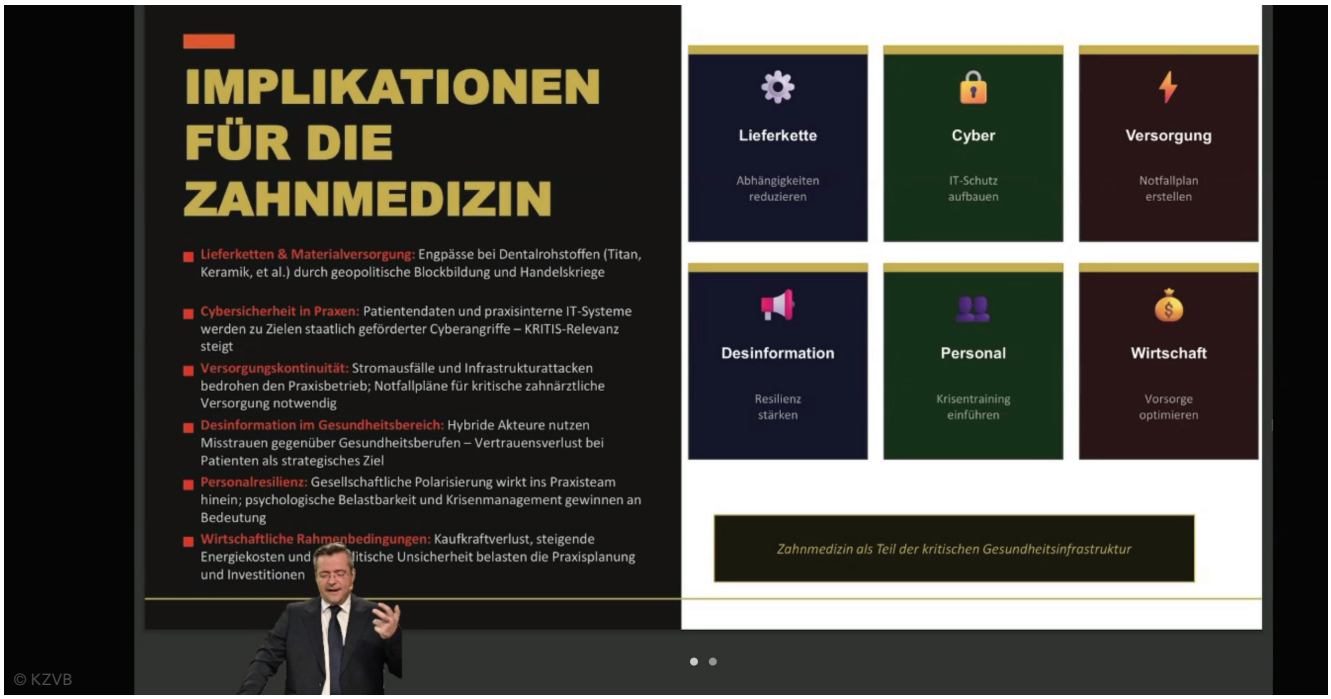
„Wir müssen resilienter werden“

Wie die Weltpolitik unseren Alltag beeinflusst

Globale Konflikte wirken sich unmittelbar auf den Alltag in Deutschland aus. Ein Beispiel dafür sind die steigenden Ölpreise nach den Angriffen der USA und Israels auf den Iran. Dr. Konstantinos Tsetsos ist Politikwissenschaftler an der Universität der Bundeswehr in München. Wir sprachen mit ihm darüber, wie sich Zahnärzte beruflich und privat auf neue Bedrohungen vorbereiten können.



Bei einer Onlinefortbildung der KZVB empfahl Dr. Konstantinos Tsetsos den Zahnarztpraxen, sich auf neue Bedrohungen vorzubereiten.

BZB: Sie nennen die moderne Kriegsführung teleologisch hybrid. Was hat man darunter zu verstehen?
Tsetos: Der Begriff Teleologische Hybride Kriegsführung (THK) beschreibt eine Kriegsführungsform der fünften Generation, bei der hybride – also physische und immaterielle – Mittel konsequent auf klar definierte strategische Endzwecke ausgerichtet werden. Das Wort teleologisch bezieht sich auf die Erklärung von Dingen durch ihre Ziele und Zwecke. In der Praxis bedeutet das: Jede hybride Maßnahme, sei es eine Desinformationskampagne, ein Cyberangriff, strategische Korruption oder die Instrumentalisierung von Migration, dient einem von zwei übergeordneten Zielen.

