Bundesamt für Verfassungsschutz

Info Blatt

Proliferation und Sanktionsumgehung

Internationale Sanktionen gegen Staaten wie Russland, Iran oder Nordkorea sind ein wichtiges Instrument der Krisendiplomatie, der Exportkontrolle und des Schutzes von Know-how. Neben Exportbeschränkungen in den Bereichen Finanzen, Transport und Energie stehen insbesondere proliferationsrelevante Güter, konventionelle Waffen und Hochtechnologieprodukte im Fokus der Maßnahmen. Oftmals versuchen sanktionierte Staaten, die Verbote zu umgehen. Dabei binden sie auch ihre Nachrichtendienste ein.

Der Verfassungsschutz ist unter anderem für die Abwehr von Spionage, Sabotage und Proliferation durch ausländische Nachrichtendienste zuständig und steht als vertraulicher Ansprechpartner zur Verfügung.

Grundsätzliche Problematik

- Die Verbreitung chemischer, biologischer, radiologischer und nuklearer Waffen (CBRN-Waffen) stellt ein globales Sicherheitsrisiko dar.
- **Staaten, die nach Massenvernichtungswaffen streben**, sind bei der Entwicklung und Herstellung **auf den Weltmarkt angewiesen**.
- Proliferationsrelevante Staaten wie **Iran, Russland, China, Pakistan oder Nordkorea** versuchen, erforderliche **Güter und Wissen auch in Deutschland zu beschaffen**.
- Im Fokus illegaler Beschaffungsbemühungen stehen **Rüstungsgüter** und andere **Spitzentechnologien**.
- Häufig geht es dabei um **Dual-Use-Güter**, die sowohl für zivile als auch für militärische Zwecke verwendet werden können.
- Es zählt daher zu den **Aufgaben der Verfassungsschutzbehörden**, die illegale Beschaffung von proliferationsrelevanten Produkten und Know-how zu verhindern.

Proliferation ist die Weiterverbreitung von ...

- *Massenvernichtungswaffen (MVW),*
- *Produkten zu deren Herstellung,*
- *erforderlichem Know-how,*
- *Waffenträgersystemen und*
- *Waffensystemen mit vergleichbaren Auswirkungen wie MVW.*

Typische Vorgehensweise bei illegalen Beschaffungsmaßnahmen

1 *Kontaktaufnahme*

- *Der Erstkontakt erfolgt über Tarn- und Beschaffungsfirmen, um das Zielland und auch den Endverbleib zu verschleiern.*
- *Die Firmen befinden sich in Deutschland, Drittstaaten oder auch im Zielland.*
- *Falsche Angaben beim Verwendungszweck verdecken die tatsächliche Endverwendung.*

2 *Zwischenhändler*

- *Hinter der Beschaffung steht oft ein ganzes Firmennetzwerk.*
- *Es erfolgt ein Weiterverkauf innerhalb des Netzwerks.*
- *Die Illegalität der Beschaffung und der eigentliche Akteur können so leichter vertuscht werden.*

3 *Export ins Zielland*

- *Die Güter werden über eine Zwischenstation an den eigentlichen Endverbleibsort überführt (Umgehungslieferung).*
- *Als Zwischenstation wird ein Drittstaat oder unkritisches Unternehmen gewählt, aus dem der Weitertransport ohne größere Hürden möglich ist.*

Typische Vorgehensweise bei illegalen Beschaffungsmaßnahmen

AUSWEICHROUTEN

- Umgehungslieferungen werden weltweit über verschiedenste Staaten ausgeführt.
- Viele dieser Länder sind nicht von Handelssanktionen betroffen, ein Weitertransport in Risikostaaten ist ohne größere Hürden möglich.
- Drittstaaten, die häufig für Umgehungen genutzt werden, sind z. B. die Nachfolgestaaten der Sowjetunion (GUS-Staaten), China, die Türkei oder die Vereinigten Arabischen Emirate.

