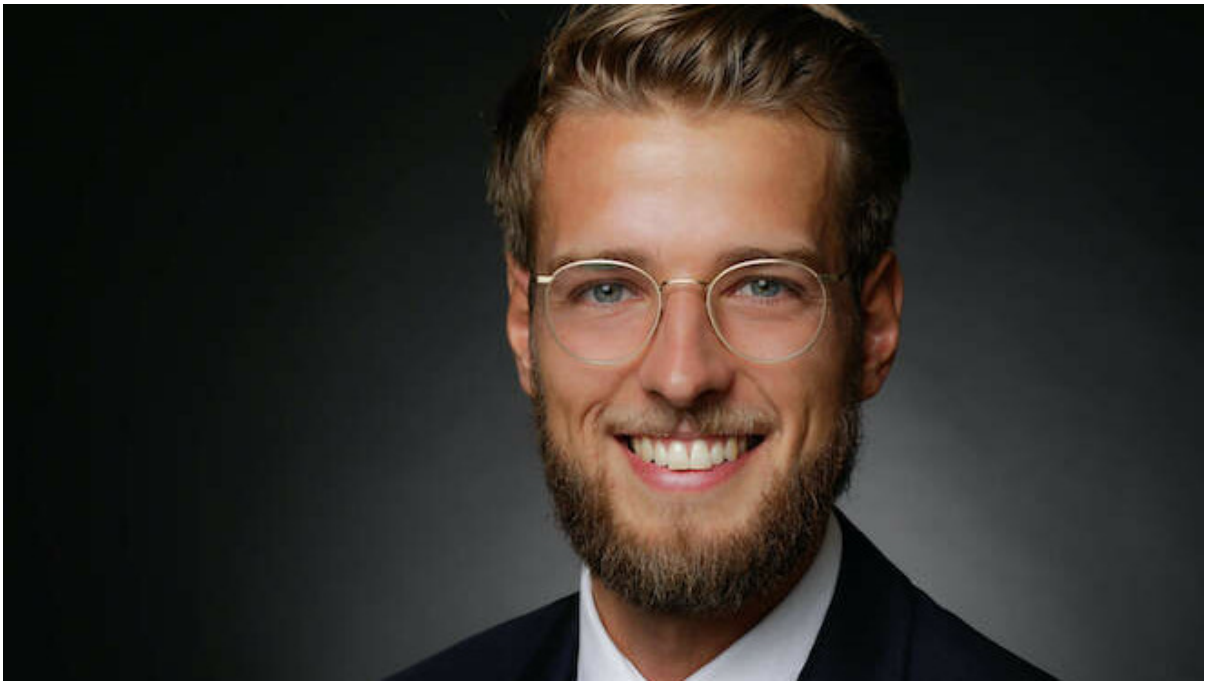
STANDPUNKT

Deutschland muss sich auf den hybriden Krieg vorbereiten

Von Ferdinand Gehringer



Ferdinand Gehringer ist Referent für Innere und Cybersicherheit bei der Konrad-Adenauer-Stiftung in Berlin.

Deutschland ist nicht auf hybride Bedrohungen vorbereitet, schreibt Ferdinand Gehringer, Referent für Innere und Cybersicherheit bei der Konrad-Adenauer-Stiftung. Er wirbt unter anderem für ein Abwehrzentrum gegen hybride Bedrohungen, in dem ein bundesweites Lagebild erstellt und analysiert wird.

Cyberangriffe auf Parteien, Kommunalverwaltungen oder auf sicherheitsrelevante Behörden, Desinformationskampagnen orchestriert durch digitale Manipulationsökosysteme, Sabotageakte an Stromtrassen oder Lichtwellenleiterkabeln der Deutschen Bahn, Spionagefälle in deutschen Sicherheitsbehörden: Die Anzahl und Dichte

der **hybriden Attacken auf Deutschland haben zugenommen**. Bei der öffentlichen Anhörung der Nachrichtendienste warnte der Präsident des Bundesamtes für Verfassungsschutz Thomas Haldenwang vor noch aggressiveren Angriffen Russlands, aus dem Sturm sei längst ein „veritabler Hurrikan“ geworden.