Das erste Ziel ist die physische Schwächung und Paralysierung des Gegners. Durch permanente, kinetische und nichtkinetische Nadelstiche sollen gesellschaftliche Entscheidungsprozesse, Wirtschafts- und Kommunikationsabläufe sowie die soziale Kohäsion eines Zielstaates gestört werden – als Vorbereitung auf einen möglichen konventionellen Konflikt. Man spricht hier auch vom Stören oder ständigen Resetten des OODA-Loops (Observe-Orient-Decide-Act) des Gegners. Das zweite Ziel ist die vollständige Übernahme der Realität des Gegners durch rein nichtkinetische psychologisch-kognitive Einflussnahme. Wenn es einem Akteur gelingt, die Wahrnehmung der Bevölkerung und der Entscheidungsträger eines Zielstaates so zu dominieren, dass sie faktisch im Interesse des Angreifers handeln, ist das ein psychologisch-kognitiver Sieg – ganz ohne physische Invasion. Russlands aktuelles Vorgehen gegenüber Europa vereint beide Dimensionen. China hingegen setzt zunehmend auf die rein immaterielle, rein psychologisch-kognitive Herangehensweise, um uns langfristig zu unterwandern.

BZB: Wer sind unsere Gegner und welche Ziele verfolgen sie?
Tsetsos: Die zentralen revisionistischen Akteure sind Russland und China, die gemeinsam die regelbasierte internationale Ordnung unter Druck setzen. Russland agiert dabei als unmittelbarer militärischer

und hybrider Bedrohungsakteur, insbesondere gegenüber der EU/NATO-Ostflanke. Moskaus strategisches Ziel ist es, die strategische Schlüsselregion entlang seiner Grenzen als Pufferzone zu etablieren, den Zusammenhalt des Westens zu untergraben und letztlich die europäische Einheit, Verteidigungsfähigkeit und weitere Integrationskapazität zu zersetzen. Im Idealfall erhofft sich der Kreml einen Erfolg durch die vollständige Übernahme politischer Realitäten in Zielländern – ohne einen einzigen konventionellen Schuss abzufeuern.

China wiederum verfolgt eine systemische Rivalität mit den USA und dem Westen, die über Wirtschaftspolitik, technologische Dominanz und die Ausdehnung geopolitischer Einflusszonen geführt wird. Beide Akteure profitieren voneinander: Wenn Russland die europäische Aufmerksamkeit und Ressourcen bindet, entlastet das China in seinem strategischen Wettbewerb im Indopazifik. Das übergeordnete Ziel beider Mächte ist die Schwächung demokratischer Institutionen, das Erodieren von Vertrauen in westliche Allianzen und die Etablierung eines multipolaren Systems, in dem autoritäre Ordnungsmodelle als gleichwertig oder überlegen erscheinen. Die größte Gefahr aus Sicht Chinas und Russlands ist daher unsere pluralistische, demokratische und liberale Regierungsform und Lebensweise, die es Autokratien unmöglich macht, totale Kontrolle über Bevölkerungen auszuüben.

BZB: Sie sprechen von einer Abwärtsspirale der Demokratien. Auch in Deutschland erstarken extreme Randparteien. Glauben Sie, dass Russland und China Einfluss auf unseren politischen Entscheidungsprozess nehmen?

Tsetsos: Ja, und dieser Einfluss ist dokumentiert und systematisch. In meinen Studien beschreibe ich, wie Russland durch gezielte strategische Korruption ein Netzwerk sogenannter Useful Idiots aufbaut – lokale und nationale Politiker, Unternehmer und Influencer, die schrittweise, oft unbewusst, die Interessen Moskaus vertreten.

Über Beraterverträge, verdeckte Spenden, Scheinkonferenzen und sogenannte Honey Traps (sexuelle Anbahnung) werden Zielpersonen schrittweise in den russischen Orbit gezogen. Aus diesen werden dann Weaponized Idiots, die in nationalen Parlamenten und EU-Institutionen aktiv gegen deutsche und europäische Interessen arbeiten.

Hinzu kommt eine massive Desinformationsinfrastruktur: Trollfabriken, KI-gestützte Bots und infiltrierte Medienpläne verbreiten antiwestliche Narrative und stärken populistische Kräfte. Algorithmen in sozialen Medien erzeugen Filterblasen, die kritisches Denken erschweren und Manipulation begünstigen. Das Ziel ist nicht unbedingt, eine bestimmte Partei an die Macht zu bringen, sondern die Gesellschaft so zu spalten und zu lähmen, dass demokratische Entscheidungsfindung ausgehöhlt wird. Die globale Demokratieentwicklung zeigt, dass wir uns seit den 2000er-Jahren in einer Phase des Democratic Backsliding befinden – dieser Trend ist kein Zufall, sondern auch das Ergebnis gezielter Einflussoperationen.

