China, 5G und die Sicherheit der Allianz: Russlands Krieg unterstreicht die Notwendigkeit der Beschlüsse der NATO-Gipfel 2021/22

Diese Zusammenfassung enthält die wichtigsten Ergebnisse eines von GMF veranstalteten runden Tisches unter Chatham-House-Regeln, bei dem Expertinnen und Experten aus Europa und den Vereinigten Staaten diskutiert haben, wie die Themen China, 5G, Resilienz und kritische Infrastruktur im Rahmen der NATO behandelt werden. Die Veranstaltung fand bereits 2021 statt, aber die Schlussfolgerungen und Analysen wurden nach Russlands Invasion in der Ukraine und dem NATO-Gipfel in Madrid im Juni 2022 ergänzt.

- Der russische Einmarsch in die Ukraine unterstreicht die unverzichtbare Rolle der NATO für die Sicherheit der europäischen Verbündeten. Gleichzeitig hat die Ankündigung Chinas, eine Partnerschaft "without limits" mit Russland einzugehen, gezeigt, dass sich die NATO künftig auf eine erweiterte Bedrohungslage einstellen muss. Diese Entwicklung unterstreicht die Notwendigkeit, die NATO auf alle Dimensionen der neuen Sicherheitslage, mit der sie jetzt konfrontiert ist, vorzubereiten.
- Bei den drei Gipfeltreffen rund um den Europa-Besuch von US-Präsident Joe Biden im Sommer 2021 und dem NATO-Gipfel 2022 wurde deutlich, dass China in den kommenden Jahren ein zentraler Faktor in den transatlantischen Beziehungen sein wird. Die Interessen Chinas kollidieren in mehrfacher Hinsicht mit der Aufgabe der NATO und nehmen in den Diskussionen innerhalb des Bündnisses mehr Raum ein als je zuvor. Die NATO befindet sich zwar nicht in einem militärischen Konflikt mit China, dennoch ist China ein geopolitischer Konkurrent des „Westens" insgesamt. Mehr noch: Die USA betrachten China als direkte Bedrohung ihrer nationalen Sicherheit und es sind Szenarien denkbar, die die beiden Seiten in eine militärische Konfrontation führen könnten. Unter den europäischen NATO Mitglieder gibt es zwar bezüglich einer Bedrohung durch China unterschiedlichen Auffassungen, doch machen sie sich – im Gegenzug für Sicherheitsgarantien – traditionell Teile der Sicherheits- und Verteidigungsagenda der USA zu eigen. Von China gehen zudem zahlreiche Risiken speziell für die europäische Sicherheit aus. Angesichts der starken Abhängigkeit der digitalen Infrastruktur Europas, vor allem Deutschlands, von chinesischer Technologie kommt dem Thema „Resilienzkritischer Infrastrukturen" eine besondere Bedeutung zu. In der aktuellen Debatte geht es darum, ob die NATO eine geeignete Plattform zur Diskussion dieser Fragen ist, ob die EU stattdessen eine aktivere Rolle übernehmen sollte oder ob sich die Zuständigkeiten sinnvoll zwischen beiden Organisationen aufteilen lassen.
- Telekommunikation wurde von der NATO als ein neuer Schwerpunktbereich definiert. Damit die NATO ihre Hauptaufgabe der kollektiven Verteidigung erfüllen kann, ist eine resiliente zivile Infrastruktur, die hybriden Angriffen standhält, auf dem Gebiet der NATO essentiell. In den meisten europäischen Ländern befindet sich diese Infrastruktur in der Regel in Privatbesitz. Daher unterliegt sie privatwirtschaftlichen Entscheidungen, bei denen Aspekten der nationalen Sicherheit nicht das notwendige Gewicht zukommt, wenn sie nicht eindeutig gesetzlich geregelt sind. Dabei ist zu berücksichtigen, dass nicht nur Russland als staatlicher Akteur auf dem Gebiet der NATO mit hybriden Taktiken unterschiedlichster Art agiert, sondern auch China damit begonnen hat , verschiedene ausgefeilte politische und nicht-militärische Taktiken gegenüber der NATO als Ganzes und gegenüber einzelnen Ländern anzuwenden, um seinen politischen und wirtschaftlichen Einfluss auszuweiten.

