Bundeskriminalamt

BKA

ST14 Gefährdung –
Zusammenarbeit mit der Wirtschaft
ST14@bka.bund.de

Information für die Wirtschaft

05.06.2025

Es wird darauf hingewiesen, dass die Informationen ausschließlich zum Zwecke der internen Verwendung übermittelt werden. Die (auch auszugsweise) Weitergabe der Informationen an Dritte sowie deren Veröffentlichung sind ohne Zustimmung des Bundeskriminalamtes nicht gestattet.

Sensibilisierung zur veränderten Gefährdungslage von Rüstungsunternehmen, Zulieferern und anderen Vertragspartnern

1. Anlass

Vor dem Hintergrund anhaltender geopolitischer Spannungen – insbesondere im Kontext des russischen Angriffskrieges gegen die Ukraine – sowie wachsender sicherheitspolitischer Herausforderungen geraten deutsche Rüstungsunternehmen zunehmend in den Fokus medialer Berichterstattungen und politischer Diskussionen. Mit der gestiegenen Sichtbarkeit entsprechender Unternehmen und einem gewachsenen Bewusstsein für die strategische Bedeutung einer nationalen Rüstungsindustrie haben sich die Rahmenbedingungen für die Bewertung der Gefährdungslage von Rüstungsunternehmen, deren Zulieferern und anderen Vertragspartnern verändert.

Diese veränderte Gefährdungslage, eine zunehmende Anzahl gefährdungsrelevanter Hinweise sowie ein Anstieg politisch motivierter Straftaten sind der Anlass für die nachfolgende Sensibilisierung im Hinblick auf potentielle Gefährdungen der Rüstungsindustrie aus den unterschiedlichen Phänomenbereichen der Politisch motivierten Kriminalität (PMK).

2. Gefährdungslage

Dem Bundeskriminalamt (BKA) liegen derzeit keine Erkenntnisse zu einer konkreten Gefährdung bestimmter Rüstungsunternehmen vor. Gleichwohl ist im Zusammenhang mit der veränderten Bedeutung der Rüstungsindustrie seit Beginn des russischen Angriffskrieges gegen die Ukraine sowie der Eskalation weiterer internationaler Krisen- und Konfliktlagen ein quantitativer und qualitativer Anstieg gefährdungsrelevanter Hinweise und Sachverhalte mit Bezug zu deutschen Rüstungsunternehmen zu verzeichnen.

Im Deliktsbereich **Spionage/Staatsterrorismus** stehen neben militärischen Liegenschaften und dem Transport militärischer Güter in die Ukraine grundsätzlich auch die hiermit verknüpfte logistische Infrastruktur in Deutschland und deutsche Rüstungsunternehmen im Fokus nachrichtendienstlich gesteuerter Ausspähungs- und Sabotagebemühungen.

Spätestens seit Beginn des russischen Angriffskrieges gegen die Ukraine und der zunehmend antagonistischen Positionierung Russlands gegen Deutschland und andere (europäische) Unterstützer der Ukraine ist anzunehmen, dass russische Nachrichtendienste versuchen, die Produktion, Lieferketten und Geschäftsabläufe von deutschen Rüstungsunternehmen auszuspähen oder zu sabotieren. Dies kann unter Umständen auch nachrichtendienstliche Operationen gegen besonders exponierte Personen umfassen.

In diesem Zusammenhang ist beispielsweise auch der Hinweis einzuordnen, wonach der Vorstandsvorsitzende eines führenden Rüstungsunternehmens Ziel russischer Aufklärungsmaßnahmen gewesen sein soll und die Möglichkeit eines Anschlages bestehe.[1]
Vor dem Hintergrund der grundsätzlich anzunehmenden positionsimmanenten Verantwortung für Rüstungsproduktion, Waffenlieferungen an die Ukraine sowie dem geplanten Aufbau von Wartungs- und Logistikinfrastrukturen in der Ukraine, ist einzukalkulieren, dass das Führungspersonal großer Rüstungsunternehmen in den Fokus russischer Nachrichtendienste geraten kann.
Einzelfallbezogen sind somit Anschlagsvorhaben gegen besonders exponierte Führungspersonen von Rüstungsunternehmen und komplexe Sabotageoperationen, auch unter Inkaufnahme von Personenschäden, grundsätzlich in Betracht zu ziehen. In diesem Zusammenhang ist die Feststellung unkonventioneller Brandvorrichtungen in Luftfrachtsendungen zu nennen, die mutmaßlich im Zusammenhang mit Sabotagehandlungen gegen logistische Einrichtungen zur Unterstützung der Ukraine steht.

