

SWP-Aktuell

NR. 50 OKTOBER 2026

Nordkorea – Europas strategischer Blind Spot

Die zunehmende sicherheitspolitische Bedrohung durch die DVRK

Eric J. Ballbach

Lange galt Nordkorea vor allem als regionales Sicherheitsproblem in Ostasien. Mittlerweile jedoch ist das Regime in Pjöngjang zu einem Akteur geworden, der überregionale Konflikte wie Russlands Krieg gegen die Ukraine aktiv beeinflusst und dessen aggressive Cyberaktivitäten sich unmittelbar auf Europas Sicherheit auswirken. Die europäische Nordkorea-Politik indes orientiert sich vielfach an strategischen Annahmen, die der veränderten Rolle des Landes nicht mehr gerecht werden. Europa muss daher die von Nordkorea ausgehenden Bedrohungen neu bewerten – und seine Antworten darauf entsprechend anpassen. Denn es könnte sich als Fehler mit hohen politischen Kosten erweisen, diese Gefahr zu ignorieren.

Russlands Krieg gegen die Ukraine hat nicht nur die Illusion eines stabilen Sicherheitsraums auf dem Kontinent zerstört, sondern auch die politische Prioritätenordnung der europäischen Staaten grundlegend verändert. Verteidigung, Abschreckung, industrielle Resilienz und die militärische Unterstützung der Ukraine stehen heute im Zentrum von Europas strategischer Planung. Diese Fokussierung ist angesichts der geopolitischen Herausforderungen notwendig. Sie birgt aber auch die Gefahr, dass wachsende Risiken jenseits von Russland keine angemessene Aufmerksamkeit erfahren. Das gilt nicht zuletzt für die sicherheitspolitische Bedrohung Europas durch Nordkorea.

Denn die Demokratische Volksrepublik Korea (DVRK) stellt längst nicht mehr nur ein Risiko für den Indo-Pazifik dar. Das

Land ist heute ein aktiver Player in überregionalen Konflikten wie dem russischen Krieg gegen die Ukraine, ein aggressiver Cyberakteur, der auch europäische Ziele angreift, und eine ernste Gefahr für das nukleare Nichtverbreitungsregime. Nordkorea ist als sicherheitspolitischer Akteur zu begreifen, dessen vertiefte militärische Kooperation mit Russland und dessen offensive Cyberaktivitäten unmittelbare Auswirkungen auf die Sicherheit Europas haben.

Vertiefte Kooperation zwischen Nordkorea und Russland

Die Beziehungen zwischen Russland und Nordkorea haben sich seit Beginn der russischen Vollinvasion in der Ukraine 2022 von



einem politischen Zweckbündnis zu einer umfassenden strategischen Partnerschaft entwickelt. Beide Staaten profitieren davon politisch, wirtschaftlich und militärisch.

Pjöngjang unterstützte den Krieg Russlands zunächst diplomatisch und stimmte im März 2022 als eines von nur fünf Ländern gegen die Resolution der UN-Generalversammlung, mit der Moskaus Aggression gegen die Ukraine verurteilt wurde. Früh erkannte Nordkorea auch die von Russland besetzten Gebiete Donezk und Luhansk als unabhängige »Volksrepubliken« an. Mit dem wachsenden Bedarf Russlands an Munition und Waffen intensivierten beide Staaten ihre hochrangigen Kontakte. Dies begann im Juli 2023, als mit Sergei Schoigu erstmals seit 1991 ein russischer Verteidigungsminister in Pjöngjang eintraf, und gipfelte im September 2023 in einem Treffen der beiden Machthaber Kim Jong Un und Wladimir Putin in Russland. Im Juni 2024 reiste Putin nach Pjöngjang – der erste Besuch eines russischen Staatschefs in der DVRK seit dem Jahr 2000. Während dieser Visite unterzeichneten beide Seiten den Vertrag über eine umfassende strategische Partnerschaft, der unter anderem auch gegenseitige militärische Unterstützung im Falle einer bewaffneten Aggression vorsieht.

