Gesprächskreis
Nachrichtendienste in Deutschland e. V.

Chinesische Direktinvestitionen – Ein klarer Fall für eine ressortübergreifende Risikogesamtrechnung

Anmerkungen zur aktuellen Diskussion

Stellungnahme des Gesprächskreises Nachrichtendienste in Deutschland e. V.
(31.10.2022)

Das strategische sicherheitspolitische Versagen gegenüber Russland hat verdeutlicht, dass Einzelfallentscheidungen zu sicherheitsrelevanten Investitionen ohne Berücksichtigung einer Risikogesamtrechnung Kernbereiche staatlicher wie wirtschaftlicher Sicherheit und Handlungsfähigkeit gefährden können.

Angesichts der noch gewichtigeren Dimensionen des chinesischen globalen Vorgehens ist eine umfassende, jeweils zu aktualisierende fachliche Bestandsaufnahme und Bewertung von bereits durch chinesische Direktinvestitionen eingegangenen Sicherheitsrisiken dringender denn je erforderlich.

Eine von der Bundesregierung einzuleitende und zu verantwortende sicherheitliche „Risikogesamtrechnung“ erfordert eine umfassende Anstrengung der zuständigen Dienste und Behörden im Rahmen eines ressortübergreifenden, vom Bundeskanzleramt zu koordinierenden Ansatzes.

Die politische Diskussion um die Nachrichtendienste in Deutschland wird ungeachtet der propagierten Zeitenwende unverändert stark von der Vorstellung geprägt, der Bürger müsse in seinen Freiheitsrechten gegenüber dem Staat und insbesondere seinen Nachrichtendiensten systematischer und weitreichender geschützt werden. Das ambitionierte Projekt einer „Überwachungsgesamtrechnung“ macht hier die Runde, mit all seinen juristischen, administrativen und

nachrichtendienstlichen Fragestellungen und Unwägbarkeiten[1], ebenso wie die Diskussion um Vorratsdatenspeicherung und „quick freeze“[2]. All dies ist Ausdruck des besonders hohen Maßes an Skrupulosität und Selbstbeschränkung, das bei der Konzipierung und Umsetzung staatlicher Machtmittel nach herrschender Meinung an den Tag zu legen sei, nicht zuletzt auch, um das Vertrauen der Bürger in Rechtsstaatlichkeit, Verhältnismäßigkeit und staatlicher Grundrechtsgarantie zu befördern.

Es bleibt jedoch festzuhalten, dass derzeit und wohl auch absehbar wesentlich gravierendere Elemente des Vertrauens zwischen Bürger und Staat zur Debatte stehen, wenn politische Entscheidungsträger es versäumen oder sich weigern, Gefährdungen elementarer Sicherheitsinteressen des Landes und seiner Menschen angemessen zur Kenntnis zu nehmen und nachvollziehbare, energische Anstrengungen zu ihrer Überwindung oder wenigsten Begrenzung zu unternehmen. Hier geht es um konkrete, Lebensverhältnisse und Zukunftsperspektiven unmittelbar tangierende, durchaus als existenziell zu bezeichnende Fragen.

Das Bekenntnis zum strategischen sicherheitspolitischen Versagen gegenüber Russland ist im Rahmen der Zeitenwende mittlerweile zum politischen „Mainstream“ geworden, in dem man sich parteiübergreifend bereits häuslich eingerichtet hat. Ob, in welchem Umfang, in welcher Tiefe und insbesondere auch mit welchem Zeithorizont jeweils ein Umsteuern in kritischen Bereichen von Wirtschaft und Infrastruktur möglich sein wird, bleibt eine der großen Herausforderungen für Staat und Gesellschaft in den kommenden Jahren. Allein die aktuelle breite öffentliche Diskussion um Vulnerabilitäten weiter Bereiche der Kritischen Infrastruktur bis hin zur jüngsten Bestandsaufnahme des BSI zur Cyberbedrohung[3] lässt die existentielle Dimension des Problems erkennen, auch wenn es hier erst eines „strategischen Schocks“ in Form der Nord-Stream-Explosionen[4] bedurft hatte, um aus der öffentlichen Behäbigkeit, die sich trotz eindringlicher und vielfältiger Warnungen seit spätestens 2014 gehalten hatte, jäh zu erwachen.

Es bleibt im allseitigen Interesse sehr zu hoffen, dass die eingeleiteten erheblichen Anstrengungen zur Schadensbegrenzung erst einmal in den kommenden Monaten einigermaßen greifen und Schlimmeres verhüten können. Nur so kann neben der rein materiellen Abwendung weiteren massiven Schadens auch Legitimität und Glaubwürdigkeit staatlichen Handelns in der elementaren Kernaufgabe staatlicher Sicherheitsgewährleistung und damit politische Akzeptanz zurückgewonnen werden. Die wenig ermutigenden Umfrageergebnisse zum mangelnden Vertrauen der Bürger in die Handlungsfähigkeit und Problemlösungskompetenz von Politik angesichts der existenziellen Herausforderungen verdeutlichen hier eine klare Erwartungshaltung[5].