Allerdings ist festzuhalten, dass russische Nachrichtendienste grundsätzlich unter Abwägung der geopolitischen Reaktionen und Eskalationsrisiken handeln.

Dementsprechend ist davon auszugehen, dass russische nachrichtendienstliche Operationen in der Regel so konzipiert werden, dass sie unterhalb der Schwelle einer offensichtlichen staatlichen Aggression bleiben oder Russland eine Verantwortungsübernahme abstreiten kann, um direkte Konsequenzen zu vermeiden. Dies wird unter anderem durch den Einsatz von Zwischenakteuren, sogenannten „Proxys“ oder durch Aktivitäten im Cyberraum erreicht.

Vor diesem Hintergrund wird die Gefährdungslage im Bereich der Sabotage seit Beginn des russischen Angriffskrieges gegen die Ukraine hauptsächlich durch die Rekrutierung und den Einsatz von „Low-Level-Agents“ geprägt.[2]

---

[1] Siehe BKA – Schreiben an die Wirtschaft „Gefährdungseinschätzung zu deutschen Wirtschaftsunternehmen im Kontext möglicher Sabotagehandlungen im Auftrag Russlands“ vom 25.07.2024.
[2] Siehe BKA – Schreiben an die Wirtschaft „Sensibilisierungsschreiben im Kontext potenzieller russischer Ausspähung und Sabotage“ vom 19.12.2024.

Als „Low-Level-Agents“ werden solche Personen bezeichnet, die im Auftrag oder im Interesse eines ausländischen Nachrichtendienstes, im vorliegenden Kontext insbesondere für russische Nachrichtendienste, tätig sind, ohne dabei selbst über eine nachrichtendienstliche Ausbildung zu verfügen oder in klassische nachrichtendienstliche Führungs- und Steuerungsstrukturen eingebunden zu sein.

Der festgestellte Einsatz von „Low-Level-Agents“ umfasst die Mitwirkung an Desinformationskampagnen, die Aufklärung von Waffenlieferungen und deren Logistik sowie vorbereitende Maßnahmen bzw. die Durchführung von Sabotageakten gegen diese Unterstützungsleistungen und damit verbundene Infrastrukturen.

Wenngleich angenommen werden kann, dass die Störung oder Unterbindung westlicher Waffenlieferungen an die Ukraine weiterhin das vorrangige Ziel russischer Nachrichtendienste darstellt, verdeutlichen die mutmaßliche Sabotage an Kriegsschiffen der Deutschen Marine im Rahmen von Werftaufenthalten in rüstungsindustriellen Anlagen sowie die (versuchte) Sabotage an Bahnstrecken im Zusammenhang mit dem Transport von Waffenlieferungen in Polen und der Brandanschlag auf eine Lagerhalle in London/GBR, dass insbesondere objektbezogene Delikte wie Sachbeschädigungen, Brandstiftungsdelikte und gefährliche Eingriffe in den Bahn-, Luft-, Schiffs- und Straßenverkehr einkalkuliert werden müssen.

Zudem ist davon auszugehen, dass die aktuell festgestellten Ausspähungshandlungen bzw. entsprechende Verdachtsfälle, der Informationsgewinnung zu Sicherheitskonzepten, Zugangsmöglichkeiten und organisatorischen Abläufen von Einrichtungen der Kritischen Infrastruktur (KRITIS) und der Rüstungsindustrie dienen. Die hierdurch gewonnenen Erkenntnisse könnten für den Zeitpunkt einer Lageverschärfung vorgehalten und zur Vorbereitung komplexer und koordinierter Operationen mit hohem Schadensausmaß genutzt werden.

Zu den Hintergründen der vermehrten **Drohnensichtungen** über KRITIS und Rüstungsunternehmen seit Beginn des russischen Angriffskrieges gegen die Ukraine lassen sich derzeit, insbesondere aufgrund der Heterogenität der Sichtungen, keine belastbaren oder allgemeingültigen Aussagen ableiten.
Erkenntnisse bzw. Nachweise, dass die Überflüge unmittelbar der Vorbereitung konkret bevorstehender Sabotagehandlungen gegen Rüstungsunternehmen dienen oder in der Vergangenheit gedient haben, liegen bislang nicht vor. Vor dem Hintergrund einer besonderen sicherheitspolitischen Bedeutung der Rüstungsindustrie und dem bestehenden Aufklärungsinteresse nachrichtendienstlicher Akteure muss die Nutzung von Drohnen zur Ausspähung oder als unmittelbares Tatmittel in Sabotagehandlungen jedoch grundsätzlich einkalkuliert werden.