Die militärische Zusammenarbeit bildet inzwischen den Kern der bilateralen Beziehungen. Nach Angaben des südkoreanischen Militärgeheimdienstes lieferte Nordkorea zwischen August 2023 und Februar 2026 rund 33.000 Container nach Russland. Je nach Schätzung unterschiedlicher Dienste sollen sie zwischen 11 Millionen und 15 Millionen 152-mm-Artilleriegeschosse enthalten haben, zudem Mehrfachraketenwerfer, ballistische Kurzstreckenraketen sowie Lenkflugkörper und Granatwerfer zur Panzerabwehr. Ferner hat Nordkorea seit Oktober 2024 offenbar bis zu 12.000 Soldaten nach Russland entsandt, vor allem in das Gebiet Kursk, sowie zusätzlich etwa 1.000 Pioniere für Minenräumungsmaßnahmen und 5.000 Arbeiter zum Wiederaufbau von Infrastruktur. Im August 2026 berichtete der ukrainische Präsident Wolo-

dymyr Selenskyj von Informationen, nach denen entschieden worden sei, weitere 30.000 bis 50.000 nordkoreanische Soldaten auf russischem Territorium einzusetzen. Die Angaben sind bisher jedoch nicht unabhängig bestätigt.

Im Gegenzug unterstützt Russland die DVRK diplomatisch, etwa mit dem Ziel, das internationale Sanktionsregime gegen Pjöngjang zu schwächen. So hat Moskau seit 2022 (teilweise gemeinsam mit China) im UN-Sicherheitsrat gegen alle amerikanischen Resolutionsentwürfe ein Veto eingelegt, die zusätzliche Sanktionen gegen die DVRK vorsahen. Im März 2024 verhinderte Russland, dass das Mandat des Expertengremiums zur Überwachung der Sanktionen gegen Nordkorea verlängert wurde, wodurch der entsprechende Mechanismus innerhalb des Sicherheitsrats faktisch abgeschafft wurde. Darüber hinaus haben hochrangige russische Politiker wie etwa Sergei Lawrow wiederholt das souveräne Recht der DVRK auf die Entwicklung atomarer Verteidigungsfähigkeiten betont und Forderungen nach einer Denuklearisierung des Landes zurückgewiesen.

Zugleich wurden Handel, Energielieferungen und Personenverkehr zwischen beiden Ländern ausgeweitet. Besonders bedeutsam sind jedoch die Einnahmen Pjöngjangs aus Waffenexporten und der Entsendung nordkoreanischer Arbeitskräfte und Soldaten, die offenbar Devisenerträge in Milliardenhöhe generieren. Laut einem Bericht des Korea Institute for Defence Analyses in Seoul beliefen sich die finanziellen Erträge für Nordkorea bis April 2025 allein aus der Lieferung von Munition und Waffen an Russland auf bis zu 19,2 Milliarden US-Dollar.

Ebenso wichtig sind jedoch die militärischen und technologischen Gewinne. Der Krieg in der Ukraine dient Nordkorea als Testfeld für Waffen und Soldaten; dort lassen sich Erfahrungen im modernen Gefecht sammeln, insbesondere was Drohnen und elektronische Kriegführung, aber auch den Umgang mit westlicher Ausrüstung betrifft. Die russische Nachfrage nach Waffen treibt die nordkoreanischen Exporte an und trägt

dazu bei, die Schwer- und Chemieindustrie des Landes auszubauen. Gleichzeitig unterstützt offenbar Moskau seinerseits die DVRK mit moderner Militärtechnologie. Berichten zufolge lieferte Russland seinem Partner unter anderem Antriebssysteme für ein sich in Entwicklung befindliches strategisches U-Boot mit nuklearem Antrieb, ebenso moderne Flugabwehrraketen und Systeme zur elektronischen Kriegführung. Moskau unterstützt zudem das Weltraumprogramm Pjöngjangs. Darüber hinaus soll russisches Know-how in die Weiterentwicklung von Nordkoreas neuesten Interkontinentalraketen (wie etwa der Hwasong-20) geflossen sein, vor allem in den Bereichen Wiedereintrittskörper, Feststofftriebwerke und hochpräzise Raketenlenkung. Dies trägt dazu bei, die militärischen Fähigkeiten der DVRK weiter zu modernisieren, und erhöht zugleich die Attraktivität nordkoreanischer Rüstungsgüter auf dem internationalen Markt.