Um so bemerkenswerter, wenngleich nicht wirklich überraschend, erscheint es angesichts dieser Problemlage, dass nun auch in Sachen China offenbar ein vergleichbarer Mangel an sicherheitspolitischer Strategiefähigkeit und Handlungsbereitschaft zu Tage tritt. Die jüngsten

---

[1] Löffelmann, Überwachungsgesamtrechnung und Verhältnismäßigkeitsgrundsatz (Berlin 2022), Überwachungs-Gesamtrechnung sucht Ministerium (Cilip, 22.07.2022); Christian Geminn, Zur Institutionalisierung einer Überwachungsgesamtrechnung (DÖV, 19/2022); Zöller, Was bringt die "Überwachungsgesamtrechnung"? (LTO, 18.03.2022)

[2] Sehl, Entwurf zur Vorratsdatenspeicherung. "Quick-Freeze"-Vorschlag vom Justizminister (LTO, 25.10.2022); Nach Urteil zu Vorratsdatenspeicherung Spielräume nutzen oder streichen? (Tagesschau, 20.09.2022)

[3] BSI-Jahresbericht: Cyberbedrohung so hoch wie nie (Tagesspiegel, 27.10.2022)

[4] Die Nord-Stream-Lecks sind ein letzter Weckruf (WiWo,28.09.2022); s. auch die kontinuierlichen Hinweise im GKND-Monitor

[5] Forsa-Umfrage, FDP fällt auf sechs Prozent – fast zwei Drittel trauen keiner Partei Problemlösungen zu. (WELT, 04.10.2022)

Diskussionen um chinesische Beteiligungen an kritischer Infrastruktur lassen erkennen, dass – wie zuvor im Fall Russlands – eine konsequente strategische Betrachtung und Bewertung sicherheitspolitischer Implikationen zumindest auf politischer Ebene unterbleibt, möglicherweise auch bewusst vermieden wird[6].

Bedenken der Sicherheits- und Nachrichtendienste werden im Einzelfall eingebracht, scheinen jedoch im Entscheidungsprozess keine ausschlaggebende Wirkung im Verhältnis zu den kurzfristig wahrscheinlich vorhandenen wirtschafts- und außenpolitischen Opportunitätserwägungen zu entfalten. Soweit in der Medienberichterstattung erkennbar, handelt es sich damit um ein klares *déjà vu*: Erneut scheint dem tagespolitischen Vorteil das langfristige elementare Sicherheitsinteresse geopfert zu werden, am Ende in der stillschweigenden Annahme, man könne später einmal im Rahmen einer weiteren Zeitenwende auf „Naivität" oder „Blindheit auf einem Auge" plädieren? Angesichts der Dimension des China-Problems sollte man da allerdings nicht so sicher sein…

Ein entscheidendes Manko dieser wieder zu beobachtenden Vorgehensweise ist deren Fokussierung auf den jeweiligen Einzelfall, bei der nicht nur das Gesamtbild der bisher eingegangenen Verpflichtungen und Abhängigkeiten, sondern insbesondere auch der einem potenten staatsnahen Käufer und den hinter diesem stehenden staatlichen Institutionen eingeräumten operativen Handlungsoptionen ausgeblendet werden. Welche zuweilen weitreichenden operativen Einflussmöglichkeiten bereits strikt limitierte Investitionen in sensiblen Bereichen eröffnen können, sei anlässlich des Cosco-Engagements im Hamburger Hafen am Beispiel von Erfahrungswerten aus Asien aus den frühen 2000er Jahren generisch skizziert, ohne dabei im konkreten Fall einer Sicherheitsanalyse vorgreifen zu können oder zu wollen. Wichtig ist hier nur, auf eine der möglichen Implikationen in einer solchen Fallkonstellation hinzuweisen.

Die unternehmerische Teilhabe an einem Containerhafen impliziert Zugang zu den IT-Strukturen, mit denen die Umschlagvorgänge kontrolliert und organisiert werden. Aus dieser Position ist ein Vordringen in die Datensysteme der Mitinhaber und Konkurrenten im Hafen bei entsprechender Professionalität in Cyber Network Operationen (CNO) prinzipiell möglich. Eine potentiell bedeutsame Rolle kann hier gegebenenfalls eine von Huawei weltweit gelieferte Telekommunikationsausrüstung spielen. Weitreichende Handlungsoptionen können mit einem solchen Vorgehen geschaffen werden: Man weiß zumindest in groben Zügen was in den einzelnen Containern ist, wer Lieferanten und Abnehmer sind. Über CNO können Container fehlgeleitet oder bei Bedarf einfach "vergessen" werden, indem sie aus den Frachtlisten gelöscht werden. Ladungen können manipuliert werden. Lieferketten für bestimmte Abnehmer können verzögert oder ganz unterbrochen werden, Firmen in die Insolvenz getrieben werden, um sie dann billig aufzukaufen. Ein Verantwortlicher des Containerhafens Singapur äußerte hierzu bereits vor Jahren einmal, dass mit der Kontrolle über die Hafen-IT Kriege entschieden werden könnten. Daher sei sie das Schützenswerteste in einem Containerhafen.

