Pressemitteilung

Berlin, 5. April 2024

Sanktionierung des Einsatzes von Cyberwaffen, nicht der Waffen selbst

Eine aktuelle Analyse von Helene Pleil, wissenschaftliche Mitarbeiterin am Digital Society Institute (DSI) an der ESMT Berlin, die in Zusammenarbeit mit Kolleginnen und Kollegen der TU Darmstadt entstand, zeigt: die größten Herausforderungen für eine wirksame Cyber-Rüstungskontrolle, die für die Außen- und Sicherheitspolitik von entscheidender Bedeutung ist, sind der rasante technologische Fortschritt, der Mangel an politischem Willen und einheitlichen Definitionen sowie die doppelte Nutzung von Cyber-Werkzeugen. Da der Cyberspace zunehmend in Konflikten genutzt wird, muss auch die Cyber-Rüstungskontrolle in Angriff genommen werden.

Pleil und ihre Kolleginnen und Kollegen haben für ihre Analyse Literatur zu den Herausforderungen und Hindernissen bei der Entwicklung von Rüstungskontrollmaßnahmen im Cyberspace ausgewertet. Die Ergebnisse dieser Analyse, die durch Experteninterviews ergänzt wurde, zeigen die wichtigsten Hürden bei der Entwicklung robuster Cyber-Rüstungskontrollmaßnahmen auf.

Folgende Herausforderungen wurden identifiziert:

- **Fehlende Definitionen.** Eine grundlegende Herausforderung bei der Einführung von effektiver Rüstungskontrolle im Cyberspace ist das Fehlen klarer, einheitlicher Definitionen von Schlüsselbegriffen wie beispielsweise “Cyberwaffe”, zumal die herkömmliche Definition einer Waffe eine “Cyberwaffe” nicht wirklich erfasst. Es ist schwierig, sich darauf zu einigen, was in einem Rüstungskontrollvertrag kontrolliert werden soll, wenn das, was man kontrollieren will, nicht ausdrücklich definiert werden kann.
- **Dual-Use-Dilemma.** Ein Computer, ein USB-Stick oder eine Software können sowohl für zivile als auch für militärische Zwecke verwendet werden. Daher kann keine klare Grenze zwischen diesen verschiedenen Nutzungsszenarien gezogen werden, weshalb die Produkte nicht grundsätzlich im Sinne der Rüstungskontrolle verboten werden können. Man kann Atomwaffen verbieten, aber keine USB-Sticks oder Computer.
- **Verifikation.** Geeignete Verifikationsmechanismen für die Rüstungskontrolle im Cyberspace zu finden, ist äußerst schwierig. Beispielsweise ist es bei Cyberwaffen nicht möglich, Waffen zu zählen oder eine ganze Kategorie zu verbieten, wie es bei Rüstungskontrollabkommen für traditionelle Waffen gehandhabt wurde.
- **Technologischer Fortschritt.** Die Werkzeuge und Technologien für Cyberangriffe ändern sich fortlaufend. Das bedeutet, dass die Entwicklung neuer Waffen schneller voranschreitet als die Regulierungsbemühungen; bis eine Regulierung diskutiert wird, ist die verwendete Technologie bereits weiterentwickelt.
- **Rolle des Privatsektors.** Aufgrund des Dual-Use-Faktors haben die Staaten nicht die alleinige Kontrolle über die als Waffen verwendeten Mittel, sondern auch nichtstaatliche Akteure haben Eigentums- und Einsatzrechte in diesem Bereich. Der Privatsektor müsste also einbezogen werden und sich engagieren, damit Rüstungskontrollen wirksam werden.
- **Fehlender politischer Wille.** Der politische Wille ist für die Einführung von Rüstungskontrollmaßnahmen von entscheidender Bedeutung, die Staaten zögern jedoch, im Falle des Cyberspace zu handeln. Die Länder entdecken gerade erst den strategischen Wert von Cybertools und haben unterschiedliche Interessen. Die Einhaltung eines neuen Abkommens über die Nutzung von Cybertools birgt das Risiko, dass ihnen potenzielle

Vorteile entgehen. Darüber hinaus ist das aktuelle geopolitische Klima eine weitere große Herausforderung.

„Nach Auswertung der Literatur und der Befragungen der Experten wird weder die Kontrolle von Cyberwaffen noch eine andere technologische Regulierung des Cyberspace funktionieren", so Pleil. „Stattdessen muss der Fokus auf dem Verbot bestimmter Handlungen liegen, da Experten keine Chance für Verifikationsmechanismen sehen, insbesondere wegen des hohen Maßes an Eingriffen, die dafür erforderlich wären."

Traditionelle Maßnahmen der Rüstungs- und Waffenkontrolle können nicht einfach auf Cyberwaffen angewendet werden. Stattdessen müssen alternative und kreative Lösungen geschaffen werden. Durch das Definieren und Sanktionieren des Einsatzes dieser Waffen und nicht der Waffen selbst könnten Vereinbarungen getroffen und eingehalten werden, auch unabhängig von der Geschwindigkeit der technologischen Entwicklungen.

Die Analyse wurde in der *Zeitschrift für Außen- und Sicherheitspolitik* veröffentlicht und kann hier eingesehen werden.

Über das Digital Society Institute
Das Digital Society Institute (DSI) an der ESMT wurde 2016 mit dem Ziel gegründet, eine Brücke zwischen Technologie und Gesellschaft zu schlagen, und zwar durch Forschung, Bildung und Aktivitäten zum Kapazitätsaufbau, die digitales Vertrauen, Datenschutz sowie Menschenrechte in den Mittelpunkt der digitalen Entwicklung stellen. Das DSI genießt einen hervorragenden Ruf hinsichtlich der Durchführung von angewandter Forschung an der Schnittstelle von Technologie, Gesellschaft und Wirtschaft und ist eine gern akquirierte Beraterin zu verschiedenen Aspekten im Bereich Digitalisierung, z. B. zum Thema digitale Identitäten, digitale Diplomatie, Internet-Governance, EU-Digital- und Technologiepolitik und deutschem IT-Recht. Durch die Ausweitung ihrer Arbeit wurde die DSI zu einer führenden Wissensdrehscheibe für digitale Technologie, Regulierung und Cybersicherheitsfragen mit besonderem Schwerpunkt auf europäischer Technologiepolitik und Regulierung.

Über die ESMT Berlin
Die ESMT Berlin ist eine weltweit führende Wirtschaftsuniversität. Von 25 globalen Unternehmen gegründet, bietet die ESMT Master-, MBA- und PhD-Studiengänge sowie Managementweiterbildung an. Die Kurse werden auf dem Berliner Campus, an Standorten weltweit, online sowie als hybride Kurse mit Teilpräsenz angeboten. Mit einem Fokus auf Leadership, Innovation und Analytics veröffentlichen die Professorinnen und Professoren der ESMT regelmäßig ihre Forschungsergebnisse in führenden wissenschaftlichen Publikationen. Zusätzlich bietet die ESMT eine Plattform für den Diskurs zwischen Politik, Wirtschaft und Wissenschaft. Die ESMT ist eine staatlich anerkannte private wissenschaftliche Hochschule mit Promotionsrecht und ist von AACSB, AMBA, EQUIS und ZEvA akkreditiert. Die Business School engagiert sich für Vielfalt, Gleichstellung und Inklusion in all ihren Aktivitäten und Gemeinschaften. esmt.berlin

Pressekontakt
Kim Matthies
PR-Managerin
kim.matthies@esmt.org
+49 151 1457 1830