Wichtig ist, dass Moskau und Pjöngjang die Kooperation offenbar nicht bloß als kriegsbedingtes Arrangement betrachten. So wurde im April 2026 bei einem Besuch des russischen Verteidigungsministers Andrei Beloussow in der DVRK vereinbart, die militärische Kooperation auf eine »stabile, langfristige Grundlage« zu stellen und noch 2026 einen Kooperationsplan für die Jahre 2027 – 2031 zu unterzeichnen.

Implikationen für Europas Sicherheit

Die Kooperation zwischen Russland und der DVRK ist nicht nur der bislang deutlichste Ausdruck einer zunehmenden sicherheitspolitischen Verflechtung zwischen Europa und dem Indo-Pazifik. Hier wird die strategische Lage des Kontinents auch am unmittelbarsten durch Pjöngjangs Vorgehen tangiert. Denn indem Nordkorea den russischen Krieg gegen die Ukraine politisch und militärisch unterstützt, stabilisiert es Moskaus Kriegsfähigkeit und trägt zur anhaltenden Belastung der europäischen Sicherheitsordnung bei. Zwar ist Nordkoreas Hilfe nicht kriegsentscheidend, doch haben vor

allem seine umfangreichen Munitionslieferungen einen substantiellen Anteil daran, dass Russland seine offensiven Operationen gegen die Ukraine fortsetzen konnte. Insbesondere nachdem die russischen Munitionsbestände im Jahr 2023 deutlich geschwunden waren, spielte die nordkoreanische Unterstützung eine entscheidende Rolle dabei, die Kampfkraft des Landes kurz- und mittelfristig aufrechtzuerhalten. Pjöngjang verringerte damit nicht nur den Druck auf Russlands Rüstungsindustrie, sondern erweiterte auch dessen Fähigkeit zur intensiven Kriegführung. 2025 berichtete der damalige Leiter des ukrainischen Militärgeheimdienstes, Kyrylo Budanow, dass zeitweise bis zu 40 Prozent der Munition, die Russland im Krieg gegen die Ukraine einsetze, aus Nordkorea stammten.

Umgekehrt trägt die russische Unterstützung für Nordkorea zu dessen beschleunigter militärischer Modernisierung bei, was nicht nur die Stabilität im Indo-Pazifik weiter untergräbt, sondern auch die internationale Nichtverbreitungsordnung zusätzlich schwächt. Dass nordkoreanische Waffen im Krieg gegen die Ukraine eingesetzt werden, dürfte die Attraktivität dieser Systeme weiter steigern – und das Risiko einer Proliferation militärischer Technologien erhöhen.

Schließlich unterminiert die Zusammenarbeit zwischen Russland und Nordkorea auch die Wirksamkeit internationaler Sanktionen. Beide Staaten kooperieren zunehmend bei der Umgehung bestehender Sanktionsregime, etwa indem sie alternative Handels- und Finanzkanäle schaffen. Damit wird nicht nur der wirtschaftliche Druck auf Russland und Nordkorea reduziert; zugleich verliert das Sanktionsinstrument insgesamt an Glaubwürdigkeit und (Abschreckungs-)Wirkung.

Zunehmende Cyberbedrohung durch Nordkorea

Eine unmittelbare Bedrohung für Europa, die oft noch immer unterschätzt wird, bilden auch nordkoreanische Cyberoperationen. Die Ursprünge von Pjöngjangs Cyber-

programm lassen sich zurückverfolgen bis in die Zeit von Machthaber Kim Jong Il (1994 – 2011). Unter seinem Nachfolger Kim Jong Un wurde die Cyberkriegführung zu einer »zentralen Säule« der nordkoreanischen Militärstrategie (neben dem Atomwaffenarsenal und den Interkontinentalraketen); die Fähigkeiten wurden entsprechend ausgeweitet.

