

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Jörn König, Joana Cotar, Barbara Lenk, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 20/897 –**

Mögliche Gefährdung des deutschen Olympiateams durch Cyberspionage im Rahmen der XXIV. Olympischen Winterspiele in Peking

Vorbemerkung der Fragesteller

Im Februar 2022 fanden in der chinesischen Hauptstadt Peking die XXIV. Olympischen Winterspiele statt. Diese standen bereits im Vorfeld massiv in der Kritik bezüglich der übertriebenen und „unzumutbaren“ Isolationsbedingungen der chinesischen Null-Covid-Politik (<https://www.zeit.de/sport/2022-02/olympische-winterspiele-china-quarantaene-bedingungen>), bezüglich der nicht nachhaltigen Gestaltung der Sportstätten (<https://www.welt.de/sport/plus236544289/Olympia-2022-in-Peking-Das-Maerchen-von-den-gruenen-Spielen.html>), bezüglich des sexuellen Übergriffs auf die Tennisspielerin Peng Shuai durch einen chinesischen Spitzenpolitiker (<https://www.zeit.de/sport/2022-02/peng-shuai-interview-china-olympia-kritik>), bezüglich der zunehmenden Menschenrechtsverletzungen in China (<https://www.amnesty.de/olympia-china-2022>), bezüglich des zunehmend autokratischen Politik- und Parteiapparats in China (<https://www.deutschlandfunk.de/100-jahre-kommunistische-partei-chinas-eine-staatspartei-100.html>) und den nicht erfolgten Fortschritten der politischen Öffnung und Demokratisierung, die eine wesentliche Hoffnung der Vergabe der XXIX. Olympischen Sommerspiele nach Peking im Jahr 2008 waren. Entsprechende politische Zusagen von Seiten der Regierung der Volksrepublik China im Zusammenhang mit der Bewerbung für den Zuschlag für die Olympischen Sommerspiele 2008, insbesondere die Menschenrechte zu stärken und die Pressefreiheit auszuweiten, wurden seitdem nicht umgesetzt (<https://www.bundestag.de/resource/blob/829038/4599b42707cbdd63e04181dc04c2075e/WD-2-017-21-pdf-data.pdf>).

Darüber hinaus gab es zahlreiche Befürchtungen der Cyberspionage, mit der die Teilnehmer der XXIV. Olympischen Winterspiele überwacht und ausgekundschaftet werden sollten. Diese betrafen nicht nur das deutsche Olympiateam, sondern auch die Teilnehmer anderer Nationen wie z. B. Großbritanniens oder der Niederlande (<https://www.tagesspiegel.de/politik/angst-vor-spionage-aus-pekings-britische-olympia-athleten-sollen-gesonderte-handys-bekommen/27973742.html>). Insbesondere die obligatorische Smartphone-Anwendung „My2022“ geriet dabei in die Kritik (<https://www.faz.net/aktuell/sport/olympische-winterspiele/my2022-app-warnung-vor-chinas-app-zu-olympia-in-pekings-17738228.html>). Die Cyberspionage soll ferner nicht nur von staatlichen

Überwachungsbehörden ausgegangen sein, sondern auch von nichtstaatlichen chinesischen Hackergruppen (<https://www.sportschau.de/olympia/investigativ/olympia-hintergrund-datenklau-100.html>).

Mehrere deutsche Sportverbände haben vor den XXIV. Olympischen Winterspielen offenbar konkrete Warnungen vor einer Abschöpfung sportwissenschaftlicher Daten durch Cyberangriffe bei Testwettkämpfen vor Ort oder den Olympischen Spielen selbst bekommen. Die Verbände erhielten daraufhin vom Bundesnachrichtendienst (BND) die Empfehlung, keine sensiblen Informationen auf elektronischen Datenträgern mit nach China zu nehmen (<https://www.augsburger-allgemeine.de/sport/Ski-alpin-Vor-Olympischen-Winterspielen-in-China-Spionage-Angst-beim-DSV-id60781461.html>). Dabei ging es unter anderem um Daten aus dem Sportgerätebau, der Materialforschung für Sportgeräte, sportartspezifische Daten wie Wachsanalysen für Skier, aber auch um personenbezogene Daten aus der Leistungsdiagnostik und der Trainingssteuerung.