- Damit Resilienz als Katalysator für eine engere Zusammenarbeit zwischen der NATO und der EU wirken kann, muss ein Gleichgewicht gefunden werden, bei dem die Rollen beider Organisationen eindeutig definiert sind. Heute verfolgt die NATO eine robuste Strategie auch im nicht-militärischen Bereich. Ihre Aufgaben liegen hier vor allem in der politischen Koordinierung und Konsultation, Krisenmanagement und der kollektiven Verteidigung sowie bei Fragen der Interoperabilität für die militärische Nutzung der Technologie. Die EU wiederum verfügt über eine Reihe von Instrumenten, von der 5G-Toolbox bis hin zum Europäischen Aktionsplan für Demokratie, die einige der umfassenderen Aspekte der Resilienz adressieren. Es ist daher sinnvoll, gemeinsame Grundlagen und Verantwortlichkeiten zwischen der EU und der NATO festzulegen. Zudem muss eine engere Verzahnung zwischen den traditionellen militärischen Anforderungen und den Notwendigkeiten in Bezug auf die Stärkung der Resilienz erreicht werden. Dieser komplementäre Ansatz wird eine der wichtigsten Säulen für die künftige Zusammenarbeit zwischen der NATO und der EU sein.
- Unklarheit besteht nach wie vor darüber, ob der Schutz der zivilen Infrastruktur in Europa in den Zuständigkeitsbereich der NATO fallen würde. Mit anderen Worten: Würde ein Cyber-Angriff auf die zivile Infrastruktur in Europa den Bündnisfall nach Artikel 5 auslösen? Wenn nicht, ist dann statt der NATO die EU zuständig? Diese Fragen müssen eindeutig geklärt werden, zumal die Grenzen zwischen ziviler und militärischer Infrastruktur fließend sind, insbesondere im Bereich der Telekommunikation.
- Private und öffentliche Telekommunikationsnetze werden für das Funktionieren unserer Gesellschaft und unserer Wirtschaft immer wichtiger und sind eine Voraussetzung für Innovationen. Diese beiden Dimensionen spielen im Wettlauf um technologische Führerschaft eine wichtige Rolle. Technologie ist und bleibt der Schlüssel für eine glaubhafte Abschreckung und Verteidigung. Technologische Überlegenheit sichert nicht nur die Vorherrschaft auf dem Schlachtfeld, sondern auch darüber hinaus. Eine solche Überlegenheit hängt von einer robusten und sich ständig weiterentwickelnden industriellen Basis ab, die zivile und militärische Innovationen, sowie Forschung und Entwicklung integriert. Gemeinsame Innovationsinitiativen auf beiden Seiten des Atlantiks sind notwendig, um kritische Fähigkeiten auf und neben dem Schlachtfeld zu erhalten und zu verbessern. Dies erfordert bessere und effizientere Kooperation zwischen der militärischen und der zivilen Industrie. Die NATO muss effektive Wege finden, um die wirtschaftlichen Aspekte zentraler Elemente ihrer Sicherheitspolitik zu integrieren – insbesondere, weil Industriepolitik in Europa und den USA wieder in den Vordergrund der nationalen Diskussion rückt. Um die Resilienz und den Wettbewerbsvorsprung des Bündnisses zu stärken bzw. zu erhalten, müssen neue politische Kanäle geschaffen werden, die eine solche Integration erleichtern.
- Derzeit sieht es so aus, als ob die NATO sich mit dieser Rolle schwertut. Daher müssen die in ihren Zuständigkeitsbereich fallenden Fragen genau identifiziert und kategorisiert werden. Ein erster Schritt für die politisch Verantwortlichen besteht darin, klar zu definieren, unter welchen Bedingungen Geschäfte mit China die nationale Sicherheit nicht gefährden würden. Die NATO ist bestens geeignet, als Plattform für den sicherheitspolitischen Austausch mit verschiedenen Institutionen, nichtstaatlichen Einrichtungen und NATO-Partnern, die Erfahrung im Umgang mit China haben, etwa Japan und Südkorea, zusammenzuarbeiten. Dabei sollte die NATO weiterhin der digitalen Infrastruktur (5G/Advanced, Unterseekabel, perspektivisch 6G) sowie Chinas Bedrohungspotenzial Priorität einräumen und diese beiden Punkte ganz oben auf ihrer Agenda belassen.
- Da Cyber-Bedrohungen für die NATO seit langem ein Problem darstellen, sind 5G-Netze ganz natürlich in den Fokus der NATO-Diskussionen gerückt – auch wenn das Thema der Abwehr solcher Bedrohungen nur sehr langsam Bedeutung gewonnen hat. Darüber hinaus ist die Art und Weise, wie Daten verarbeitet und gespeichert werden, ein wichtiger sicherheitsrelevanter Aspekt, der nicht aus dem Blickfeld geraten darf. Dem Schutz unseres öffentlichen Sektors und unserer Industrie sowie der Gewährleistung, dass Unternehmen, Bürgerinnen und Bürger sowie staatliche Institutionen die Möglichkeit haben, ihre Daten Ende-zu-Ende über ein nicht-chinesisches Netz zu transportieren, kommt hierbei eine