Pjöngjangs Cyberprogramm: Ein Überblick

Unter Kim Jong Un haben sich die Cyberfähigkeiten der DVRK zu einem umfassenden nationalen Projekt entwickelt, das in seiner Professionalität durchaus mit den Cyberprogrammen Chinas und Russlands zu vergleichen ist. Vielen politischen Entscheidungsträgern in Europa fällt es jedoch nach wie vor schwer zu akzeptieren, dass Nordkorea auf diesem Feld zu einer »gleichberechtigten Nation« und zu einer der fähigsten, aktivsten und aggressivsten Mächte weltweit geworden ist.

Nordkoreanische »Advanced Persistent Threat« (APT)-Gruppen sind für hochkarätige cybergestützte Spionage, für Cyberangriffe auf Infrastrukturen und Lieferketten sowie insbesondere für Finanzdiebstahl in einem Ausmaß verantwortlich, wie es von keinem anderen Land bekannt ist. Vorangetrieben wurde dieser Aufschwung durch ein strategisches Programm zur Förderung einheimischer Talente, durch die Unterstützung internationaler Partner, vor allem Russlands und Chinas, und den Aufbau eines globalen Netzwerks von IT-Fachkräften im Ausland. Das Multilateral Sanctions Monitoring Team (MSMT) – ein im Oktober 2024 geschaffener Mechanismus, der die Umsetzung der UN-Sanktionen gegen die DVRK überwacht – geht davon aus, dass derzeit zwischen 1.000 und 2.000 nordkoreanische IT-Fachkräfte im Ausland stationiert sind. Die Mehrheit davon (zwischen 1.000 und 1.500) soll sich in China aufhalten. Die am MSMT beteiligten Staaten haben jedoch Pläne Pjöngjangs aufgedeckt, bis zu 40.000 zusätzliche Arbeitskräfte nach Russland zu entsenden, darunter weitere IT-

Spezialisten. Tatsächlich gibt es Anzeichen, dass sich die russisch-nordkoreanische Zusammenarbeit auch im Cyberspace intensiviert; dabei sollen Verbindungen zwischen nordkoreanischen APT-Gruppen und dem russischsprachigen Cybercrime-Ökosystem bestehen.

Der Militär- und Parteiapparat der DVRK stellt Ressourcen bereit, bildet spezialisierte Einheiten aus und setzt diese ein, um Cyberkampagnen durchzuführen. So ist in Nordkorea ein leistungsfähiges Netzwerk von APT-Gruppen entstanden, die direkt staatlichen Stellen wie dem Generalbüro für Aufklärung (RGB) und dem Ministerium für Staatssicherheit unterstehen – und die für zahlreiche Cyberoperationen im Ausland verantwortlich sind. Zwar gibt es keine offiziellen Daten zu den verschiedenen APT-Gruppen, doch Schätzungen zufolge verfügt die »Cyberarmee« der DVRK über mehr als 6.000 Spezialisten. Weiter gestärkt wurden deren Fähigkeiten durch ein hohes Maß an Koordination zwischen den verschiedenen Zweigen des nordkoreanischen Cyberapparats – auch beim Austausch von Ressourcen – und durch die Integration neuer Technologien, insbesondere der künstlichen Intelligenz (KI).

Fortschritte im Bereich der generativen KI haben es nordkoreanischen Cyberakteuren etwa ermöglicht, bestimmte Teile ihrer Operationen effizienter und skalierbarer durchzuführen. Auf großen Sprachmodellen (LLM) basierende Anwendungen werden auf vielfältige Weise eingesetzt – so zur Erstellung und Personalisierung von Phishing-Inhalten, zur Recherche und Aufklärung, zur Erstellung gefälschter Biografien und Identitäten sowie unterstützend bei der Entwicklung und Anpassung von Schadcodes.

Bestehende Sanktionen gegen Nordkorea werden international nur lückenhaft überwacht und durchgesetzt. Dies hat es Pjöngjang ermöglicht, Cyberoperationen gezielt zur Umgehung von Sanktionen, zur Generierung illegaler Einnahmen und zur Beschaffung sensibler Informationen einzusetzen und dadurch seine Cyberfähigkeiten weiter auszubauen. Deshalb stellt das Regime von Kim Jong Un nicht mehr nur

aufgrund seines Atomwaffenarsenals eine Bedrohung dar, sondern auch wegen seiner Aktivitäten im Cyberraum.