Die Welle systematischer weltweiter chinesischer Investitionen in Seehäfen ist seit Jahren bekannt[7]; es wäre zu hoffen, dass sich alle Beteiligten in angemessener Weise der möglichen Implikationen im Bereich der Sicherheit bewusst sind, ebenso wie in Bezug auf zahlreiche weitere Dimensionen der modernen Seidenstraßenpolitik der vergangenen 20 Jahre[8]. In vielen

[6] Zur Diskussion vgl. GKND-Monitor vom 27.10. und 31.10.2022

[7] Hafenbeteiligungen. Chinas Einfallstore in der Welt. (FAZ, 28.10.2022)

[8] Strategische Rivalität zwischen USA und China. Worum es geht, was es für Europa (und andere) bedeutet. (SWP, 2020)

Fällen geht es hier nicht nur um wirtschaftliche Präsenz und Einflussnahme sondern um den Aufbau operativ nutzbarer Infrastruktur für den „Bedarfsfall".

China gehört seit Jahrzehnten zu den großen Einkäufern von Technologien in Deutschland und zugleich zu den bedeutenden Investoren in technischer Infrastruktur wie zum Beispiel im Telekommunikationsbereich[9]. Dies gilt bekanntlich bereits für die 4G-Technologie und auch für Teile der 5G-Technologie, die ohne chinesische Hard- und Software nicht funktionstüchtig sind[10]. Nicht zuletzt in Bezug auf die Beteiligung von Huawei im 5G-Ausbau haben es die Nachrichten- und Sicherheitsdienste in ganz Westeuropa seit spätestens 2017 an deutlichen Warnungen nicht fehlen lassen[11]. Die Vereinigten Staaten lassen mittlerweile weniger denn je einen Zweifel daran, dass sie in China den zentraler sicherheitspolitischen Herausforderer, wenn nicht Gegenspieler sehen, und dies gerade auch in der Beschaffung, Entwicklung und Nutzung von Hochtechnologie zum Erwerb von strategischer globaler Informationsüberlegenheit und Handlungsmacht. Entsprechende weitreichende Maßnahmen sind eingeleitet worden[12].

Die jüngsten Medienberichte über ein mögliches internationales Netz an illegalen „Polizeistationen" zur Überwachung und Verfolgung von Dissidenten im Ausland verdeutlichen weitere Aspekte dieses Anspruchs, der auch vor der territorialen Integrität und Freiheitsordnung der betroffenen Länder nicht Halt macht[13]. Umfängliche nationale und internationale Analysen der Geheimdienste wie namhafter Think Tanks zu den Strukturen, Zielsetzungen und zum modus operandi langfristig und systematisch angelegter, von den Nachrichtendiensten massiv genutzter chinesischer globaler Wirtschafts- und Sicherheitspolitik im Dienst expliziter Weltmachtambitionen stehen seit Jahren zur Verfügung[14]. Sie werden dem Grunde nach soweit erkennbar auch keineswegs bestritten. Wie so häufig aber werden ganz offensichtlich konkrete Konsequenzen, erneut angesichts kurzfristiger Opportunitätserwägungen, gescheut. Durchwursteln mit Einzelfallentscheidungen unter Ausblendung des Gesamtbildes scheint hier die Handlungsmaxime zu sein, im Übrigen wohl nicht nur in Deutschland.

Aus fachlicher Sicht ist hier weiterer dringender Handlungsbedarf entstanden, von dem zu hoffen ist, dass er nunmehr auch auf parlamentarischer Ebene, gerade auch im Rahmen der aktuellen Befassung des Parlamentarischen Kontrollgremiums mit den Investitionsvorhaben, aufgenommen und artikuliert wird[15]: Mit der bisher verfolgten allgemeinen Beschwörung abstrakter Sicherheitsrisiken chinesischer Einflusspolitik kommt niemand weiter – dies haben bereits

---

[9] Aktuell: Chinas Einfluss auf die deutsche Wirtschaft (ZDF, 26.10.2022)

[10] 5G, Huawei und die Sicherheit unserer Kommunikationsnetze. Handlungsoptionen für die deutsche Politik (SWP, 01.02.2019); Analyse der sicherheitsrelevanten Risiken in Bezug auf den 5G Ausbau durch Huawei in Deutschland (HFTL 2019)

