Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport – VBS
Frau Botschafterin Pälvi Pulli
Chefin Sicherheitspolitik
Bundeshaus Ost
3003 Bern

Genf, 30. Mai 2021

Die Sicherheitspolitik der Schweiz - Bericht des Bundesrates
Stellungnahme im Rahmen des Vernehmlassungsverfahrens 2021/36

Sehr geehrte Frau Botschafterin

Gerne nehmen wir im Rahmen des Vernehmlassungsverfahrens Stellung zum Bericht des Bundesrates «Die Sicherheitspolitik der Schweiz». Als in der Schweiz domizilierter international tätiger Think Tank beschränkt sich die Stiftung ICT4Peace in ihrer Stellungnahme auf Aspekte der Cyberrisiken und Cyberkriegsführung.

1. Grundsätzliches

Der neue sicherheitspolitische Bericht ist ein sehr gutes Strategiedokument. Es analysiert das Umfeld, die Risiken und Bedrohungen zutreffend. Die Prinzipien, Interessen und Ziele sind klar formuliert und werden verknüpft mit den wichtigen sicherheitsrelevanten Politikbereichen und Instrumenten. Der Bericht eignet sich deshalb als konzeptionelle Grundlage für die Weiterentwicklung der schweizerischen Sicherheitspolitik für die kommenden Jahre. Wir halten es auch für zweckmässig, einen sicherheitspolitischen Bericht einmal je Legislatur zu veröffentlichen.

2. Cyberraum und Cyberkriegsführung

Die rasant fortschreitende Digitalisierung sämtlicher Lebensbereiche und die absehbaren technologischen Innovationen in Bereichen wie Künstliche Intelligenz, Quantum-Computing

oder 5G-Technologie machen den Cyberraum zum Schlüsselbereich auch für die zukünftige Sicherheitspolitik.

Mit den laufenden und absehbaren technologischen Entwicklungen entstehen nicht nur eine zusätzliche Sphäre und zusätzliche Instrumente der Konfliktaustragung. Kontinuierlich und sehr fundamental findet ein umfassender Paradigmenwechsel statt. Einst für unumstösslich gehaltene Parameter wie Raum, Zeit oder Territorium lösen sich auf oder verändern ihre Bedeutung grundlegend. Die neuartigen Risiken erfordern militärische und technische Kapazitäten, was vom VBS bzw. der Armee an die Hand genommen und zurecht intensiviert wird.

Der Paradigmenwechsel bedarf aber auch neuer sicherheitspolitischer Konzepte und der Klärung wichtiger völkerrechtlicher und neutralitätspolitischer Fragestellungen. Ansonsten besteht ein erhebliches Risiko, ungewollt Völkerrecht zu brechen, neutralitätsrechtliche Vorgaben zu missachten oder die technischen Kapazitäten wenig wirkungsvoll einzusetzen.

International besteht ein Konsens, dass das Völkerrecht auch im Cyberspace anwendbar ist, das gilt auch für das Neutralitätsrecht. Sämtliche bisherigen multilateralen Beratungen und Bestrebungen haben aber gezeigt, dass die bestehenden Rechtsnormen nicht ohne Weiteres auf den Cyberraum und die Cyberkriegsführung angewendet werden können. Zentrale neutralitätsrechtliche und neutralitätspolitische Aspekte sind heute unbeantwortet.

Zurecht hebt der neue Sicherheitspolitische Bericht hervor, dass zukünftige Konflikte hybride Formen der Kriegsführung sein werden, also eine Kombination von herkömmlicher Kriegsführung, irregulären Kampfformen und Cyber-Kriegsführung unter Anwendung eines breiten Spektrums weiterer Mittel wie der politischen Beeinflussung, dem Verbreiten von Falschinformationen, politischem Druck usw. Das macht die völkerrechtliche Einordnung und das Entwickeln tragfähiger Konzepte besonders schwierig, aber auch besonders notwendig und dringlich. Diese Einschätzung ist der Ausgangspunkt für die folgenden Empfehlungen für die sicherheitspolitische Strategie der Schweiz.