Europa als Ziel nordkoreanischer Cyberoperationen

Waren Nordkoreas Cyberoperationen zunächst vor allem gegen Südkorea und die USA gerichtet, so haben sie sich mehr und mehr zu einem globalen Unternehmen entwickelt. Dabei gerät auch Europa verstärkt in den Fokus. In ihrer »Threat Landscape 2025« stuft ENISA, die Agentur der EU für Cybersicherheit, Nordkorea nach Russland und China als drittgrößte Bedrohung für Europa ein, was entsprechende Angriffe betrifft. Die Aktivitäten mit Verbindungen zur DVRK richten sich dabei insbesondere gegen private Unternehmen in Europa, mit einem Schwerpunkt auf Personalwesen, Finanzdienstleistungen (einschließlich Kryptowährungen), Verteidigung, Luft- und Raumfahrt, Medien, Gesundheit und Energie; betroffen sind aber auch staatliche Stellen und regierungsnahe Forschungseinrichtungen.

Dabei lassen sich Nordkoreas Cyberaktivitäten in Europa drei Hauptkategorien zuordnen: finanziell motivierte Angriffe, wie etwa Diebstahl von Kryptowährungen, betrügerische IT-Arbeitsprogramme sowie Spionage.

Finanziell orientierte Operationen. Ab 2017 intensivierte Nordkorea jene Cyberoperationen, die dazu dienen, finanzielle Einnahmen zu generieren. Dies fiel in eine Phase erheblich verschärfter internationaler Sanktionen und zunehmenden wirtschaftlichen Drucks auf das Land. Der Diebstahl von Kryptowährungen wurde nun zu einer besonders wichtigen Einnahmequelle für das Regime. Damals befand sich der Markt für virtuelle Vermögenswerte noch in einer frühen Entwicklungsphase; er war durch erhebliche regulatorische und sicherheitsbezogene Defizite gekennzeichnet, die es erleichterten, Schwachstellen auszunutzen. Nach 2020 — dem Jahr, in dem Nordkoreas Außenhandel durch den Covid-19-beding-

ten Lockdown fast vollständig zum Erliegen kam — stieg die Zahl finanziell motivierter Cyberoperationen des Landes weiter an. Wie der Analyst Perry Choi formulierte, entwickelte sich die DVRK in den frühen 2020er Jahren zu einem »Cyber-Raubzugsunternehmen industrieller Größenordnung«.

Nordkoreanische Akteure beschränkten sich zunächst darauf, zentralisierte Kryptobörsen anzugreifen. Später weiteten sie ihre Angriffe zunehmend auf verschiedene Komponenten des Blockchain-Ökosystems aus, darunter Cross-Chain-Bridges, DeFi (Decentralized Finance)-Protokolle sowie die IT- und Zugangs-Infrastruktur von Unternehmen und deren Beschäftigten. Mit Nordkorea verbundene APT-Gruppen stahlen nicht nur Kryptowährungen von Einzelpersonen und Beschäftigten entsprechender Firmen. In den vergangenen Jahren gelang es ihnen auch, zahlreiche Kryptowährungsbörsen und andere Unternehmen des digitalen Vermögenssektors erfolgreich zu kompromittieren und zu bestehlen, etwa in den Vereinigten Arabischen Emiraten, Japan, Indien und Singapur. Der Angriff auf die in Dubai ansässige Kryptowährungsbörse Bybit im Februar 2025, bei dem eine nordkoreanische APT-Gruppe Vermögenswerte von fast 1,5 Milliarden US-Dollar entwendete, gilt als der bislang größte gemeldete Kryptoraub der Geschichte.