Betroffen davon waren offenbar vor allem der Deutsche Skiverband (DSV), Bereich Ski Alpin sowie auch weitere Verbände bzw. Verbandsteile wie der Bereich Biathlon und der Bob- und Schlittenverband für Deutschland (BSD). Insbesondere Letzterer hatte auch durch seinen Materialvorteil neun von zehn möglichen Goldmedaillen gewonnen, im Zweierbob der Männer sogar als Dreifachtriumph mit Gold-, Silber- und Bronzemedaille (<https://www.nzz.ch/sport/unmut-ueber-eine-medailenrazzia-die-deutschen-schlittensportler-vergol-den-ihren-materialvorteil-es-ertoenen-rufe-nach-einer-revolution-ld.1670764>).

Diese Vorwürfe im Sportbereich gehen einher mit Vorwürfen der Cyberspionage durch China auch im Bereich der Entwicklungszusammenarbeit (<https://www.golem.de/news/spionage-china-baut-abhoerfunktion-in-den-sitz-der-afrikanischen-union-1801-132458.html>) sowie im Bereich der Wirtschaftsspionage (<https://www.handelsblatt.com/politik/deutschland/cyberattacken-berlin-verdaechtigt-chinas-regierung-der-industriespionage-im-grossen-stil/24911728.html?ticket=ST-526405-Es3AKLaxO3yrL6AtdLjL-ap1>).

1. Waren der Bundesregierung konkrete Hinweise bekannt, die bereits vor den XXIV. Olympischen Winterspielen in Peking davor gewarnt haben, dass sensible Daten der deutschen Sportverbände durch Cyberspionage vor Ort gefährdet sind?
 - a) Wann gingen diese Hinweise bei der Bundesregierung ggf. ein, und durch wen erfolgten die Hinweise, z. B. deutsche oder ausländische Behörden, deutsche oder ausländische Sportverbände, Journalisten, IT-Sicherheitsfirmen, etc.?
 - b) Bezogen sich die möglichen Hinweise auf spezifische deutschen Spitzensportverbände oder spezifisches Datenmaterial, wenn ja, bitte erläutern?
 - c) Wurden diese möglichen Hinweise den entsprechenden Sportverbänden mitgeteilt, wenn ja, wann, und durch wen?
 - d) Wurden von der Bundesregierung ggf. Handlungsanweisen für die entsprechenden Sportverbände erarbeitet, wenn ja, wann wurden diese den Verbänden mitgeteilt, durch wen, und wie wurde deren Umsetzung sichergestellt?
 - e) Wurden von der Bundesregierung auch deutsche Journalisten für eine entsprechende Gefährdung sensibilisiert, und wurde ihnen Unterstützung im Umgang mit der Cyberproblematik gegeben, wenn ja, wann, durch wen, und in welcher Form?

Die Fragen 1 bis 1e werden zusammenhängend beantwortet.

Konkrete Hinweise im Sinne der Fragestellung liegen der Bundesregierung nicht vor. Jedoch haben Behörden auf verschiedener Art und Weise die Ziel-

gruppe sensibilisiert. So hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) am 19. Januar 2022 im Rahmen einer Veranstaltung, an der die aktiven Sportlerinnen und Sportler und die Betreuerinnen und Betreuer des deutschen Olympia-Teams teilgenommen haben, über mögliche Cybersicherheitsrisiken aufgeklärt. Der Schwerpunkt des Beitrags lag auf Empfehlungen zum Umgang mit mobilen Endgeräten vor, während und nach den Olympischen Spielen. Zudem wurde dem Deutschen Olympischen Sportbund (DOSB) ein Sicherheitsleitfaden für die Teilnehmenden zur Verfügung gestellt.

Das Bundeskriminalamt (BKA) hat mit Schreiben vom 26. Januar 2022 bundesweit zur Gefährdungslage im Zusammenhang mit den Olympischen Winterspielen informiert und darin auf die abstrakte Gefährdung durch Cyberangriffe hingewiesen.

Darüber hinaus wurde am 28. Januar 2022 eine Sensibilisierung der deutschen Wirtschaftsunternehmen und -verbände veranlasst. Hier wurde insbesondere darauf aufmerksam gemacht, dass grundsätzlich Aktivitäten Chinas zur Informations- und Datenbeschaffung in Betracht zu ziehen sind. So war beispielsweise aufgrund anhaltender Berichterstattung über die Kompromittierung von Endgeräten (insbesondere Mobiltelefone, Laptops) eine entsprechende Gefährdung auch für den Zeitraum der Olympischen Winterspiele anzunehmen.

