#BTW2025 | NR. 07 | JAN 2025

DGAP MEMO

Deutsche Gesellschaft für Auswärtige Politik e. V.

DEUTSCHLAND GLOBAL: DIE WAHL FÜR KLARE AUSSENPOLITISCHE ZIELE

Valentin Weber, Senior Research Fellow, Zentrum für Geopolitik, Geoökonomie und Technologie

Gegen Chinas und Russlands Cyberaggressionen ist Cyberabwehr nicht genug

Wie Deutschland mit geoökonomischen und diplomatischen Mitteln zukünftige Cyberangriffe abschrecken kann

Russische und chinesische Cyberoperationen gegen Deutschland haben in den letzten Jahren gefährlich zugenommen. Statt den Fokus auf Gegenmaßnahmen im Cyberraum zu setzen, die teils ineffektiv und kurzfristig in ihrer Wirkung sind, sollten die Regierenden in Berlin als Reaktion auf Cyberoperationen aus Russland und China ein Instrumentarium an geoökonomischen und diplomatischen Maßnahmen ausarbeiten. Solche sollten nach Angriffen, wie zum Beispiel Russlands Viasat-Angriff oder Chinas Hacks auf das Bundesamt für Kartographie, unmittelbar eingesetzt werden. Die Folge: Deutschland könnte zukünftig ein Dutzend russische Diplomaten ausweisen oder ausgewählten chinesischen Softwareanbietern den Zugang zum deutschen Markt verbieten.

ZIEL: DIE KOSTEN FÜR CHINA UND RUSSLAND SCHMERZHAFT ERHÖHEN

Als Reaktion auf Cyberaggressionen seitens feindlicher Akteure, allen voran aus China und Russland, hat die Bundesregierung bislang auf die Attribution (Zuweisung) von Angriffen und europäische Sanktionen im Rahmen der „Cyber Diplomacy Toolbox“ gesetzt. Obwohl beide Instrumente wichtig sind, haben sie bisher wenig Wirkung in Peking und Moskau gezeigt. Die kürzliche Einberufung des chinesischen Botschafters in Berlin nach einem Cyberangriff auf das Bundesamt für Kartographie und Geodäsie wurde mit einem Achselzucken abgetan, genauso wie die Sanktionierung von sechs Personen, die von russischen Geheimdiensten beschäftigt werden.

Fest steht daher: In Zukunft müssten substanziellere Kosten für Russland und China entstehen, sobald sie schwerwiegende Cyberoperationen gegen Deutschland unternehmen. Ein Beispiel für eine derartige chinesische Maßnahme war etwa der Angriff auf den Microsoft Exchange Server, welcher 2021 entdeckt wurde und fahrlässig tausende Systeme gefährdete. Zukünftig sollte Deutschland jedes Mal, wenn eine inakzeptable chinesische Cyberoperation öffentlich wird, mit Verweis auf die nationale Sicherheit einem hierzulande zugelassenen chinesischen Softwareprodukt den Markt verwehren. Denn mit jedem inakzeptablen Cyberangriff Chinas steigt das zukünftige Risiko für Deutschlands Sicherheit und die Ausnutzung von potenziellen Backdoors durch China in chinesischen Produkten.

Das Verursachen von Kosten für Russland ist hingegen schwieriger. Es ist eines der aktuell am stärksten sanktionierten Länder weltweit. Eine Möglichkeit im Falle russischer Cyberoperationen wäre die Ausweisung von Diplomatinnen und Diplomaten. So würden die Machthaber im Kreml dadurch in Bedrängnis geraten, dass sie kontinuierlich abwägen müssten, wie viel Personal sie noch in Deutschland halten können.

AUSGANGSLAGE: DIE EFFEKTIVITÄT VON CYBER-GEGENMASSNAHMEN IST EIN TRUGSCHLUSS

Im Wahlprogramm der CDU/CSU für die Bundestagswahl 2025 und im SPD-geführten Bundesministerium des Innern und für Heimat (BMI) herrscht die Überzeugung, dass aktive Cyberabwehr den Gegner abschrecken und Deutschland sicherer machen würde. Die AfD geht in ihrem Wahlprogramm einen Schritt weiter und fordert den „Aufbau von offensiven Cyberfähigkeiten, um potenzielle Gegner von Angriffen auf kritische Infrastruktur abzuschrecken". Dies ist ein nichtbelegter Irrglaube. Gerne wird auf die USA verwiesen, welche seit Jahren auf solche Maßnahme setzen, um chinesische und russische Angriffsinfrastrukturen zu unterwandern. Dennoch haben erfolgreiche Cyberoperationen wie etwa durch die chinesische Gruppierung „Volt Typhoon", die kritische Infrastruktur in den USA unterwandert hat, die chinesische Cyberoperation „Salt Typhoon" (eine Infiltration von US-Telekommunikationsunternehmen) sowie der Hack auf das US-Unternehmen SolarWinds gezeigt, dass die Angreifer nicht durch die USA abgeschreckt wurden, sondern im Gegenteil womöglich noch mehr bei ihren malignen Aktivitäten angespornt wurden.