Deutsche Unternehmen im Fokus

- Illegale Beschaffungsbemühungen ausländischer Staaten mit Blick auf Technologien und Know-how aus Deutschland bewegen sich auf hohem Niveau und nehmen tendenziell zu.
- Damit wächst für deutsche Unternehmen das Risiko, von Proliferationsversuchen und Sanktionsumgehungen betroffen zu sein.
- Eine erhöhte Sensibilität beim Handel mit sanktionierten, militärischen und Dual-Use-Gütern ist daher geboten.

EXKURS: RUSSLAND

Die umfassenden EU-Sanktionen erschweren die Beschaffung von Rüstungsgütern sowie Dual-Use-Produkten für russische Akteure deutlich. Gleichzeitig besteht angesichts des Angriffskrieges gegen die Ukraine erhöhter Bedarf an solchen Waren.

- Bereits vor Februar 2022 waren proliferationsrelevante Beschaffungsaktivitäten Russlands zu verzeichnen, bei denen auch deutsche Unternehmen im Fokus standen.
- Um die geltenden Exportkontrollverfahren zu umgehen, werden die russischen Beschaffungsmethoden ständig weiterentwickelt und optimiert. Hierbei werden auch russische Nachrichtendienste eingebunden.
- Die russischen Aktivitäten konzentrieren sich nicht allein auf proliferationsrelevante Güter, sondern erstrecken sich auf alle sanktionierten Produkte.

EU-SANKTIONEN

- *Seit Februar 2022 hat die EU die Russlandsanktionen deutlich verschärft.*
- *Zentrale Gesetzestexte:*
  EU-VO Nr. 833/2014
  EU-VO Nr. 269/2014
  **In der jeweils gültigen Fassung*

Besonders gefährdete Branchen

- *Werkzeugmaschinenbau*
- *Sicherheit und Verteidigung*
- *Elektrotechnik*
- *Maritime Wirtschaft*
- *Luft- und Raumfahrt*
- *Halbleiterproduktion*
- *Werkstofftechnik*
- *Umwelt- und Energietechnik*
- *Informations- und Kommunikationstechnologie*

Illegale Beschaffungsvorhaben erkennen

- Es bestehen Verbindungen vom betreffenden Unternehmen zu einer sanktionierten Entität.
- Angaben in der Endverbleibserklärung zeigen Auffälligkeiten.
- Die Käuferin oder der Käufer verzichtet auf Einweisungen, Service-Leistungen oder Garantien.
- Es bestehen geschäftliche Verbindungen zu einem proliferationsrelevanten Staat.
- Untypische Versandwege und Bestimmungsorte, z. B. Speditionen als Endpunkt.
- Die Kundin oder der Kunde wünscht eine außergewöhnliche Etikettierung/Kennzeichnung/Beschriftung, um die Ware unverdächtig erscheinen zu lassen.
- Das Unternehmen wurde nach Beginn des russischen Angriffskrieges gegen die Ukraine gegründet.

Haben Sie den Verdacht einer proliferationsrelevanten Anfrage, melden Sie sich bitte beim Bundesamt für Verfassungsschutz unter den angegebenen Kontaktdaten.

Exportkontrolle und Wissenschaft

- Exportvorschriften für Dual-Use- und Rüstungsgüter gelten auch für die Wissenschaft.
- Die Wissenschaftsfreiheit entbindet nicht von der Einhaltung außenwirtschaftsrechtlicher Vorschriften.
- Dies schließt insbesondere auch die Weitergabe von Know-how ein (z. B. im Rahmen von internationalen Forschungskooperationen).
- Nur Grundlagenforschung, die allgemein zugänglich ist und nicht für Dual-Use-Zwecke missbraucht werden kann, ist in der Regel von Ausfuhrbeschränkungen ausgenommen.