Rüstungsunternehmen in Deutschland und Europa stehen zudem im besonderen Fokus staatlich gesteuerter **Cyberspionageaktivitäten**, insbesondere durch russische und chinesische Nachrichtendienste. Ziel dieser Operationen ist regelmäßig der Zugriff auf sensible Informationen zu Forschungsvorhaben, Produktionstechnologien, Exportprojekten sowie militärisch relevante Systemarchitekturen. Auch Erkenntnisse über Kooperationen, Lieferketten oder logistische Planungen, insbesondere im Kontext von Unterstützungsleistungen für die Ukraine, sind von erheblichem nachrichtendienstlichem Interesse.

Seit Beginn des Angriffskrieges Russlands gegen die Ukraine konnte eine Vielzahl von Cyberangriffen festgestellt werden, die sich u. a. gegen Rüstungsunternehmen und unterstützende Produktions- und Logistikunternehmen der Bundeswehr richteten. So wurden beispielsweise Phishing-Angriffe auf einen langjährigen Vertragspartner der Bundeswehr im Bereich der Instandsetzung von Militärfahrzeugen sowie auf ein Rüstungsunternehmen aus dem Bereich der Entwicklung von Flugkörpersystemen festgestellt. Auch wenn eine eindeutige Attribution des verantwortlichen Cyberakteurs bislang nicht möglich ist, lassen die verwendeten Techniken und Vorgehensweisen auf eine russische Urheberschaft schließen.

Zusammenfassend ist in Bezug auf Spionage- und Sabotagehandlungen somit eine erhöhte abstrakte Gefährdung von Rüstungsunternehmen und deren Zulieferer zu konstatieren.

Neben der Gefährdung durch staatlich gesteuerte oder veranlasste Spionage bzw. Sabotage zum Nachteil von Rüstungsunternehmen haben zunehmende internationale Krisen- und Konfliktlagen zu einem Anstieg **Politisch motivierter Kriminalität (PMK)** gegen Rüstungsunternehmen geführt. In diesem Zusammenhang sind insbesondere die Phänomenbereiche PMK -ausländische Ideologie- und PMK -links- einschlägig.

- In Bezug auf den **Phänomenbereich PMK -ausländische Ideologie-** haben insbesondere der anhaltende Nahostkonflikt infolge der terroristischen Angriffe der HAMAS auf Israel am 07.10.2023 sowie die türkischen Militäroperationen gegen kurdische Kräfte unmittelbare Auswirkungen auf den gesellschaftlichen Diskurs in Deutschland und führen zu einer verstärkten Emotionalisierung und Mobilisierung.
  Vor diesem Hintergrund nahmen zuletzt pro-palästinensische Gruppierungen Geschäftstätigkeiten sowie Investitionen in Israel und wirtschaftliche Kooperationen mit israelischen Firmen zum Anlass, um Boykottkampagnen gegen deutsche Unternehmen zu initiieren.

  Im Rahmen des entsprechenden Versammlungs- und Demonstrationsgeschehens sowie von Boykottkampagnen können sich Störaktionen pro-palästinensischer Personen und Gruppie-

rungen auch gegen Rüstungsunternehmen und deren Zulieferer oder andere Vertragspartner (Logistik- und Finanzdienstleister) richten.
Mittels überwiegend niedrigschwelliger objektbezogener Straftaten (Hausfriedensbrüche und Sachbeschädigungen) soll eine Bedrohungskulisse aufgebaut werden, die auf eine Beeinträchtigung der Geschäftstätigkeit israelischer (Rüstungs-)Unternehmen in Deutschland abzielt, um letztendlich die deutsch-israelischen Wirtschaftsbeziehungen zu unterbinden.

Angriffe gegen Personen der betroffenen Unternehmen sind grundsätzlich eher auszuschließen. Im Kontext einer (zufälligen) direkten Konfrontation mit Personen, die aus Sicht propalästinensischer Aktivisten eine Verantwortung für die Situation im Nahen Osten aufweisen, sind allerdings Beleidigungen, Bedrohungen und ggf. sogar situationsbedingte körperliche Übergriffe in Betracht zu ziehen.

Darüber hinaus sind im Kontext türkischer Militäreinsätze gegen die kurdische Freiheitsbewegung oder dem Export von Rüstungsgütern in die Türkei vereinzelte Kampagnenaufrufe aus der kurdischen Diaspora und der linken Szene sowie niedrigschwellige Straftaten gegen Rüstungsunternehmen und deren Geschäftspartner feststellbar.