Die Schätzungen variieren, wie hoch Pjöngjangs durch den Diebstahl von Kryptowährungen erzielte Einnahmen sind. Laut einem MSMT-Bericht hat Nordkorea zwischen Januar 2024 und September 2025 Kryptowährungen im Wert von mindestens 2,8 Milliarden US-Dollar erbeutet. Laut dem »Crypto Crime Report 2026« der Analyseplattform Chainalysis waren staatlich geförderte nordkoreanische Hackergruppen für den Diebstahl von etwa 60 Prozent aller weltweit im Jahr 2025 entwendeten Kryptowährungen verantwortlich. In den Worten von Perry Choi bedeutet dies, dass das Regime faktisch einen »Staatsfonds aus gestohlenen digitalen Vermögenswerten aufgebaut hat — eine Kriegskasse, die außerhalb des traditionellen Dollarsystems liegt (und)

schwer einzufrieren ist«, Beobachter gehen davon aus, dass Nordkorea zeitweise der weltweit drittgrößte unter den staatlichen Bitcoin-Besitzern war.

Cyberspionage. Nordkoreanische Cyberespionage in Europa richtet sich gegen die Bereiche Rüstung, Luft- und Raumfahrt, Medien, Energie und Regierung sowie gegen individuelle Fachleute. Im Fall von Rüstungsunternehmen zielen entsprechende Operationen offenbar darauf ab, Informationen über Europas wachsende Verteidigungsstrukturen, diesbezügliche Partnerschaften mit Südkorea sowie technologische Details zu einzelnen Waffensystemen zu sammeln. So führten nordkoreanische Hacker 2025 etwa Cyberspionagekampagnen gegen europäische Drohnenunternehmen durch, um Technologie und Fertigungswissen zu unbemannten Luftfahrzeugen zu stehlen. Andere (darunter deutsche) Firmen aus den Sektoren Verteidigung sowie Luft- und Raumfahrt waren gezielten Phishing-Kampagnen ausgesetzt.

IT-Fachkräfte. Nordkoreanische IT-Fachkräfte stellen für das Regime in Pjöngjang eine wichtige Einnahmequelle dar – und für Europa ein wachsendes Sicherheitsrisiko. Mit dem Regime verbundene IT-Spezialisten sind oft hochqualifiziert; sie nutzen gestohlene oder gefälschte Identitäten und bewerben sich bei ausländischen Firmen etwa über Online-Plattformen als Remote-Mitarbeiter in einschlägigen Bereichen – wie der Entwicklung von Websites, mobilen Anwendungen, KI, Software und Blockchain-Verfahren. Ziel ist dabei nicht nur die Generierung von Deviseneinnahmen, sondern auch der Zugang zu sensiblen Informationen und Technologien.

Resolution 2375 des UN-Sicherheitsrats von 2017 untersagt es zwar grundsätzlich, nordkoreanische Arbeitskräfte im Ausland zu beschäftigen. Dennoch erzielte die DVRK im Jahr 2024 zwischen 350 und 800 Millionen US-Dollar durch weltweit tätige IT-Fachkräfte. Parallel baut das Regime die Infrastruktur aus, um solche Aktivitäten

zunehmend direkt von Nordkorea aus zu steuern.

Nach Erkenntnissen des amerikanischen Cybersicherheitsunternehmens Mandiant haben nordkoreanische IT-Fachkräfte ihre Aktivitäten seit 2024 deutlich auf Europa ausgeweitet, vor allem auch auf Deutschland, Portugal und das Vereinigte Königreich. In einem am 31. Juli 2026 veröffentlichten Statement warnte der Europäische Auswärtige Dienst (EAD) vor erheblichen finanziellen Schäden durch nordkoreanische Cyberoperationen. Diese würden auch zur Finanzierung von Pjöngjangs Nuklear- und Raketenprogrammen beitragen und die internationale Sicherheit und Stabilität bedrohen, so der EAD. Die Mitteilung folgte einer gemeinsamen Erklärung mehrerer Staaten bezüglich der Risiken, die nordkoreanische IT-Fachkräfte für Regierungen, private Unternehmen und einzelne Bürger darstellen.

Die von Nordkorea ausgehende Cyberbedrohung dürfte sich durch die vertiefte Zusammenarbeit des Regimes mit Russland weiter verschärfen. Insbesondere entwickelt sich das Land zu einem wichtigen Standort für nordkoreanische IT-Operationen; Moskau stärkt so die Fähigkeit Pjöngjangs, weltweit Einnahmen zu erzielen und Unternehmen zu infiltrieren.