PRAXISTIPP

BZB: Wir erleben bereits seit Jahren Cyberattacken – auch auf Gesundheitseinrichtungen. Rechnen Sie damit, dass solche Angriffe zunehmen?
Tsetsos: Absolut, und das ist systembedingt. Cyberangriffe auf kritische Infrastrukturen, Krankenhäuser sowie Gesundheitseinrichtungen gehören eindeutig dazu, da sie ein zentrales Instrument der physischen teleologischen hybriden Kriegsführung sind. Das Ziel ist die Störung der Regierungsfähigkeit sowie ein Paralysieren der Resilienz der Gesellschaft. Wenn Kliniken ausfallen, Menschen keine medizinische Versorgung erhalten und das Vertrauen in staatliche Schutzfähigkeit schwindet, ist das exakt das Ergebnis, das die Angreifer beabsichtigen.

Das Repertoire hybrider Angriffsmittel ist nahezu grenzenlos. Wir sehen bereits Social-Engineering-Angriffe auf Kuratoren von Softwarestandards, um Backdoors zu etablieren, das Durchtrennen von Unterseekabeln durch Handelsschiffe und koordinierte Ransomware-Attacken auf kritische Einrichtungen. Die Zunahme dieser Angriffe ist keine Frage des Ob, sondern des Wie und Wann. Gesundheitsdaten sind zudem besonders sensibel und erpressungsrelevant. Praxen und Kliniken stehen vor der Herausforderung, dass sie einerseits stark vernetzt sein müssen, um effizient zu arbeiten, andererseits genau diese Vernetzung Angriffsflächen bietet. Besondere Vorsicht gilt bei der gesamten digitalen Lieferkette von Medizingeräten über Praxisverwaltungssoftware bis hin zu Cloud-Diensten. Wer vermeintlich günstig aus China importiert, holt sich in manchen Fällen bereits die Schadsoftware oder eine Backdoor in die Praxis.



„Die Geopolitik sollte man auch bei der Vermögensanlage berücksichtigen", betonten Manuela Probst und Max Drexler (rechts) von der Deutschen Bank.

PRAXISTIPP

BZB: Wie können Praxen resilienter gegenüber möglichen Krisenszenarien werden?
Tsetsos: Resilienz entsteht durch Vorbereitung, Redundanz und Vernetzung. Auf der operativen Ebene empfehle ich zunächst eine ehrliche Bestandsaufnahme: Welche digitalen Systeme sind kritisch? Was passiert, wenn der Strom ausfällt, das Internet wegbricht oder die Praxissoftware blockiert wird? Dann gilt es, analoge Rückfalllösungen zu planen – sei es das Vorhalten von Papierformularen für Notfälle, redundante Kommunikationswege oder regelmäßige Offline-Back-ups wichtiger Patientendaten. Auf der strategischen Ebene geht es um die Einbindung in lokale und regionale Krisenstrukturen. Praxisinhaber sollten die Kontakte zu lokalen Gesundheitsbehörden, Katastrophenschutz und Kassen(zahn)ärztlichen Vereinigungen aktiv pflegen und wissen, wie im Krisenfall Informationen fließen.

Ein oft unterschätzter Hebel liegt in der gezielten Kooperation zwischen Praxen untereinander. Einzelne niedergelassene Ärztinnen und Ärzte stoßen bei der Absicherung ihrer digitalen Infrastruktur schnell an wirtschaftliche Grenzen, da professionelle IT-Sicherheitslösungen, regelmäßige Penetrationstests oder ein dezidierter IT-Notfallplan die Kapazitäten einer Einzelpraxis häufig übersteigen. Schließen sich mehrere Praxen zu einem lokalen Verbund zusammen, verändert sich diese Rechnung grundlegend. Gemeinsam lassen sich Managed-Security-Dienste, verschlüsselte Back-up-Infrastrukturen oder eine geteilte IT-Betreuung zu Konditionen einkaufen, die für die einzelne Praxis schlicht nicht erreichbar wären.