Das Bundesamt für den Militärischen Abschirmdienst (BAMAD) stellte dem DOSB am 12. Januar 2022 zwei Publikationen zur Verfügung, die sich mit Sicherheitsvorkehrungen im Zusammenhang mit Auslandsdienstreisen und chinesischen Aktivitäten der Informations- und Datenbeschaffung über Soziale Netzwerke befassen. Das Bundesamt für Verfassungsschutz (BfV) stimmte zu, die Publikationen zu Sensibilisierungszwecken auch denjenigen Angehörigen der Olympiamannschaft zur Verfügung zu stellen, die nicht dem Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) angehören.

2. Sind der Bundesregierung Überwachungs- und Spionagevorfälle mithilfe digitaler Anwendungen bekannt, von denen das deutsche Olympiateam, inklusive Sportler, Betreuer, Funktionäre, Journalisten etc., im Rahmen der XXIV. Olympischen Winterspiele in Peking betroffen war, wenn ja, in welchem Umfang, und mit welchen Folgen?
 - a) Wenn ja, waren davon Sportler, Betreuer, Journalisten oder andere Teilnehmer gleichermaßen betroffen, oder gab es bevorzugte Ziele, wenn ja, welche?
 - b) Kam es ggf. dabei zu einem Datenabfluss, und wenn ja, in welchem Umfang, und von welcher Qualität?
 - c) Konnte bei den möglichen Vorfällen eine spezifische Zielrichtung analysiert werden, z. B. technische Geheimnisse oder Kommunikationsverhalten von Journalisten, wenn ja, welche?
 - d) Gab es entsprechende Vorfälle bereits auch bei den Olympischen Sommerspielen im Jahr 2008, und wenn ja, in welchem Umfang, und von welcher Qualität?
 - e) Gab es entsprechende Überwachungs- und Spionagevorfälle mithilfe digitaler Anwendungen seit den Olympischen Sommerspielen im Jahr 2008 bereits auch bei anderen Sportgroßereignissen, und wenn ja, in welchem Umfang, und von welcher Qualität?
 - f) Wenn ja, mithilfe welcher digitalen Anwendungen erfolgten die Cyberangriffe?
 - g) Konnten, sofern die Hauptfrage bejaht wurde, Akteure identifiziert werden, von denen die Cyberangriffe ausgingen, wenn ja welche?

- h) Durch wen wurden die Überwachungs- und Spionagevorfälle der Bundesregierung ggf. bekannt, durch eigene Aufklärung oder durch Hinweise befreundeter Staaten oder durch welche anderen Quellen?

Die Fragen 2 bis 2h werden zusammenhängend beantwortet.

Der Bundesregierung liegen keine Erkenntnisse zum Fragegegenstand vor.

3. Sind der Bundesregierung Cyberangriffe auf das deutsche Olympiateam, inklusive Sportler, Betreuer, Funktionäre, Journalisten etc., bekannt, die bereits im Vorfeld der XXIV. Olympischen Winterspiele, z. B. auf Olympiastützpunkte in Deutschland etc., stattgefunden haben?
- a) Waren, wenn die Hauptfrage bejaht wurde, davon Sportler, Betreuer, Journalisten oder andere Teilnehmer gleichermaßen betroffen, oder gab es bevorzugte Ziele, wenn ja, welche?
- b) Wenn ja, kam es dabei zu einem Datenabfluss, und wenn ja, in welchem Umfang, und von welcher Qualität?
- c) Wenn ja, konnte bei den Vorfällen eine spezifische Zielrichtung analysiert werden, z. B. technische Geheimnisse oder Kommunikationsverhalten von Journalisten, wenn ja, welche?
- d) Wenn ja, mithilfe welcher digitalen Anwendungen erfolgten diese Cyberangriffe nach Kenntnis der Bundesregierung?
- e) Wenn ja, konnten Akteure identifiziert werden, von denen diese Cyberangriffe ausgingen, wenn ja welche?
- f) Wenn ja, durch wen wurden diese Cyberangriffe der Bundesregierung bekannt, durch eigene Aufklärung oder durch Hinweise befreundeter Staaten oder durch welche anderen Quellen?

Die Fragen 3 bis 3f werden zusammenhängend beantwortet.

Der Bundesregierung liegen keine Erkenntnisse zum Fragegegenstand vor.

4. Hat die Bundesregierung die obligatorische Smartphone-Anwendung „My2022“ (vgl. Vorbemerkung der Fragesteller) vor Beginn der XXIV. Olympischen Winterspiele analysiert, wenn ja, hat sie sich aus den Erkenntnissen in technischer und rechtlicher Sicht eine Auffassung gebildet, und wie lautet diese hinsichtlich der Vorwürfe der Cyberspionage und Cyberüberwachung ggf.?

