Gegensatz zur Vorgehensweise von autoritären Staaten können Demokratien nicht einfach Grundrechte wie die Presse- und Informationsfreiheit aushöhlen und sich von ihren eigenen Werten entfernen, um mit diesen Narrativen umzugehen. Freie Gesellschaften müssen akzeptieren, dass sie diesen Darstellungen – mögen sie auch verzerrt sein – nicht mit Verboten zuvorkommen können.

Vielmehr muss sich der Westen folgender Aspekte bewusst werden, um im Rahmen der eigenen Public Diplomacy effektiv zu agieren: Zunächst muss er sich fairerweise die Frage stellen, ob nicht etwas Wahres an den Darstellungen ist. Dann darf es ihm nicht um Gegenpropaganda gehen, sondern lediglich um die Richtigstellung verzerrter Darstellungen. Auf der Basis einer solchen Selbsteinschätzung kann dann Aufklärung unternommen werden. So sollten westliche Regierungen stets darauf hinweisen, dass Maßnahmen wie Demokratieförderung durch NGOs sich nicht gegen eine bestimmte Regierung richten, sondern schlicht der Verbreitung von Werten dienen. Hier sollte auch stärker darauf hingewiesen werden, dass in Russland solche Aktivitäten entweder verboten oder stark eingeschränkt werden, wohingegen in den allermeisten westlichen Staaten kremlnahe Gruppierungen frei operieren dürfen.

Denkbar wäre, dass EU und NATO aktiv Gegen-Narrative schaffen und verbreiten

Auch sollte ganz klar darauf hingewiesen werden, wenn Aktion und Reaktion verwechselt werden: Ohne die vorangegangene Krim-Annexion hätte es keine EU-Sanktionen gegeben. Erstere soll zudem durch falsche Analogien wie dem Eingreifen in Libyen oder im Kosovo legitimiert werden: Hier wurde im Kontext einer internationalen Schutzverantwortung gehandelt, was sich über die russische Vorgehensweise bei der Krim-Annexion nicht sagen lässt.

Die Herausforderung für westliche Regierungen und Zivilgesellschaften besteht darin, Aufklärung zu betreiben, ohne propagandistische Züge anzunehmen. Es wäre denkbar, dass Organisationen wie EU und NATO ihre strategische Kommunikation insoweit ausbauen, dass sie aktiv eine Art Gegennarrativ schaffen. Hierfür müssten jedoch die Ressourcen in diesem Bereich stark ausgebaut werden. Die „EU East StratCom Task Force“ etwa ist eine wichtige Einrichtung, die aber immer noch unterbesetzt ist. • •

Kaan Sahin arbeitete beim IISS, bei der OSZE, Carnegie Europe und der NATO.

„Rotes Telefon“ fürs Internetzeitalter

Die OSZE bietet sich als Plattform zur Prävention von Cyber-Konflikten an

Nikolas Ott | Spionage, Manipulation oder Sabotage – das Internet etabliert sich als neuer Austragungsort für zwischenstaatliche Konflikte. Internationale Organisationen wie die Vereinten Nationen oder die Organisation für

Sicherheit und Zusammenarbeit in Europa (OSZE) bemühen sich, als Plattform des zwischenstaatlichen Austauschs zu dienen, vor allem um unbeabsichtigte militärische Eskalation zu verhindern.

Ein Beispiel: Ende Juni 2017 legte die Schadsoftware „Petya/NotPetya" in der Ukraine Tausende Rechner lahm. Die Malware aktivierte sich auf Geräten, die eine Software installiert hatten, die für Steuererklärungen in der Ukraine benötig wird, und löschte Daten auf den befallenen Geräten unwiderruflich. Der ukrainische Geheimdienst SBU beschuldigte Russland, in die Attacke verwickelt zu sein – was russische Stellen zurückwiesen. Unabhängig vom Ursprung des Vorfalls verdeutlicht er die globale Reichweite von moderner Malware. Denn betroffen waren längst nicht nur Computer in der Ukraine: Die dänische Reederei Maersk erlitt Schäden in Höhe von bis zu 300 Millionen Dollar. Beim Milka-Schokoladen-Hersteller Mondelez stand die Produktion still, auch Unternehmen wie Beiersdorf und der US-Pharmakonzern Merck waren betroffen.

Von der Destabilisierung des Internets als globaler Plattform würde niemand profitieren

Die Schadsoftware „NotPetya" verdeutlicht, dass das Austragen zwischenstaatlicher Spannungen im Cyber-Raum die Gefahr birgt, das Internet als Plattform globaler Kommunikation und Interaktion zu destabilisieren. Davon würde niemand profitieren. Cyber-Attacken verunsichern nicht nur Internetnutzer, sie richten auch immense betriebswirtschaftliche Schäden an – wichtige Gründe, um die Grundursache auf politischer Ebene anzupacken.

Welches Recht gilt im Cyber-Raum?