Aktive Cyberabwehr oder gar offensive Cyberoperationen sind nicht zur Abschreckung geeignet, da der Cyberraum der wohl schlechteste Ort für zwischenstaatliche Kommunikation ist. Ein feindlicher Staat ist schwer einzuschüchtern, da aktive Gegenmaßnahmen nicht unter deutscher Fahne durchgeführt werden, sondern im Stillen und Verborgenen. Eine Botschaft Richtung China oder Russland wäre deshalb von beiden Staaten nicht unbedingt Deutschland zuzuordnen und hätte folglich kaum Auswirkung auf ihr Verhalten.

Problematisch ist, dass dieser Irrglaube und Fokus auf offensive Cybertätigkeiten als Allheilmittel zurzeit eine Diskussion über alternative Maßnahmen verhindert und somit auch Deutschlands Cybersicherheit gefährdet.

NÄCHSTE SCHRITTE FÜR DIE BUNDESREGIERUNG

1 Modernisierung
Die Cybersicherheits-Doktrin Deutschlands ist veraltet und benötigt eine Rundumerneuerung. Ideen wie die aktive Cyberabwehr werden ohne kritische Evaluierung von den USA übernommen, mit der Überzeugung, die großen Staaten wüssten, was zu tun ist. Eine moderne Doktrin muss auf Beweisen fußen und Folge eigener, unabhängiger Untersuchungen sein. Es braucht daher in Deutschland eine intensive Diskussion zwischen dem BMI, der Bundeswehr, dem Auswärtigen Amt, dem Kanzleramt und Bundestagsabgeordneten, um eine evidenzbasierte Cyber-Doktrin zu beschließen.

2 Souveränitätssicherung
Viel wichtiger als reaktive Maßnahmen ist die proaktive Rückerlangung der Souveränität über die kritische Infrastruktur in Deutschland. Derzeit sind bei Transport, in Häfen, der Telekommunikation und weiterer wichtiger Infrastruktur chinesische Software und Hardware verbaut. Dies sind Schwachstellen, die bei Bedarf von der Kommunistischen Partei Chinas genutzt werden könnten. Deutschland muss daher als nächsten Schritt eine systemische Analyse durchführen, um risikoreiche chinesische Technologien aus der kritischen Infrastruktur zu entfernen.

3 Internationale Partnerschaften
Um wirtschaftliche und diplomatische Gegenmaßnahmen zu verhängen, müssen die zukünftigen Zuordnungen von Cyberangriffen zu feindlich gesinnten Staaten weiterhin stets auf festem Fundament stehen. Zudem muss Deutschland, um Gefahrenakteure und deren Aktivitäten besser einordnen zu können, seinen „Threat Intelligence"-Austausch mit Partnern in Europa und Verbündeten in Asien vertiefen. Gleichzeitig können auch gemeinsame wirtschaftliche und diplomatische Gegenmaßnahmen verhängt werden, sollte beispielsweise ein feindlich gesinnter Akteur Cyberoperationen gegen mehrere Partnerstaaten gleichzeitig durchführen.

4 Reaktionsfähigkeit
In Zukunft muss Deutschland schneller reagieren. Deutschlands Schuldzuweisung an China für die Kompromittierung des Bundesamtes für Kartographie und Geodäsie dauerte beispielsweise Jahre und hatte keine größeren Konsequenzen. Für zukünftige Attributionen sollte die Bundesregierung eine Liste an chinesischen Dienstleistern und Produkten bereithalten, gegen die sie Maßnahmen verhängen könnte, sowie eine Liste von Diplomatinnen und Diplomaten, ob aus Russland oder China, die des Landes verwiesen würden. So kann Deutschland durch die unmittelbare Reaktion Stärke zeigen und mit den Jahren zunehmende Kosten für Peking und Moskau erzeugen.

Memo-Reihe zur Bundestagswahl

Die Memo-Reihe „Deutschland Global: Die Wahl für klare außenpolitische Ziele" (#btw2025) beleuchtet die zentralen außen- und sicherheitspolitischen Herausforderungen vor der Bundestagswahl 2025. Sie liefert fundierte Analysen und konkrete Empfehlungen, um politische Prioritäten zu setzen und Deutschlands Rolle in einer zunehmend fragmentierten Welt zu stärken. Ziel ist es, der nächsten Bundesregierung praxisnahe Impulse für eine strategische, souveräne und partnerschaftliche Außenpolitik zu geben, die Handlungsfähigkeit sichert, Verantwortung übernimmt und globale Kooperationen ausbaut.

www.dgap.org/dossier/btw2025

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.

Die DGAP ist gefördert vom Auswärtigen Amt aufgrund eines Beschlusses des Deutschen Bundestages.

Herausgeber
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2749-5542

Redaktion Jana Idris

Layout Daniel Faller