollsystem, Sanktionen und weitreichende rechtliche Reformen, um den Missbrauch dieser Technologien einzudämmen.

**Hisbollah: Professionalisierte Cyberfähigkeiten**
Die Hisbollah verfügt über komplexere und professionellere Cyberfähigkeiten als andere Terrororganisationen, was auf eine Unterstützung durch den Iran hinweist. Bereits zwischen 2012 und 2015 führte die Gruppe die Cyberkampagne „Volatile Cedar“ durch, bei der maßgeschneiderte Malware zum Einsatz kam, um Medienunternehmen und Bildungseinrichtungen in den USA, Kanada, Israel und weiteren Ländern zu überwachen. Ab 2019 infiltrierte die mit Hisbollah verbundene Gruppe „Lebanese Cedar“ weltweit rund 250 Server, darunter in den USA, Großbritannien und dem Nahen Osten. Die dabei angewandten Techniken ähnelten stark denen des Irans, dessen Überwachungstechnologie, wie etwa das System „SIAM“, umfassende Kontroll- und Manipulationsmöglichkeiten bei Mobilfunknetzen bietet, einschließlich der Verfolgung von Bewegungsprofilen.

**Hamas: Effektive, aber weniger ausgereifte Cyberstrategien**
Die Cyberstrategien der Hamas setzen vor allem auf Massen-Phishing-Kampagnen, um Malware mit Spionagezwecken zu installieren. Eine Kampagne vom April 2022, die der Hamas zugeordnet wird, zielte auf israelisches Militär- und Sicherheitspersonal ab. Dabei kam eine zuvor unbekannte Malware mit verbesserten Tarnmechanismen zum Einsatz. Diese Operationen lieferten der Hamas wahrscheinlich Informationen über militärische Einrichtungen und Ausrüstungen der israelischen Verteidigungsstreitkräfte.

Zudem wird vermutet, dass die Türkei der Hamas nicht nur als Basis für kinetische Angriffsplanungen dient, sondern offenbar auch als Schutzraum für eine Cybereinrichtung im Ausland. Laut westlichen Geheimdienstberichten betreibt die Hamas seit spätestens 2018 ein geheimes Büro in Istanbul für Cyberoperationen und Gegenspionage, das Cyberangriffe gegen gegnerische Akteure in der Region koordiniert und interne Überwachung gegen mutmaßlich illoyale Mitglieder durchführt. Dieses Büro operiert angeblich unabhängig vom offiziellen Hamas-Hauptquartier in Istanbul und war offiziell weder anderen Hamas-Mitgliedern noch der türkischen Regierung bekannt.

**Spionagesoftware im mexikanischen Drogenkrieg: Verflechtung zwischen Staat und Kartellen**
Neben Terrororganisationen nutzen auch andere nicht-staatliche Akteure Spionagesoftware, etwa im Kontext des organisierten Verbrechens. So hat sich beispielsweise Mexiko in den letzten zehn Jahren zu einem bedeutenden Importeur von Spionagesoftware entwickelt, vornehmlich zur Unterstützung der Behörden im Kampf gegen kriminelle Kartelle. Neben der NSO Group sind laut DEA mehr als 20 weitere Anbieter solcher Technologien in Mexiko aktiv. Gleichzeitig wird vielen lokalen Beamten vorgeworfen, heimlich mit korrupten Politikern und Kartellen zusammenzuarbeiten, was diesen den Zugang zu Überwachungstechnologie erleichtert. Untersuchungen des Cartel Project seit 2020 zeigen, dass Polizeikräfte Spionagesoftware möglicherweise direkt an Kartelle weiterverkaufen. Im US-Prozess gegen Joaquín “El Chapo” Guzmán gestand ein Ingenieur des Kartells, Abhörgeräte beschafft zu haben, die Telefonate, Internetnutzung und Textnachrichten überwachen konnten. Kartelle ohne eigenes technisches Know-how greifen zudem auf korrupte Beamte zurück, die gegen Bestechungsgelder gezielte Überwachungsdienste für sie übernehmen.

## DEUTSCHLANDS REAKTIONEN UND HANDLUNGSOPTIONEN ZUR EINDÄMMUNG VON SPIONAGESOFTWARE

Deutschland sollte eine aktive Rolle bei der Eindämmung der Verbreitung kommerzieller Spionagesoftware spielen, da die unkontrollierte Verbreitung nicht nur autoritäre Regime stärkt, sondern auch die Sicherheit und digitale Souveränität demokratischer Staaten gefährdet.