3. Völkerrecht und Neutralitätspolitik

Das Neutralitätsrecht ist nicht nur für dauernd neutrale Staaten wie die Schweiz von Bedeutung. Sämtliche Staaten können in Konflikten, an denen sie nicht beteiligt sind, einen neutralen Status einnehmen, aus dem ganz bestimmte Rechte und Pflichten aus dem Völkerrecht hervorgehen. Deshalb besteht ein allgemeines Interesse der Staatengemeinschaft, eine rechtliche Klärung herbeizuführen. Diese ist allerdings bisher nur in Ansätzen gelungen. Ein Beispiel ist das Tallinn Manual, [1] das von Rechtsexperten auf Einladung des NATO Cooperative Cyber Defence Center of Excellence geschrieben wurde und auch ein Kapitel über das Neutralitätsrecht enthält. Es lässt allerdings viele Fragen offen.

Solche und ähnliche Diskussionen und Auffassungen sind zwar wichtig, um die Auslegung des

[1] Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare (2017). Cambridge University Press

Völkerrechts zu kennen. Sie haben aber für die schweizerische Neutralität nur eine beschränkte Bedeutung. Insbesondere machen keine Aussagen darüber, welche Verhaltensweisen und Politiken für einen dauernd neutralen Staat angebracht sind. Diese Analyse und die entsprechenden politischen Entscheide müssen von der Schweiz selbst vorgenommen werden. Wir empfehlen dringend davon abzusehen, eine Neutralitätspraxis

---

fallweise zu entwickeln (Kasuistik). Das würde nicht nur das Risiko beinhalten, im Voraus nicht zu wissen, in welche Richtung sich die Schweiz bewegt und möglicherweise längerfristig nicht tragbare Positionen zu entwickeln. Ein solches Vorgehen verunmöglicht auch, die eigene Politik und die eigenen Verhaltensweisen gegenüber anderen Staaten glaubwürdig darzustellen.

Weil der neue sicherheitspolitische Bericht der Digitalisierung und dem Cyberspace eine zentrale Bedeutung beimisst und darin eine grosse Veränderung verglichen mit der Vergangenheit sieht, wäre unseres Erachtens sogar zu überlegen, ob der sicherheitspolitische Bericht mit einem Neutralitätsbericht ergänzt werden soll, ähnlich wie das beim Bericht 90 am Ende des Kalten Krieges der Fall war.

Für die Entwicklung einer Neutralitätspolitik für das Zeitalter der Cyberkriegsführung sind wissenschaftliche Studien und juristische Abklärungen eine wichtige Grundlage. Sie erfordert aber unseres Erachtens auch eine breitere politische Diskussion und politische Entscheide, die auch Parlament einbeziehen müssen.

Empfehlung 1: Eine vertiefte Analyse der völkerrechtlichen, neutralitätsrechtlichen und neutralitätspolitischen Auswirkungen der Cyberkriegsführung vornehmen.

Empfehlung 2: Eine Neutralitätspolitik für das Zeitalter der Cyberkriegsführung erarbeiten.

4. Einwirkung auf das sicherheitspolitisch relevante Umfeld im Cyberspace

Das umfassende Ziel der Schweizer Sicherheitspolitik besteht darin, die Handlungsfähigkeit, Selbstbestimmung und Integrität der Schweiz und ihrer Bevölkerung sowie ihre Lebensgrundlagen gegen Bedrohungen und Gefahren zu schützen, aber auch einen Beitrag zu Stabilität und Frieden jenseits der Grenzen zu leisten, d.h. auf das sicherheitspolitisch relevante Umfeld einzuwirken. Zu diesem Zweck hat die Schweiz in vielen Bereichen ein international anerkanntes Instrumentarium entwickelt: sie leistet Gute Dienste, setzt sich für die Stärkung des Völkerrechts ein, fördert Transparenz und vertrauensbildende Massnahmen oder leistet in verschiedener Form Unterstützung, um Konfliktursachen zu entschärfen oder deren Folgen zu bewältigen helfen. Wie kann aber dieses Anliegen unter den neuen Rahmenbedingungen der Digitalisierung und Cyberkriegsführung verwirklicht werden?