Implikationen für Europa

Nordkoreas Operationen im Cyberraum stellen eine direkte sicherheitspolitische Herausforderung für Europa dar. Europäische Behörden, Finanzinstitute, Unternehmen, Forschungseinrichtungen sowie Betreiber kritischer Infrastruktur gehören verstärkt zum Zielspektrum nordkoreanischer Hackergruppen. Deren Aktivitäten reichen von Spionage über Ransomware-Angriffe bis hin zum Diebstahl digitaler Vermögenswerte. Die Besonderheit dieser Bedrohung liegt in ihrer Asymmetrie. Während Cyberoperationen für Nordkorea vergleichsweise kostengünstig und politisch risikoarm, da schwer zuzuordnen sind, können sie für Europa erhebliche wirtschaftliche Schäden, den Abfluss sensibler Tech-

nologien und Störungen kritischer Infrastrukturen verursachen.

Hinzu kommt, dass Kryptowährungsdiebstahl eine zentrale Finanzierungsquelle für Nordkoreas Programme zur Entwicklung von Massenvernichtungswaffen ist. Digitale Verwundbarkeiten in Europa können so mittelbar dazu beitragen, nordkoreanische Rüstungsprojekte zu stärken – und damit auch jene militärische Kooperation mit Russland, über die Pjöngjang den Krieg gegen die Ukraine unterstützt.

Zusätzliche Brisanz erhält diese Entwicklung durch die vertiefte russisch-nordkoreanische Zusammenarbeit im Cyberraum. Die Nutzung gemeinsamer Infrastruktur sowie Überschneidungen zwischen nordkoreanischen und russischen Cyberakteuren erhöhen Reichweite, Resilienz und Effektivität entsprechender Operationen. Die europäische Cyberabwehr steht damit vor einer Herausforderung, die zunehmend über nationale Zuständigkeiten hinausgeht.

Für Europa ergibt sich daraus die Notwendigkeit eines umfassenderen sicherheitspolitischen Ansatzes. Nato, EU und ihre jeweiligen Mitgliedstaaten sollten Nordkorea als eigenständigen sicherheitspolitischen Akteur mit unmittelbarer Relevanz für Europa behandeln. Erforderlich sind eine engere europäische Koordinierung im Cyberbereich, ein deutlich verbesserter Austausch von Lageinformationen – einschließlich entsprechender Informationssicherheitsabkommen –, eine stärkere Resilienz kritischer Infrastrukturen sowie eine konsequentere Einbindung des Indo-Pazifiks in die europäische Sicherheitsstrategie. Obwohl sich Nordkorea mittlerweile zu einer zentralen Gefahr im Bereich Cyberangriffe und Kryptowährungsdiebstahl entwickelt hat, orientieren sich europäische Regierungen noch immer an einer früheren Ära. Wenn sie diese Risiken weiterhin als Randthema wahrnehmen, werden sie noch mehr an Boden gegenüber einem Regime verlieren, das Cyberkriminalität in allen Facetten als Kernstück seiner staatlichen Strategie betrachtet.

Empfehlungen

Nordkorea stellt längst nicht mehr nur ein regionales Sicherheitsproblem im Indo-Pazifik dar, sondern ist heute ein unmittelbarer Faktor für die europäische Sicherheits-, Verteidigungs- und Cyberpolitik. An der vertieften Zusammenarbeit zwischen Pjöngjang und Moskau wird dies ebenso deutlich wie an Nordkoreas Cyberoperationen gegen Europa.