Als Mitglied des im Februar 2024 gegründeten Pall-Mall-Prozesses unterstützt Deutschland schon die Entwicklung internationaler Leitprinzipien und politische Optionen im Umgang mit kommerziell verfügbaren Cyber-Intrusionstechnologien. Dieser Prozess befindet sich jedoch noch in einer frühen Phase, und es ist bislang unklar, ob sich Staaten, Industrie und die Zivilgesellschaft auf gemeinsame Prinzipien einigen können. Zudem gibt es bislang keinen Aktionsplan für deren mögliche Umsetzung.

In Fällen, in denen staatliche Akteure offensive Cyberfähigkeiten an nicht-staatliche Akteure weitergeben, kann Deutschland durch gezielte Maßnahmen wie Exportkontrollen, Sanktionen und internationale Kooperationen den Zugang nicht-staatlicher Akteure zu diesen Technologien erheblich einschränken und die Verbreitung auf autorisierte Kanäle lenken.

## POLITISCHE UND RECHTLICHE EMPFEHLUNGEN FÜR DIE BUNDESREGIERUNG

- **Zertifizierungspflicht einführen:** Nationale Datenschutzbehörden oder der Europäische Datenschutzbeauftragte sollten unabhängige Prüfungen durchführen, um die Sicherheitspraktiken der Anbieter und potenzielle Risiken für die Zivilgesellschaft unabhängig zu bewerten. Unternehmen könnten verpflichtet werden, die Kunden sowie deren beabsichtigte Nutzung der Produkte gründlich zu überprüfen, bevor sie Verkäufe oder Exporte genehmigen.

- **Endnutzungszertifikaten etablieren:** Mechanismen einführen, die gezielt verhindern, dass nicht-staatliche Akteure Zugang zu Cyber-Intrusionstechnologien erhalten. Diese Mechanismen könnten digitale Wasserzeichen oder Lizenzschlüssel beinhalten, um den Verbleib und die Nutzung der Technologie zu überwachen.

- **Exportkontrollregime etablieren:** Ein wirksames Exportkontrollsystem speziell für Überwachungstechnologien sollte entwickelt werden, um die Verbreitung und den Missbrauch solcher Technologien einzudämmen. Diese könnten Sanktionen gegen Firmen wie die NSO Group oder Intellexa nach dem Vorbild der USA einschließen.

- **Verhinderung unkontrollierter Weitergabe:** Maßnahmen entwickeln, um die ungewollte Diffusion von Cyber-Intrusionstechnologien und Spionagesoftware an nicht-staatliche Akteure zu verringern. Dazu gehören die verstärkte Analyse, Kontrolle und Regulierung von Schwachstellenmärkten und Sanktionen gegen Zwischenhändler und Drittstaaten. Diese Ansätze sollten in den bestehenden internationalen Rahmen für Exportkontrollen und Sanktionen integriert werden, um eine umfassende Strategie zur Verhinderung des Missbrauchs sicherzustellen.

- **EU-Sanktionen bei Missbrauch verhängen:** Deutschland und die EU sollten Sanktionen gegen Unternehmen und Staaten verhängen, die Cyber-Intrusionstechnologien missbräuchlich verwenden, insbesondere wenn dies gegen internationale Standards für den Schutz der Privatsphäre und der Menschenrechte verstößt. Sanktionen sollten auch jene Staaten treffen, die diese Technologien zur Repression der Zivilgesellschaft oder zur Unterstützung von Terrororganisationen und kriminellen Netzwerken einsetzen.

Durch die verstärkte internationale Zusammenarbeit und die Umsetzung der genannten Empfehlungen kann Deutschland eine zentrale Rolle im globalen Kampf gegen den Missbrauch von Spionagesoftware einnehmen und gemeinsam mit anderen Akteuren verbindliche Leitlinien sowie effektive Umsetzungsstrategien entwickeln.

DGAP
Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

*Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.*

*Die DGAP ist gefördert vom Auswärtigen Amt aufgrund eines Beschlusses des Deutschen Bundestages.*

**Herausgeber**
Deutsche Gesellschaft für
Auswärtige Politik e.V.

**ISSN** 2749-5542

**Redaktion** Wiebke Ewering

**Layout** Daniel Faller