Dieselbe Logik gilt für die materielle Vorhaltefähigkeit. Eine Praxis, die allein Schutzmaterial, Notfallmedikamente oder Verbrauchsmaterialien für Krisenszenarien bevorraten will, bindet erhebliches Kapital und Lagerkapazität. Über gemeinsames Storing, also das koordinierte, rotationsbasierte Einlagern von Vorräten innerhalb eines Praxisverbundes, lässt sich eine wirtschaftlich tragfähige Bevorratung aufbauen, ohne dass jede einzelne Praxis die volle Last trägt. Entscheidend dabei ist eine klare Vereinbarung über Zugriff, Verantwortung und regelmäßige Auffrischung der Bestände, damit die gemeinsame Reserve im Ernstfall tatsächlich verfügbar und nutzbar ist.

BZB: Wie kann Europa wirtschaftlich und militärisch im Wettbewerb mit den alten und neuen Großmächten bestehen?
Tsetsos: Europa muss nach innen institutionell resilienter werden und nach außen durch stabile demokratische Allianzen seine Handlungsfähigkeit sichern. Das ist meine Kernthese zur Zukunft globaler demokratischer Allianzen. Konkret bedeutet das militärisch: eine Vertiefung europäischer Rüstungskooperation inklusive klarer Systemführerschaften, die Aufstellung ständiger europäischer Flottenverbände, die Stärkung der EU-Battlegroups als Ergänzung zu NATO-Reaktionskräften sowie die Ausweitung von NATO-Partnerschaften mit gleichgesinnten Demokratien wie Japan, Südkorea, Indien, Australien und Brasilien. Deutschland kommt dabei eine Schlüsselrolle zu: Berlin muss mehr sicherheitspolitische Verantwortung übernehmen.

Wirtschaftlich geht es um die Reduktion kritischer Abhängigkeiten bei Halbleitern, Batterien, seltenen Erden und Pharmazeutika sowie um die Stärkung technologischer Souveränität. Ein transatlantisches Handelsabkommen im Geiste eines TTIP 2.0 mit gemeinsamen Standards und resilienten Lieferketten wäre ein wichtiger Schritt. Das wahrscheinlichste Szenario bis 2035 sieht vor, dass Europa trotz geschwächter transatlantischer Kohärenz durch vertiefte demokratische Integration seine strategische Handlungsfähigkeit bewahrt. Die zentrale Herausforderung dabei bleibt, sicherheitspolitische und wirtschaftliche Kosten innenpolitisch zu legitimieren, ohne die gesellschaftliche Akzeptanz zu verlieren.

BZB: Welche Fähigkeiten braucht die Bundeswehr und lassen sich die mit dem 100 + 500 Milliarden Sondervermögen erreichen?
Tsetsos: Neben der konventionellen Rüstung für den Verteidigungsfall im Zuge

eines konventionellen Krieges benötigt die Bundeswehr vor allem drei Fähigkeitsbereiche, um hybriden Bedrohungen wirksam zu begegnen. Erstens benötigen wir erweiterte Aufklärungsfähigkeiten für den Ausbau der Prüfung digitaler Räume, die systematische Analyse von Desinformationskampagnen und das Erkennen physischer Sabotageakte. Spezialisierte Cyber- und Intelligence-Einheiten spielen dabei eine Schlüsselrolle. Zudem brauchen wir spezialisierte Einsatzkräfte für hybride Lagen, die sowohl physische als auch kognitive Kriegsführung abdecken und hybride Operationen defensiv abwehren sowie proaktiv kontern können. Drittens muss der Fokus auf der Resilienz kritischer Infrastrukturen und Lieferketten liegen – von Unterseekabeln über Energieversorgung bis zur digitalen Infrastruktur.

Das Sondervermögen ist ein wichtiger Schritt, aber es reicht nicht. Der entscheidende Faktor ist ein ressortgemeinsamer Ansatz, der zivile, gesellschaftliche und technologische Aspekte einbindet. Die Bundeswehr darf sich nicht aus sozialen Medien zurückziehen – das überlässt gegensätzlichen Narrativen kampflos den Informationsraum. Stattdessen braucht sie enge Kooperationen mit zivilen Medienplattformen und muss Medienkompetenz sowie psychologische Widerstandskraft des eigenen Personals fördern. Zudem muss der Klimawandel stärker in strategische Überlegungen einbezogen werden. Er erzeugt Vulnerabilitäten, die von hybriden Akteuren gezielt ausgenutzt werden können. Letztlich benötigen wir enorme Investitionen in politische und staatsbürgerliche Bildung und Forschung, um sicherzustellen, dass sich unsere Demokratie nicht von innen heraus zersetzt.

BZB: Sie sehen auch im Klimawandel Gefahren für die Stabilität von Gesellschaften. Welche Risiken sind für Deutschland und Europa damit verbunden?