Auf strategischer Ebene sollte die EU daher *erstens* ihren »Critical Engagement«-Ansatz gegenüber Nordkorea weiterentwickeln. Den bisherigen primär auf Sanktionen und begrenzten Dialog ausgerichteten Sonderkurs für dieses Land gilt es dabei zum integralen Baustein einer breiteren EU-Strategie gegenüber autoritären Staaten zu machen. Dies erfordert, Nordkorea-Fragen nicht isoliert zu behandeln, sondern sie systematisch mit der Russland-Politik der EU, ihrer Indo-Pazifik-Strategie sowie ihrer Agenda für Cyber- und hybride Bedrohungen zu verknüpfen. Gefragt ist auch eine engere operative Zusammenarbeit mit Südkorea, Japan und den USA bei der Aufklärung und Unterbrechung von Waffenlieferungen. In multilateralen Foren, etwa bei den UN, bedarf es einer diplomatischen Offensive, um klar zu benennen, dass bei der nordkoreanisch-russischen Kooperation systematisch das Völkerrecht gebrochen wird.

Zweitens muss die Cyberdimension explizit und systematisch in die Nordkorea-Strategie der EU und in ihre übergreifende Strategie gegenüber autoritären Staaten integriert werden. Die EU sollte das horizontale Cybersanktionsregime konsequenter gegen nordkoreanische Akteure nutzen und zeitnah eine gezielte Erweiterung der Cybersanktionsliste vornehmen. Aus der DVRK ist dort bislang die Firma Chosun Expo designiert. Darüber hinaus zu erfassen gilt es aber auch zentrale Akteure der nordkoreanischen Cyberinfrastruktur wie das erwähnte Generalbüro für Aufklärung sowie ausgewählte Einheiten und Schlüsselpersonen, die mit den Gruppen Lazarus,



Dieses Werk ist lizenziert
unter CC BY 4.0

Das Aktuell gibt die Auf-
fassung des Autors wieder.

In der Online-Version dieser
Publikation sind Verweise
auf SWP-Schriften und
wichtige Quellen anklickbar.

SWP-Aktuells werden intern
einem Begutachtungsverfahren,
einem Faktencheck und
einem Lektorat unterzogen.
Weitere Informationen
zur Qualitätssicherung der
SWP finden Sie auf der SWP-
Website unter [https://www.
swp-berlin.org/ueber-uns/
qualitaetssicherung/](https://www.swp-berlin.org/ueber-uns/qualitaetssicherung/)

SWP

Stiftung Wissenschaft und
Politik
Deutsches Institut für
Internationale Politik und
Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
DOI: 10.18449/2026A50

Kimsuky und Famous Chollima in Verbin-
dung stehen.

Gleichzeitig sollte die EU in ihren ein-
schlägigen Rechtsakten und Ratsbeschlüs-
sen klarstellen, dass Erlöse aus nordkorea-
nischen Cyberangriffen, insbesondere Kryp-
todiebstählen, als Mittel zur Finanzierung
von Massenvernichtungswaffen gelten. Dies
würde die rechtliche Grundlage erweitern,
um künftig gegen Drittländer, Unterneh-
men und Finanzintermediäre effektivere
Sekundärsanktionen zu verhängen. Die
operative Umsetzung solcher Sanktionen
sollte durch eine engere Koordination zwi-
schen den Mitgliedstaaten, dem EAD, der
Europäischen Kommission, ENISA, dem
Cybersicherheitsdienst CERT-EU und natio-
nalen Cyberbehörden verbessert werden.
Dies schließt den systematischen Austausch
von Attributionsinformationen ein.

Drittens sollte die EU die nordkoreanisch-
russische Militärkooperation als direkte
sicherheitspolitische Herausforderung für
Europa behandeln. Sanktionsdurchsetzung,
Abschreckung und diplomatische Instru-
mente gegenüber Pjöngjang sind daher eng
mit der europäischen Russland- und Ukrai-
ne-Politik abzustimmen. Alle identifizierten
Akteure, Einrichtungen und Transportnetz-
werke, die an der Lieferung von Munition,
Raketen und Drohnen oder der Entsendung
von Truppenkontingenten aus der DVRK
nach Russland beteiligt sind, sollten syste-
matisch in die Sanktionsregime einbezogen
werden. Zu erfassen gilt es dabei auch Ree-
dereien, Versicherer, Häfen und Zwischen-
händler, die diese Transfers ermöglichen.

Dr. Eric J. Ballbach ist Gastwissenschaftler in der Forschungsgruppe Asien.