besondere Bedeutung zu**.** Bei 5G zum Beispiel wird die Cloud-Infrastruktur eine wichtige Rolle spielen. Nach chinesischem Recht kann die chinesische Regierung aus Gründen der „öffentlichen Sicherheit“ jederzeit alle Daten anfordern, die private chinesische Unternehmen – auch außerhalb Chinas – sammeln, was bedeutet, dass alle Daten in einer chinesischen 5G-Cloud gefährdet sind. In Belgien beispielsweise war die gesamte Telekommunikationsinfrastruktur des Landes bisher auf chinesische Ausrüstung angewiesen, auch die von den EU- und NATO-Behörden genutzten Mobilfunknetze. Ähnlich weit verbreitet ist auch noch heute chinesische Ausrüstung in deutschen Netzen – was bedeutet, dass praktisch der gesamte Mobilfunkverkehr aller in Deutschland stationierten NATO-Truppen irgendwann über ein Netzelement läuft, das chinesische Technologie nutzt. Das neue deutsche IT-Sicherheitsgesetz verweist zu Recht auf die Sicherheitsbedürfnisse der NATO, wenn es darum geht, die Vertrauenswürdigkeit von Anbietern zu bewerten. Es zeigt zudem, dass Ziele und deren Umsetzung weit auseinanderklaffen können: Seit dem Inkrafttreten des Gesetzes im vergangenen Jahr ist der Anteil von Huawei am 5G-Netz der Deutschen Telekom auf weit über 60 % gestiegen. Beim Launch der von Huawei aufgebauten und betriebenen Cloud der Deutschen Telekom 2020 war das CERN, die europäische Organisation für Kernforschung, ein wichtiger Referenzkunde. Das heißt, das weltweit führende Kernforschungszentrum speichert Daten in einer chinesischen Cloud. Dabei sollte es eine Mindestanforderung sein, dass Netze, die Funktionen für Regierungs- und Behördennetze, die Verteidigungsindustrie und den Bereich der inneren Sicherheit erfüllen, ohne chinesische Technik auskommen. Gleiches gilt für Netzwerke, die kritische Funktionen für die Gesellschaft erfüllen, etwa bei Versorgungsdiensten, in der Pharmaindustrie, im Gesundheits- und Bankwesen oder im Transport- und Kommunikationssektor.

- Die osteuropäischen NATO-Verbündeten haben bisher eine verstärkte Aufmerksamkeit der NATO für China eher kritisch gesehen, da sie befürchteten, dies könnte von der Bedrohung durch Russland ablenken. Die letzten Monate haben gezeigt, dass die NATO beides tun muss: sich mit den Bedrohungen aus Russland und aus China auseinandersetzen – schließlich hängen sie eng zusammen. Der Krieg gegen die Ukraine hat auf drastische Weise gezeigt, wie real die Gefahr einer Aggression durch das russische Regime ist. Andererseits unterstreichen Chinas immer engere Beziehungen zu Russland, seine ausdrückliche Unterstützung für Russlands Haltung zur NATO, der volle Einsatz seiner Propaganda zugunsten der Positionen Moskaus und die latente Aussicht, dass Peking mit wirtschaftlicher Unterstützung – oder sogar Waffenlieferungen – einspringen könnte, dass die „grenzenlose“ chinesisch-russische Kooperation vor allem eine Kooperation gegen den Westen bedeutet. Die NATO muss in Betracht ziehen, dass sich die gemeinsamen chinesisch-russischen Fähigkeiten sowohl auf russische Ziele in Europa und chinesische Ziele in Asien als auch auf gemeinsame Interessen in anderen Regionen richten.

- Daraus ergibt sich ein drastisch erhöhtes Sicherheitsrisiko durch chinesische Telekommunikationsausrüstung in den Netzen der europäischen Verbündeten. Während die NATO angesichts der russischen Bedrohung ihre militärischen Verteidigungskapazitäten an ihrer Ostgrenze ausbaut, kommt in den Telekommunikationsnetzen Polens, Tschechiens, Rumäniens und anderer Länder nach wie vor in hohem Maße chinesische Technik zum Einsatz. Mehr noch: Keines dieser Länder garantiert den Ausbau von Equipment nicht-vertrauenswürdiger Anbieter in den kommenden Jahren. Die strengsten Vorschriften beschränken zwar das Verbauen weiterer chinesischer Technik, nehmen aber das Risiko nicht-vertrauenswürdiger Altausrüstung bis Mitte des Jahrzehnts und länger in Kauf – ein kaum akzeptabler Zustand. Die Möglichkeit, dass China Russland im Falle eines Konflikts über Huawei oder ZTE Zugang etwa zu polnischen Telekommunikationsnetzen verschaffen könnte, ist real und hätte dramatische Folgen.