Deutschland im hybriden Krieg mit Russland

Hybride Bedrohungen sind Mittel, die aus dem kombinierten Einsatz verschiedener Instrumente, wie Cyberangriffe, gezielte Propaganda und Desinformation, Sabotage oder Spionage, Angriffe auf kritische Infrastrukturen, wirtschaftlicher Druck oder auch Migration bestehen. Die Angreifer nutzen die **Verwundbarkeiten der liberalen Gesellschaft,** der sozialen Marktwirtschaft, der demokratischen Willensbildung oder digitalisierter Prozesse aus. Die Ziele sind klar: Staatliche Belange beeinträchtigen, Gesellschaften verunsichern, destabilisieren und die öffentliche Meinung beeinflussen. Deutschland ist dabei vor allem im Fokus von Russland, aber auch China und der Iran werden zunehmend aktiver.

Bei einem **Angriff ist es für deutsche Sicherheitsbehörden nicht sofort ersichtlich**, ob es sich um eine militärische, nachrichtendienstliche Operation eines Staates oder um Aktivitäten privater beziehungsweise krimineller Gruppen handelt. Staatliche Angreifer nutzen diese Gruppen, um die Herkunft des Angriffs zu verschleiern. Die behördlichen Zuständigkeiten sind nicht immer klar und eine schnelle Reaktion ausgeschlossen. Unsere verfassungsrechtliche Ordnung kennt den Zustand der hybriden Angriffe nicht. Sie unterscheidet nur zwischen Krieg und Frieden. Hybride Angriffe befinden sich oftmals unterhalb der Schwelle von kriegerischen Handlungen. Daher bedarf es einer **verfassungsrechtlichen Anerkennung des „hybriden Zustandes“** mit klaren und fähigkeitsspezifischen Zuständigkeiten.

Es braucht ein Abwehrzentrum gegen hybride Bedrohungen

In der breiten **Bevölkerung sind hybride Bedrohungen weitestgehend unbekannt**. Vorbereitungshandlungen auf Ausfälle von Infrastrukturen erfolgen so gut wie nicht. Die Bevölkerung muss mehr über hybride Bedrohungen, die Akteure, deren Ziele und unsere Verwundbarkeiten aufgeklärt werden und sich auf Ausfälle vorbereiten.

Auch gibt es **kein umfassendes bundesweites Lagebild** und Behörden verfügen teilweise

nicht über entsprechende Befugnisse und Ressourcen zur schnellen, flexiblen Reaktion. Es braucht ein Abwehrzentrum gegen hybride Bedrohungen, in dem ein Lage- und ein Analysezentrum zusammenlaufen. Alle relevanten Sicherheitsbehörden sind am Abwehrzentrum angedockt. Im Lagezentrum werden die erheblichen Vorfälle in einem **dynamischen Echtzeit-Lagebild-Dashboard** dargestellt. Angreifer werden künftig Cyberangriffe, Sabotage oder Spionage und Informationsoperationen noch gezielter und koordinierter ausführen.

Reaktionen müssen international koordiniert sein

Daher sollte das Dashboard Cyberangriffe, Desinformationskampagnen, Narrative sowie die wesentliche Grundversorgung in Deutschland (bspw. Energie-, Wasser-, Gesundheits-, Nahrungsmittelversorgung und Internet) erfassen. Die Vorfälle und Versorgungslage werden im Analysezentrum ausgewertet und die Intensität des Vorfalles wird bestimmt. Je nach Intensität des Vorfalls stehen unterschiedliche **Krisenreaktionsmechanismen** für die zuständigen Behörden zur Verfügung. Das Analysezentrum erstellt Profile der Angreifer. Außerdem werden fortlaufend die eigenen systemischen Schwachstellen analysiert.

Zudem bedarf es einer **international koordinierten Attribution und Reaktion** auf Angriffe, auch um die Hemmschwelle für künftige Angriffe zu erhöhen. Diese könnte im Rahmen der Nato oder innerhalb der EU erfolgen.

Die Zeit drängt. Derzeit ist **Deutschland nicht auf hybride Bedrohungen vorbereitet.** Die Zahl der Angriffe nimmt zu. Die Angreifer werden schneller und agieren kombiniert. Unsere Antwort sollte mindestens genauso sein und staatliche sowie gesellschaftliche Strukturen müssen angepasst werden.

Ferdinand Gehringer ist Referent für Innere und Cybersicherheit bei der Konrad-Adenauer-Stiftung in Berlin. Er beschäftigt sich unter anderem mit Cybersicherheit, dem Schutz kritischer Infrastruktur und hybriden Bedrohungen.