Die Bundesregierung hat keine eigenen Analysen durchgeführt.

- a) War der Bundesregierung die Analyse der „My2022“-App durch das Citizen Lab der Universität Toronto vor Abreise des Olympia-Teams nach Peking bekannt (<https://citizenlab.ca/2022/01/cross-country-exposure-analysis-my2022-olympics-app/>)?

Der Bundesregierung war die Analyse des Citizen Lab bekannt.

- b) Hat die Bundesregierung vor Abreise des Olympiateams nach Peking Empfehlungen ausgesprochen oder andere Maßnahmen ergriffen hinsichtlich des Umgangs mit der App durch die Teilnehmer des deutschen Olympiateams, wenn ja, welche?

Es wird auf die Antwort zu den Fragen 1 bis 1e verwiesen.

- c) Ist der Bundesregierung bekannt, wie viele Teilnehmer des deutschen Olympia-Teams die „My2022“-App auf ihren Smartphones installiert, genutzt und in welcher Form genutzt haben?

Der Bundesregierung liegen keine Erkenntnisse zum Fragegegenstand vor.

5. Welche Maßnahmen insgesamt hat die Bundesregierung ggf. ergriffen, um das deutsche Olympiateam, inklusive Sportler, Betreuer, Funktionäre, Journalisten etc., vor chinesischer Cyberspionage und Cyberüberwachung im Rahmen der XXIV. Olympischen Winterspiele zu schützen, und welche Kosten sind dafür ggf. entstanden (bitte nach Maßnahmen aufschlüsseln)?
- Gab es systematische Sensibilisierungen, Informationen oder Handlungsanweisungen für die Teilnehmer des deutschen Olympiateams, wenn ja welche, und zu welchem Zeitpunkt?
 - Gab es technische Maßnahmen, wenn ja, welche, und zu welchem Zeitpunkt?
 - Gab es organisatorische Maßnahmen, wenn ja welche, und zu welchem Zeitpunkt?
 - Haben deutsche Sicherheitsbehörden das deutsche Olympia-Team zur Unterstützung vor Ort begleitet, wenn ja, in welchem Umfang?
 - Gibt es nach Kenntnis der Bundesregierung im Deutschen Olympischen Sportbund (DOSB) oder den Fachverbänden spezifische Strukturen, Verfahren und Verantwortliche, um die deutschen Olympiateilnehmer vor diesen Cybergefahren zu schützen, wenn nein, warum nicht, und sollen diese bis wann eingerichtet werden?

Die Fragen 5 bis 5e werden zusammenhängend beantwortet.

Das BKA unterstützte im Rahmen der Zuständigkeit der Sicherungsgruppe für Sportkoordination analog zu vorhergehenden Olympischen Spielen die deutsche olympische Mannschaft in beratender Funktion und begleitete das Team auch während der Olympischen Winterspiele in China vor Ort mit einer Polizeivollzugsbeamtin.

Ein Themenschwerpunkt der durchgeführten Besprechungen mit dem DOSB im Vorfeld der Olympischen Winterspiele war die Informationssicherheit genutzter Technik während des Aufenthaltes in China. Für eine eingehende Beratung wurde der DOSB zuständigkeitshalber an das BSI verwiesen.

Im Übrigen wird auf die Antwort zu den Fragen 1 bis 1e verwiesen.

6. Wer trägt nach Kenntnis der Bundesregierung für den Schutz der deutschen Olympiateilnehmer vor Cybergefahren die Gesamtverantwortung?

Es wird auf die Antwort zu den Fragen 5 bis 5e verwiesen.

- Wie sind nach Kenntnis der Bundesregierung die deutschen Olympiastützpunkte und vergleichbare Trainingseinrichtungen vor Cyberangriffen geschützt?
- Gibt es auf behördlicher und nach Kenntnis der Bundesregierung auf Verbandsseite entsprechende Verantwortliche, Strukturen und Verfahrensweisen, wenn nein, warum nicht, und bis wann sollen diese etabliert werden?

- c) Welche finanziellen Mittel stehen den deutschen Olympiastützpunkten und vergleichbaren Trainingseinrichtungen nach Kenntnis der Bundesregierung zum Schutz vor Cyberangriffen zur Verfügung?

Der Bundesregierung liegen keine Erkenntnisse zum Fragegegenstand vor.