Spionage als Mittel der Umgehung bestehender Sanktionen und Exportvorgaben:

- *Ausländische Nachrichtendienste versuchen die bestehenden Restriktionen mit klandestinen Mitteln zu umgehen.*
- *Es besteht die Gefahr, dass nach Deutschland entsandte Gastwissenschaftler und Gastwissenschaftlerinnen Forschungsergebnisse gezielt entwenden.*
- *Teilweise sind sie direkte Mitarbeitende von Militär oder Nachrichtendiensten. Autoritäre Staaten verpflichten aber häufig auch Bürgerinnen und Bürger zur Mitarbeit.*

BEISPIELFALL

Vor wenigen Jahren arbeitete ein chinesischer Gastwissenschaftler für ein norddeutsches Medizintechnikunternehmen. Er war an der Entwicklung von neuartigen antimikrobiellen Oberflächen beteiligt. Nach der Rückkehr des Wissenschaftlers nach China fand man auf der Festplatte seines Arbeitsrechners Fotografien von Forschungsergebnissen und Laboreinrichtungen, die ohne Zustimmung des Arbeitgebers entstanden waren. Als das Unternehmen die Technologie zum Patent anmelden wollte, erfuhr man, dass in China bereits eine entsprechende Anmeldung erfolgt war. Der chinesische Wissenschaftler erhielt nach seiner Rückkehr ins Heimatland eine Professur an einer führenden Universität.

Schutzmaßnahmen

- Führen Sie bei der Auswahl wissenschaftlichen Personals Background-Checks durch. Achten Sie insbesondere auf Verbindungen zu Militär und Verwaltung (gerade bei chinesischen/russischen/iranischen Wissenschaftlern und Wissenschaftlerinnen ist besondere Vorsicht geboten).
- Schließen Sie Vertraulichkeitsvereinbarungen mit den Mitarbeitenden ab.
- Bewerten Sie das Dual-Use-Potenzial von Forschungsprojekten.
- Schulen Sie Ihre Mitarbeitenden im Hinblick auf mögliche Anbahnungsversuche durch ausländische Nachrichtendienste.
- Lassen Sie Vorsicht bei Besuchen von Gruppen oder Einzelpersonen in Ihren Einrichtungen walten. Kontrollieren Sie insbesondere den Zugang zu sensiblen Bereichen. Etablieren Sie auch für Besucherinnen und Besucher Background-Checks.

- *Ausführliche Informationen zur Exportkontrolle in der Wissenschaft finden Sie im Handbuch „Exportkontrolle und Academia“ auf der Webseite des Bundesamtes für Wirtschaft und Ausfuhrkontrolle (BAFA).*
- *In unserem Informationsblatt „Spionage in Wissenschaft und Forschung“ finden Sie tiefergehende Erläuterungen zu Spionagerisiken.*

Weiterführende Informationen

- *Hinweise zu weiteren Risikoindikatoren/illegalen Beschaffungsmaßnahmen finden Sie auf dem „Hinweispapier zur Unterstützung der Unternehmen beim Umgang mit warenverkehrsbezogenen Sanktionen“ auf der Webseite des BMWK.*
- *Auf der Webseite des BAFA erhalten Sie ausführliche Informationen zu länderbezogenen Embargomaßnahmen, Güterlisten und den Anträgen für Ausnahmegenehmigungen.* **www.bafa.de | Außenwirtschaft**
- *Es gilt eine Sorgfaltspflicht für die Einhaltung der bestehenden Vorgaben und Sanktionen (EU-Recht).*
- *Bei vorliegenden Anhaltspunkten für eine Sanktionsumgehung müssen Sie diese dem BAFA mitteilen (Art. 6b EU-VO 833/2024).*

Publikationen

Informationsblätter zum Wirtschaftsschutz

*Die **Informationsblätter zum Wirtschaftsschutz** („Infoblatt") werden vom Bundesamt für Verfassungsschutz herausgegeben. Sie bieten zu verschiedenen Themen Informationen und Hilfestellungen und können über **www.verfassungsschutz.de** kostenlos bezogen werden.*

Sicherheit auf Geschäftsreisen
Die Checkliste gibt Ihnen Hinweise, wie Sie sich vor, auf und nach einer geschäftlichen Auslandsreise vor Spionageaktivitäten schützen können.

Sicherheit auf Geschäftsreisen: China
In diesem Infoblatt finden Sie spezifische Verhaltenshinweise für Ihre Geschäftsreise nach China.