[11] Germany spy chief warns against 5G role for Huawei (FT, 29.10.2019); Huawei: China's Controversial Tech Giant (CFR, 06.08.2020)

[12] Biden Is Now All-In on Taking Out China. The U.S. president has committed to rapid decoupling, whatever the consequences.(Foreign Affairs, 12.10.2022) Limiting Chinese National Security Espionage (Carnegie, 25.04.2022); US, UK Officials Raise Fresh Alarms About Chinese Espionage (VOANEWS, 06.07.2022)

[13].Chinesische Auslandspolizei: Ein Netzwerk zur Einschüchterung (FAZ, 26.10.2022) China's 'Overseas Police Stations' Breach Sovereignty, Report Claims (VOANEWS; 11.10.2022)

[14] Aktuell: China: MI5 and FBI heads warn of 'immense' threat (BBC 07.07.2022); Bundesnachrichtendienst warnt vor Gefahr durch China (FAZ, 17.10.2022)

[15] Geheimdienst-Gremium des Bundestags nimmt China-Deals in den Fokus. Erst der Hamburger Hafen, jetzt eine deutsche Chipfabrik: Das Vordringen Chinas in sensible Wirtschaftsbereiche in Deutschland sorgt für Unruhe im politischen Berlin. (Handelsblatt, 28.10.2022)

die deprimierenden Erfahrungen im Falle Russlands gezeigt. Erforderlich ist vielmehr eine **fachlich basierte Risikogesamtrechnung**, ein umfassender Bewertungsansatz, mit dem eine konkrete Übersicht über die bisher bereits durch chinesische Investitionen und Ankäufe eingegangenen Sicherheitsrisiken in staatlicher Infrastruktur wie im privatwirtschaftlichen Bereich anzustreben ist. Es wird festzustellen sein, welche **sicherheitsrelevanten** Handlungsoptionen sich für China im Bedarfsfall aus den bisherigen Engagements ergeben und wo diese sich ggf. gegenseitig verstärken und durch grenzüberschreitende Vernetzungen akkumulieren und potenzieren könnten. Gefordert bei einer solchen Bestandsaufnahme und Bewertung sind alle Nachrichten- und Sicherheitsdienste, ebenso wie Fachbehörden auf Bundes- und Länderebene, sowie die zuständigen Geschäftsbereiche der Bundesregierung wie der Länder. Ein internationaler Informationsaustausch wird diesen Ansatz zu ergänzen haben.

Ein solcher, aufgrund seiner Sicherheitsempfindlichkeit unter strikter Vertraulichkeit umzusetzender Untersuchungsansatz würde als gesamtstaatliche Herausforderung notwendig ressortübergreifend durch das Bundeskanzleramt zu formulieren und zu koordinieren sein.

Eine Risikogesamtrechnung würde einen tragfähigen Bewertungsrahmen für die Erörterung potentiell kritischer Direktinvestitionen bieten. Sie würde insbesondere aufzeigen, wo und wie sich bereits sicherheitliche Implikationen manifestieren, die durch anstehende Projekte entstehen oder verstärkt werden. Die Gesamtrechnung würde ebenfalls anzeigen, wo im Interesse der nationalen Sicherheit durch geeignete Maßnahmen gegenzusteuern ist. Mit einem solchen Ansatz würden die anstehenden Bemühungen um eine Bestandsaufnahme der Gefährdungslage für Kritische Infrastruktur[16] in einem besonders exponierten Bereich maßgeblich ergänzt. Sie würde im Übrigen auch im Bereich der wissenschaftlichen Zusammenarbeit mehr als angezeigt sein, in der ebenfalls erhebliche spezifische know-how-Abflüsse zu verzeichnen und zu besorgen sind, die ihrerseits ebenfalls von potentiell hoher nachrichtendienstlicher und sicherheitlicher Relevanz sind[17].

Darüber hinaus wäre eine solche Risikogesamtrechnung auch bei Direktinvestitionen einer ganzen Reihe anderer internationaler Akteure geboten. Sie sollte aus hiesiger Sicht zur verpflichtenden Grundlage für entsprechende Entscheidungs- und Genehmigungsverfahren werden. Vor allem aber würden so auch evidenzbasierte Voraussetzungen für eine Nationale Sicherheitsstrategie geschaffen, die ohne diese Grundlagenarbeit weitgehend im Bereich der Wünsche und Hoffnungen stecken bliebe.

Für den Vorstand des GKND

Gez.

Dr. Gerhard Conrad

[16] Vgl. bereits die umfänglichen Hinweise in GKND-Monitor 17.10. und 24.10.2022

[17] S. hierzu jüngst: Geopolitisches Dilemma für die Wissenschaft: China ist Kooperationspartner – und Systemkonkurrent (Tagesspiegel, 27.10.2022)