7. Wurden nach Kenntnis der Bundesregierung die deutschen Olympiateilnehmer mit fabrikneuen Endgeräten, z. B. Smartphones, Laptops, etc., ausgestattet und entsprechend eingewiesen, wenn ja, durch wen, wenn nein, warum nicht?
- a) Erfolgten nach Kenntnis der Bundesregierung spezielle IT-Sicherheitstests dieser Geräte vor ihrer Ausgabe, wenn ja, durch wen, wenn nein, warum nicht?
- b) Welche Kosten entstanden nach Kenntnis der Bundesregierung für Ausstattung, Einrichtung und Einweisung?

Die Fragen 7 bis 7b werden zusammenhängend beantwortet.

Laut öffentlich verfügbaren Medienberichten wurden deutschen Olympia-Teilnehmern neue Smartphones zur Verfügung gestellt. Es ist nicht bekannt, ob dieses Angebot von allen deutschen Sportlern in Anspruch genommen wurde. Weitere Erkenntnisse liegen der Bundesregierung nicht vor.

8. Wurden in Peking von deutschen Olympiateilnehmern verwendete Endgeräte nach Rückkehr nach Deutschland nach Kenntnis der Bundesregierung vernichtet?
- a) Wenn ja, wer ist nach Kenntnis der Bundesregierung für die Vernichtung der Geräte verantwortlich?
- b) Wenn ja, wurden sämtliche Geräte nach Kenntnis der Bundesregierung vernichtet, wenn nein, warum nicht, und bis wann soll dies erfolgen?
- c) Wenn nein, werden nach Kenntnis der Bundesregierung nicht vernichtete Geräte forensischen Untersuchungen unterzogen, um weitere Kenntnisse über Cyberbedrohungen zu erhalten, wenn nein, warum nicht?
- d) Wenn nein, werden nicht vernichtete Geräte nach Kenntnis der Bundesregierung vor einer weiteren Nutzung speziellen IT-Sicherheitstests unterzogen, wenn ja, auf wessen Kosten, und durch wen, wenn nein, warum nicht, und bis wann soll dies erfolgen?

Die Fragen 8 bis 8d werden zusammenhängend beantwortet.

Der Bundesregierung liegen keine Erkenntnisse zum Fragegegenstand vor.

- e) Wie groß ist nach Auffassung der Bundesregierung die Gefahr, dass über Geräte, die in China im Einsatz waren und die in Deutschland weiter benutzt werden, weiterhin Daten ausgeleitet werden und wie will die Bundesregierung mit dieser Gefährdung ggf. umgehen?

Generell besteht eine Gefahr, dass über Geräte, die in China im Einsatz waren und in Deutschland weiterhin genutzt werden, Daten gesammelt und ausgeleitet werden (z. B. Standortdaten, E-Mails, Textnachrichten und Kontakte der Geräte).

9. Stand, steht oder wird die Bundesregierung mit dem Internationalen Olympischen Komitee (IOC) hinsichtlich möglicher Cyberspionage und Cyberüberwachung im Rahmen der XXIV. Olympischen Winterspiele in Kontakt stehen, wenn ja, mit welchen Personen, mit welchem Ziel, und mit welchen Ergebnissen, wenn nein, warum nicht, und ist dies noch geplant?

Der regelmäßige, etablierte, stete Austausch der Bundesregierung mit den deutschen Sportverbänden umfasst auch diese Thematik.

10. Werden nach Kenntnis der Bundesregierung aus den Cyberrisiken im Rahmen der XXIV. Olympischen Winterspiele Handlungsanweisungen des DOSB oder von Fachverbänden für weitere Sportgroßereignisse abgeleitet werden, wenn ja, durch wen, und auf welche Weise?

Steht die Bundesregierung dabei mit internationalen Sportverbänden wie IOC oder FIFA und/oder mit anderen Teilnehmernationen in Verbindung, und wie begründet die Bundesregierung ihre Absicht?

Der Bundesregierung liegen keine Erkenntnisse zum Fragegegenstand vor.

11. Wird sich die Bundesregierung bei internationalen Sportverbänden wie IOC oder FIFA und oder anderen Teilnehmernationen dafür einsetzen, Cybersicherheit als ein Auswahlkriterium künftiger Sportgroßereignisse zu etablieren, und wie begründet die Bundesregierung ihre Absicht?

Cyber-Sicherheit ist ein Aspekt bei der Vergabe von Sportgroßveranstaltungen, der, soweit angezeigt, im Vergabeprozess thematisiert wird.