Schutz vor Phishing
Was sich hinter der Angriffsmethode Phishing verbirgt und wie Sie sich davor schützen, können Sie in diesem Infoblatt nachlesen.

Methoden der Spionage: HUMINT
Hier erhalten Sie einen Einblick, wie ausländische Nachrichtendienste spionieren und was Sie selbst dagegen tun können.

Schutz vor Social Engineering –
Hinweise für Leitungsebene und Sicherheitsverantwortliche
Hier finden Sie Informationen, wie ein Social-Engineering-Angriff abläuft und wie Sie Ihr Unternehmen und Ihre Beschäftigten vor Manipulation schützen können.

Schutz vor Social Engineering –
Hinweise für Beschäftigte
In diesem Infoblatt erfahren Sie, wie Sie sich als Beschäftigte im Umgang mit Social-Media, E-Mail und Co. gegen Social-Engineering-Angriffe wappnen können.

Pre-Employment Screening
Mittels Pre-Employment Screening als Teil einer sicherheitsorientierten Personalauswahl tragen Sie dazu bei, sensible Daten und Informationen zu schützen.

Bedrohung durch Innentäter
Dieses Infoblatt bietet Ihnen Informationen über die Motivation und Gefahr von Innentätern und gibt Hinweise zur Etablierung eines Schutzkonzepts.

Spionage in Wissenschaft und Forschung
Das Infoblatt beschreibt Ziele und Folgen von Wissenschaftsspionage und gibt Anregungen und Tipps zum Umgang mit Bedrohungen.

Schutz vor Sabotage
Sabotageschutz umfasst verschiedene Sicherheitsaspekte. Dieses Infoblatt gibt Hinweise zum präventiven Informationsschutz und zur Kommunikation im Ernstfall.

Schutz vor Desinformation
Neben den Wirkungs- und Verbreitungsweisen von Desinformation stehen geeignete Handlungsempfehlungen im Mittelpunkt des Informationsblattes.

Extremismus –
Eine Gefahr für Wirtschaft und Wissenschaft
Extremismus ist eine zunehmende Gefahr für Unternehmen und Forschungseinrichtungen. Das Informationsblatt beleuchtet die entsprechenden Risiken und Schutzmaßnahmen.

Scannen Sie den QR-Code und gelangen Sie direkt zu allen bisher erschienenen Infoblättern.

SCAN ME
Direkt zu den Infoblättern

Wirtschaft & Wissenschaft.
Zukunftssicher.
Verfassungsschutzverbund des Bundes und der Länder

*Das Bundesamt für Verfassungsschutz und die 16 Landesbehörden für Verfassungsschutz bilden gemeinsam den Verfassungsschutzverbund. Auch im Bereich des präventiven Wirtschaftsschutzes arbeitet dieser eng zusammen. Auf diese Weise entsteht ein starkes Netzwerk bis zu Ihnen vor Ort. Eine Übersicht über die Ansprechbarkeiten in den Landesbehörden finden Sie unter **www.verfassungsschutz.de**.*

initiative wirtschaftsschutz
Gemeinsam. Werte. Schützen.

*Die Initiative Wirtschaftsschutz ist ein Zusammenschluss von BfV, BKA, BND und BSI. Auf der Informationsplattform **www.wirtschaftsschutz.info** stellen sie zusammen mit verschiedenen Partnerverbänden ihre Expertise im Bereich Wirtschaftsschutz zur Verfügung. Dazu gehört das Thema Cyberkriminalität genauso wie Wirtschafts- und Wissenschaftsspionage oder das Thema IT-Sicherheit.*

SCAN ME

Ihr direkter Kontakt zum Wirtschaftsschutz

SCAN ME

Bundesamt für Verfassungsschutz
Bereich Prävention (Wirtschafts- und Wissenschaftsschutz)
030 18792-3322
wirtschaftsschutz@bfv.bund.de

Ihr direkter Kontakt zur Proliferationsabwehr

Bundesamt für Verfassungsschutz
Bereich Proliferation
counter-proliferation@bfv.bund.de