Manche Beiträge zu Stabilität und Frieden, welche die Schweiz heute in anderen Bereichen leistet, können relativ problemlos auch auf den Cyberspace und die Cyberkriegsführung

ausgeweitet werden, beispielsweise das Engagement für eine regelbasierte Ordnung, die Stärkung des Völkerrechts oder Initiativen zur friedlichen Streitbeilegung.

Zudem gibt es naheliegende Tätigkeitsfelder wie Factfinding-Aktivitäten (von der Zuordnung von Cyber-Zwischenfällen bis zur Fakten-Überprüfung im Zusammenhang mit Informationsoperationen), die Unterstützung von Initiativen wie FIRST (Forum for Incident Response and Security Teams), oder auch die Unterstützung von Staaten, die Opfer von Cyberangriffen geworden sind.
Wir halten es aber für besonders wichtig, in diesem Bereich eine gründliche Auslegeordnung vorzunehmen, erfolgversprechende neue Ansätze zu identifizieren und als Elemente einer zukünftigen Sicherheits- und Aussenpolitik zu beurteilen. Dazu ist eine breite und offene Diskussion unter Einbezug von Wissenschaft und Privatsektor, aber auch von internationaler Expertise erforderlich. Falls daran ein Interesse besteht, ist ICT4Peace gerne bereit, in diesem Rahmen eine Studie zu erstellen und dabei das bestehende Netzwerk zu nutzen.

Die Schweiz als neutraler Kleinstaat mit grossen technischen Kenntnissen und Fähigkeiten ist besonders geeignet, in diesem Rahmen auch internationale eine profilierte Rolle zu spielen.

Empfehlung 3: Innovative Ansätze entwickeln, mit denen die Schweiz Beiträge zur Sicherheit im Cyberspace leisten kann als Teil einer zukünftigen Sicherheits- und Aussenpolitik.

5. Cyberrisiken in der öffentlichen Debatte über die schweizerische Sicherheitspolitik

Aus dem beruflichen und privaten Umfeld ist die schweizerische Bevölkerung zunehmend vertraut mit den Folgen der Digitalisierung und mit Cyberrisiken. Die sicherheitspolitische Dimension des Cyberbereichs ist aber bisher eher eine Angelegenheit von Insidern und Experten geblieben. Das ist der Weiterentwicklung und breiten Verankerung einer zukünftigen Sicherheitspolitik nicht förderlich.

Wir halten es deshalb für sehr wichtig, Cyberrisiken und der Cyberkriegsführung in der öffentlichen Diskussion über die zukünftige Sicherheitspolitik der Schweiz viel Raum zu geben. Der neue Sicherheitspolitische Bericht eignet sich dazu ausgezeichnet. Nicht nur, weil er dem Cyberbereich selbst ein grosses Gewicht beimisst, sondern auch weil er den umfassenden sicherheitspolitischen Kontext und den Bezug zu anderen Bedrohungsformen herstellt.

Empfehlung 4: In der öffentlichen Debatte über die zukünftige Sicherheitspolitik der Schweiz dem Cyberraum und der Cyberkriegsführung grosses Gewicht geben.

Wir hoffen, dass unsere Stellungnahme auf Ihr Interesse stösst.

Mit freundlichen Grüssen

Daniel Stauffacher
President
ICT4Peace Foundation

Beilage
One Pager ICT4Peace
Policy Brief «Schweizer Neutralität im Zeitalter der Cyberkreigsführung»