- Die Kosten für einen Verzicht auf chinesische Telekommunikationsinfrastruktur in Europa sind moderat wenn die Betreiber den 5G Ausbau von Beginn an nutzen. Dabei wird veraltetes Equipment ohnehin ersetzt. Allerdings könnte so die Umsetzung eines vollständigen Verbots der Nutzung neuer Huawei-Ausrüstung „auf natürliche Weise“ etwa sechs Jahre dauern, denn erst dann wäre die gesamten installierten Komponenten nicht

vertrauenswürdiger Anbieter aus Altersgründen ausgetauscht – besonders kritisch sind die Fälle, in denen erst vor Kurzem eine Netzmodernisierung mit chinesischen Komponenten begonnen hat, wie z.B. in Deutschland. Aus Gründen der nationalen Sicherheit muss der Übergang zu vertrauenswürdiger Technologie schneller gelingen, wobei kurzfristige kommerzielle Erwägungen hinsichtlich der Auslaufzeiten nicht das Tempo bestimmen sollten. Eine der immer wiederkehrenden Mythen ist, dass chinesische Anbieter technologisch fortschrittlicher seien als europäische Anbieter. Die USA und Südkorea gelten als Vorreiter beim Rollout von 5G-Netzen. Hier wurden die ersten 5G Netze ausgebaut und hier kommen die modernste 5G Varianten zur kommerziellen Anwendung. Ihre Infrastruktur wurde ohne chinesische Geräte aufgebaut und basiert stattdessen hauptsächlich auf europäischer und südkoreanischer Technologie. Auch bei den Preisen können die europäischen Anbieter mit ihren chinesischen Konkurrenten mithalten – nicht aber mit dem chinesischen Staat. Chinas Subventionen für einheimische Unternehmen, die auf globalen Märkten aktiv sind, sowie die Bevorzugung chinesischer Unternehmen auf dem heimischen Markt sorgen weiterhin für ungleiche Wettbewerbsbedingungen. Am dringlichsten ist das Problem für die kleineren Betreiber in Europa, Lateinamerika und Asien, die eine schwächere Kreditwürdigkeit haben und daher auf chinesische Kredite zurückgreifen müssen, wenn keine alternativen Finanzierungsmechanismen angeboten werden. Seit einiger Zeit wird „Open-RAN“ als eine Alternative zu klassischen Mobilfunknetzen diskutiert und als eine Möglichkeit, die Abhängigkeit von chinesischer Technologie zu beenden. Tatsächlich hat China jedoch eine erhebliche institutionelle Präsenz und entsprechenden Einfluss bei der ORAN Entwicklung, was sicherheitsrelevante Fragen aufwirft. Eine umfassende Risikobewertung ist notwendig, damit ausgeschlossen werden kann, dass sich ORAN nicht als trojanische Pferd herausstellt.

- Die EU-Toolbox für 5G-Sicherheit ist ein guter Ausgangspunkt für weitere Schritte. Da die Toolbox jedoch nicht verbindlich ist, wird sie in den einzelnen EU-Mitgliedstaaten unterschiedlich ausgelegt und umgesetzt, was zu Sicherheitslücken führt. Ein konkreter nächster Schritt könnte darin bestehen, für eine konsequentere Umsetzung der Toolbox in der gesamten EU zu sorgen. Dabei kann jedoch die EU-Toolbox für 5G nur der Anfang sein. Netze, die kritische Ressourcen über Glasfaser-, Transport- und Unterseekabel miteinander verbinden, erfordern die gleiche sorgfältige Prüfung und strenge Umsetzung von Schutzmaßnahmen wie Zugangs- und Kernnetz des Mobilfunks. Politische und regulatorische Maßnahmen, welche die Vertrauenswürdigkeit der gesamten Telekommunikationsinfrastruktur adressieren sind notwendig.

- Die differenzierte und nuancierten Formulierungen der NATO-Gipfel 2021/22 sollten nicht darüber hinweg täuschen, dass sich die Verbündeten einig sind, dass Chinas Verhalten unsere demokratischen Grundwerte und unsere nationale Sicherheit bedroht. Daher ist die systemische Herausforderung, die von China ausgeht, in der NATO zu einem zentralen Thema geworden; sie wird durch die engere russisch-chinesische Zusammenarbeit noch verstärkt. Die Politik der Allianz gegenüber China wurde in dem neuen Strategischen Konzept der NATO konkretisiert, das während des NATO-Gipfeltreffens in Madrid verabschiedet wurde. Die Aufgabe der NATO ist es, den vielfältigen und unterschiedlichen aktuellen Sicherheitsbedrohungen gleichzeitig zu begegnen: hybride Abschreckung, Bedrohungen durch disruptive Technologien und eine verwundbare kritische Infrastruktur. Angesichts einer sich rasch verändernden Sicherheitslandschaft und der rasanten technologischen Entwicklung wird es für den weiteren Erfolg der NATO von entscheidender Bedeutung sein, die Fähigkeit und Entschlossenheit zu entwickeln in all diesen Bereichen erfolgreich zu sein.