Eines der wichtigsten internationalen Gremien für zwischenstaatlichen Austausch war dabei bis zuletzt eine Arbeitsgruppe der Vereinten Nationen, die „UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (UN GGE). Der Schwerpunkt dieser Arbeitsgruppe lag auf der Entwicklung freiwilliger Verhaltensregeln – „Normen für verantwortungsbewusstes Staatenverhalten" – sowie bis 2013 auf der Klärung der grundsätzlichen Anwendbarkeit und ab 2015 die praktische Anwendung des Völkerrechts im Cyber-Raum.

Lange war strittig, ob – und wenn ja, wie – existierendes Völkerrecht im Cyber-Raum angewendet werden kann. Im Konsensbericht der UN GGE von 2013 hieß es dazu am Ende aber klar, dass „bestehendes Völkerrecht, allen voran die Charta der Vereinten Nationen, auch im Cyber-Raum anwendbar" ist. Eine genaue Ausarbeitung dieser Aussage ließ man offen in der Erwartung, die Praxis würde klare Regeln schaffen. Im Konsensbericht von 2015 wurden dann sechs Ausführungen zur Anwendbarkeit des Völkerrechts definiert sowie elf Normen für verantwortungsbewusstes Staatenverhalten verabschiedet.

Dieser Prozess sollte unter deutschem Vorsitz in den Jahren 2016/17 weitergeführt werden. Westliche Staaten hofften, die Errungenschaften der vergangenen Jahre weiter auszubauen, um Spannungen zu reduzieren und klare

Regeln zu definieren. Doch die Verhandlungen scheiterten: Die Vertreter der BRICS- und der G77-Staaten waren nicht länger bereit, auf der Basis vorheriger Konsensberichte zu verhandeln.

Man müsse auch über neue Regeln und Verfahren sprechen, lautete die Begründung. Hierzu hatten China, Russland, Tadschikistan und Usbekistan 2011 einen „Code of Conduct for Information Security" der UN-Generalversammlung vorgestellt. Dieser wurde 2015 aktualisiert und erneut zur Debatte gestellt. Während der abschließenden Verhandlungen der UN GGE im Sommer 2017 wurde klar, dass Vertreter der BRICS- und G77-Staaten nun diesen Verhaltenskodex als Verhandlungsgrundlage nutzen möchten – eine Zäsur in den multilateralen Bemühungen. Westliche Staaten waren mit diesem Vorstoß nicht einverstanden. Letztendlich konnte man sich auf keinen Konsenstext einigen.

Die Reduzierung von Konfliktpotenzial im Cyber-Raum wird eine Priorität bleiben

Eine neue Aufgabe für die OSZE

Derzeit ist schwer abzusehen, ob und mit welchem Auftrag die UN-Generalversammlung 2018 eine neue Gruppe mandatiert. Parallel könnten aber regionale Organisationen, allen voran die OSZE, bei der Entwicklung vertrauensbildender Maßnahmen im Cyber-Raum eine größere Rolle übernehmen. Abseits der Öffentlichkeit treffen sich Vertreter aller 57 OSZE-Staaten sowie der EU in der Regel viermal im Jahr als informelle Arbeitsgruppe, um die Schaffung neuer und die Umsetzung bereits beschlossener Maßnahmen zu diskutieren. Dass dieser Prozess auch vor dem Hintergrund der Ukraine-Krise und anderer politischer Spannungen zu konstruktiven Ergebnissen führen kann, zeigt die Verabschiedung fünf weiterer vertrauensbildender Maßnahmen im März 2016 sowie die einstimmige Erklärung auf Außenminister-Ebene, die unter deutschem OSZE-Vorsitz im Dezember 2016 abgegeben wurde. Darin kündigten die teilnehmenden Staaten an, bereits bestehende vertrauensbildende Maßnahmen auszubauen und weitere zu entwickeln. Auch wurde die informelle Arbeitsgruppe beauftragt, die Einrichtung von Kommunikationskanälen im Cyber-Krisenfall – eine Art „rotes Telefon" bei Cyber-Angriffen – weiter voranzubringen. Dadurch könnten Staaten schneller Informationen austauschen, wenn verdächtige Aktivitäten im Netz beobachtet werden. Es sind kleine Schritte, die man aber nicht unterschätzen sollte.

Darüber hinaus ist die OSZE die einzige multilaterale Organisation, die eine etablierte Plattform für einen konstruktiven Austausch zu Cyber-Sicherheitsthemen zwischen den USA, Russland und der EU anbietet. Keiner der involvierten Staaten sollte daran interessiert sein, auch diesen Prozess zu blockieren oder gar aufzulösen. Im Gegenteil: Unter dem Vorsitz Italiens wird das Thema Reduzierung von Eskalationspotenzial im Cyber-Raum zwischen Staaten 2018 ganz oben auf der Agenda stehen. • •

Nikolas Ott arbeitete während seines Kolleg-Jahres in Wien, Tallinn und Brüssel.