Tsetsos: Deutschland verzeichnet bereits heute eine um 1,6 Grad Celsius höhere Durchschnittstemperatur gegenüber dem Jahr 1881. Der Trend zu häufigeren, stärkeren und länger andauernden Extremwetterereignissen ist erkennbar: Überschwemmungen, Waldbrände, Dürren, Hitzewellen. Die sicherheitspolitischen Klimaauswirkungen zeigen, dass der Klimawandel nicht isoliert betrachtet werden kann – er verstärkt bereits bestehende gesellschaftliche, politische und ökonomische Vulnerabilitäten, die auch im Globalen Norden bereits Bestand haben. Besonders gefährlich ist die Schnittstelle zwischen Klimawandel und hybrider Bedrohung. In einem von mir erstellen Szenario bis 2050 nutzt der russische Geheimdienst die durch Dürreperioden entstehende Trockenheit aus, um Schläferzellen in Deutschland mithilfe KI-gestützter Radikalisierungskampagnen zu aktivieren. Die werden dann für koordinierte Brandstiftung in deutschen Waldgebieten mit dem Ziel eingesetzt, staatliche Krisenmanagementorgane zu überlasten und die Regierung in Handlungsunfähigkeit zu stürzen. Was als Naturkatastrophe beginnt, entpuppt sich als hybrider Angriff. Deutschland benötigt daher ein nationales zivil-militärisches Einsatzführungssystem zur Krisenbewältigung, höhere Investitionen in Bundeswehr-Helikopter und Löschflugzeuge sowie einen engeren Koordinationsmechanismus zwischen Bund und Ländern im Krisenfall.

Die Fragen stellte Leo Hofmeier.

PRAXISTIPP

BZB: Die globalen Krisen beeinflussen auch unsere Psyche. Was sollten Praxisinhaber vor diesem Hintergrund tun, um die Mitarbeiter zu motivieren?
Tsetsos: Die psychologisch-kognitive Dimension der aktuellen Bedrohungslage zielt bewusst darauf ab, gesellschaftliche Erschöpfung, Zukunftsangst und politische Verdrossenheit zu erzeugen. Wer ständig mit Krisen konfrontiert wird, ohne das Gefühl zu haben, selbst etwas bewirken zu können, verliert Orientierung und Motivation. Das gilt für Gesellschaften, aber ebenso für Praxisteams. Mein Rat orientiert sich an dem, was auch auf gesellschaftlicher Ebene wirkt.

Erstens: Klare und ehrliche Kommunikation, denn Mitarbeiterinnen und Mitarbeiter brauchen keine Verharmlosung, aber auch keine Panikmache, sondern Einordnung, Kontext und Information darüber, was die Praxis tut, um vorbereitet zu sein. Zweitens: Handlungsfähigkeit stärken. Wer im Ernstfall weiß, was zu tun ist, reduziert die Angst erheblich. Hierbei hilft die regelmäßige Teilnahme an jährlichen Übungen der Rettungsdienste oder des THW, um Krisenszenarien zu üben. Mitarbeiter sollten dafür einen Tag im Jahr ggf. freigestellt werden. Drittens: Gemeinschaft und Sinn betonen. Gesundheitsversorgung ist systemrelevant und Praxisteams leisten in Krisenzeiten im erhöhten Maße unverzichtbare Arbeit. Stimmt der Teamgeist nicht, so leidet in der Regel die Kohäsion, Resilienz und Effektivität. Das sollte bewusst kommuniziert und wertgeschätzt werden. Die gesellschaftliche Legitimität sicherheitspolitischer Kosten hängt davon ab, ob Menschen den Zusammenhang zwischen ihrem eigenen Handeln und dem großen Ganzen verstehen. Wer eine Praxis führt, muss also auch Menschen führen, und auch dies gilt es, zu lernen oder zu üben.

Dr. Konstantinos Tsetsos ist Head of Foresight beim Metis Institut für Strategie und Vorausschau an der Universität der Bundeswehr München. Er forscht und berät das Bundesverteidigungsministerium zu strategisch relevanten Fragen der internationalen Politik. Seine Arbeiten umfassen Beiträge zu Geopolitik, Kriegstheorien und asymmetrische Kriege, Kriegsursachenforschung, hybride Kriegsführung, politische Risikoanalyse, strategische Vorausschau, zukunftsanalytische Sicherheitspolitik, Szenarioanalyse, maritime Sicherheit, zivil-militärische Zusammenarbeit, Katastrophen- und Krisenmanagement.