- Seit Beginn des russischen Angriffskrieges gegen die Ukraine hat das Themenfeld „Antimilitarismus“ innerhalb des **Phänomenbereichs der PMK -links**- deutlich an Bedeutung gewonnen. Diesbezüglich richtet sich der Protest vor allem gegen Waffenlieferungen an die Ukraine sowie gegen die Aufrüstung der Bundeswehr. Auch Entwicklungen im Nahostkonflikt haben zuletzt entsprechende Tatdynamiken ausgelöst.
  Dies zeigt sich unter anderem in einer zunehmenden Anzahl an Aufrufen zu (strafrechtlich relevanten) Aktionen gegen die Rüstungsindustrie sowie gegen Unternehmen, die unmittelbar oder mittelbar in sicherheits- und verteidigungspolitische Strukturen eingebunden sind.

  Auf verschiedenen Plattformen der linken Szene wurden wiederholt öffentlichkeitswirksame Mobilisierungen und Aufrufe zu Sabotage, Sachbeschädigungen und Blockadeaktionen dokumentiert. Beispielhaft kann hier auf eine Informationssammlung und Handlungsanleitung zur Sabotage auf der Plattform „ruestungsindustrie.noblogs.org.“ mit dem Titel „Eine Einführung in die Kartographie lokaler Rüstungsindustrie und ihrer sensiblen Punkte – Rüstungsindustrie angreifen“ verwiesen werden.[3]

[3] Siehe BKA – Schreiben an die Wirtschaft „Gefährdungseinschätzung anlässlich eines Beitrags auf der Plattform „ruestungsindustrie.noblogs.org“ mit Anregungen zur Informationsbeschaffung“ vom 01.07.2022.

In diesem Zusammenhang wird ergänzend auf die bereits bekannte Mitmachkampagne mit der Bezeichnung „switch-off“ verwiesen.[4] Auch unter diesem Rubrum wird zu Straftaten u. a. gegen Rüstungsunternehmen aufgerufen.

Grundsätzlich gehören Brandstiftungsdelikte aufgrund ihrer oft erheblichen Wirkung sowie der vergleichsweise einfachen Tatausführung, verbunden mit einem geringen Risiko entdeckt und gefasst zu werden, zu einer effektiven und daher häufig genutzten Strategie militanter Linksextremisten. Insbesondere Kraftfahrzeuge stellen in diesem Kontext ein häufig gewähltes Ziel dar.

Brandstiftungen dürften aufgrund der oben erwähnten günstigen Tatumstände auch in Zukunft eine häufig gewählte Aktionsform des militanten Linksextremismus bleiben.

Zusammenfassend ist festzustellen, dass – insbesondere in Abhängigkeit von der geopolitischen Lage sowie den korrespondierenden politischen Diskussionen – mit einer Fortführung von Aktionen bzw. weiteren objektbezogenen Straftaten (Sachbeschädigungen und Brandstiftungsdelikte) von Akteuren aus dem Bereich der PMK -links- zum Nachteil von Rüstungsunternehmen, aber auch gegen Unternehmen und Institutionen, die lediglich mittelbar in Zusammenhang mit der Rüstungsindustrie stehen, zu rechnen ist.

3. Fazit

Insgesamt ist von einer abstrakten Gefährdungslage für deutsche Rüstungsunternehmen sowie deren Zulieferer auszugehen. Einzelfallbezogen sind Verschärfungen der Gefährdungslage einzukalkulieren. So ist in Bezug auf den Bereich der Spionage und Sabotage mitunter eine erhöhte abstrakte Gefährdung festzustellen. Diese wird insbesondere durch das anhaltende Aufklärungsinteresse und Sabotagevorhaben russischer Nachrichtendienste bedingt. Entsprechende Operationen richten sich maßgeblich gegen Unternehmen, die an Waffenlieferungen oder anderen Unterstützungsleistungen für die Ukraine beteiligt sind.

Angesichts der sicherheitspolitischen Relevanz der Rüstungsindustrie und der erhöhten öffentlichen Aufmerksamkeit für verteidigungspolitische Entscheidungen ist davon auszugehen, dass Rüstungsunternehmen auch künftig im Zielspektrum unterschiedlicher politisch motivierter Akteure bleiben.

[4] Siehe BKA - Schreiben an die Wirtschaft „Sensibilisierung anlässlich linksextremistisch motivierter Brandstiftungsdelikte im Kontext der „switch-off“-Kampagne“ vom 25.03.2024.