GENEVA DIALOGUE: MITGESTALTUNG GLOBALER SICHERHEITSNORMEN FÜR DEN CYBERRAUM

Von Jacqueline Eggenschwiler

Am 18. April 2018 hat der Bundesrat die überarbeitete Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) für die Periode 2018–2022 verabschiedet. Die Neuauflage der erstmals im Jahr 2012 erlassenen NCS reagiert in zentraler Weise auf eine sich im stetigen Wandel befindende Cyber-Bedrohungslage. Im Zentrum des Dokumentes stehen sieben strategische Ziele, welche kumulativ dazu beitragen sollen, die Cyberresilienz der Schweiz zu stärken. Die Ziele reichen vom Aufbau von Kompetenzen und Wissen und der Förderung der internationalen Kooperation über die Stärkung des Vorfall- und Krisenmanagements sowie der Zusammenarbeit bei der Cyber-Strafverfolgung bis hin zu Massnahmen der Cyberabwehr durch die Armee und den Nachrichtendienst des Bundes (NDB).

Der NCS 2018–2022 liegt ein umfassender, risikobasierter Ansatz zugrunde, der sich auf eine enge Zusammenarbeit zwischen Gesellschaft, Wirtschaft und Politik abstützt. Die Cybersicherheit tangiert nahezu alle Lebens-, Wirtschafts- und Verwaltungsbereiche, weshalb sämtliche gesellschaftlichen Organe zum Handeln aufgerufen sind und gemeinsam in der Schutzverantwortung stehen. Diese auf Kooperation ausgelegte Haltung trägt die Schweiz auch nach aussen und engagiert sich bewusst für die Zusammenarbeit mit internationalen Partnern. «Sie fördert den Dialog in der Cyber-Aussen- und Sicherheitspolitik, beteiligt sich aktiv in den internationalen Fachgremien und pflegt den Austausch mit anderen Staaten und internationalen Organisationen».[1]

Ein aktuelles und einschlägiges Beispiel für das internationale Engagement der Schweiz im Bereich Cybersicherheit ist der im Juni 2018 durch das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) lancierte Dialog zu verantwortungsbewusstem Verhalten im

1 Bundesrat, *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–22* (Bern: ISB, 2018).

Cyber-Raum, auch bekannt unter dem Namen *Geneva Dialogue on Responsible Behaviour in* Cyberspace (kurz: *Geneva Dialogue*). Das Center for Security Studies (CSS) beteiligt sich aktiv an diesem Dialog.

Seit nunmehr zwei Dekaden setzt sich das CSS aktiv mit Fragen der Cybersicherheit auseinander und hat sich als Kompetenzzentrum in diesem Fachgebiet etabliert und eine Vielzahl wissenschaftlicher Studien veröffentlicht. Seine Expertise in diesem Bereich bringt das CSS auch in der Zusammenarbeit mit dem EDA ein. Konkret unterstützt das CSS das EDA bei der Erstellung eines sogenannten Framework Dokuments sowie der Durchführung von Expertenworkshops.

Vor dem Hintergrund zunehmender Cyberkriminalität, der Häufung weitgreifender Fälle von Cybersabotage auf kritische Infrastrukturen sowie der Mehrung digitaler Spionageangriffe auf private und öffentliche Institutionen beabsichtigt der Geneva Dialogue eine Grundlage für massvolle Handlungsweisen im Cyberraum zu schaffen.[2] Im Gegensatz zu vorhergehenden Initiativen, wie etwa dem von der UNO-Generalversammlung ins Leben gerufene *Groups of Governmental Experts* (UNGGE) Prozess, konzentriert sich der Geneva Dialogue nicht nur auf die Ausarbeitung verhaltensleitender Prinzipien für staatliche Akteure, sondern auch auf die Identifizierung von Normen für nichtstaatliche Akteure. Mit dem Ziel der Durchbrechung bestehender, siloartiger Strukturen und Diskussionen sowie der Zuschreibung akteursspezifischer Verantwortlichkeiten leistet der Geneva Dialogue einen wichtigen Beitrag zu mehr Stabilität im Cyberraum.

Neben dem CSS wird das EDA bei der Formulierung der globalen Verhaltensgrundsätze von drei weiteren Projektpartnern unterstützt: der *Geneva Internet Platform* (GIP), dem *United Nations Institute for Disarmament Research* (UNIDIR), sowie der Universität Lausanne. Gesamthaft besteht der Geneva Dialogue aus drei Arbeitsgruppen. Während sich UNIDIR und die Universität Lausanne auf die Konzeptionierung und Analyse von Verhaltensregeln für staatliche (Arbeitsgruppe 1) beziehungsweise zivilgesellschaftliche Protagonisten (Arbeitsgruppe 2) fokussieren, widmet sich das CSS der Erarbeitung von Verhaltensmassstäben für private Akteure (Arbeitsgruppe 3).

2 EDA, *Fact Sheet: Geneva Dialogue on Responsible Behaviour in Cyberspace,* Juni 2018.

Private Akteure waren und sind von zentraler Bedeutung für das Wachstum und die Verbreitung von Informations- und Kommunikationstechnologien (IKT). Als Entwickler von Produkten und Dienstleistungen sowie Betreiber kritischer Netzwerkinfrastrukturen sind sie Teil internationaler Cyber-Steuerungssysteme und einschlägiger Governanzmechanismen. Technologieunternehmen sind zu wichtigen Plattformen für Austausch und Diskussion, Informationszugang, Handel und menschliche Entwicklung geworden. Sie sammeln und speichern die persönlichen Daten von Milliarden von Benutzern weltweit, kennen deren Gewohnheiten, Aufenthaltsorte und Aktivitäten, und dringen in die intimsten Bereiche ihres Lebens vor. Aus wirtschaftlichen und gesellschaftlichen Blickpunkten haben private Akteure ein Interesse an der friedlichen Nutzung ihrer Technologien und dem Vorhandensein resilienter Infrastrukturen. Angesichts zunehmender Bedrohungen aus dem Cyberraum haben sich internationale Unternehmen daher vermehrt auch an politischen Debatten zur Einschränkung schädlicher Verhaltensweisen beteiligt. Grosse internationale Technologiekonzerne wie Microsoft, Siemens, Telefónica oder Google beispielsweise haben konkrete normative Vorschläge zum Schutz digitaler Infrastrukturen erarbeitet und sich als sogenannte Norm-Entrepreneure etabliert.[3]

Die akteursbezogenen Erörterungen der einzelnen Arbeitsgruppen bilden die Grundlage für einen zweitägigen Workshop im November 2018. Ziel des Workshops ist es, kritische Stakeholder zusammenzuführen und in substanzielle Diskussionen zu verantwortungsbewusstem Verhalten im Cyberraum einzubinden. Mit seiner Multistakeholder-basierten Ausrichtung greift der Geneva Dialogue die Tatsache auf, dass die erfolgreiche Eindämmung sicherheitspolitischer Risiken der nachhaltigen Kooperation unterschiedlicher Akteure bedarf. Internationale Normsetzungsprozesse, besonders im Bereich Cybersicherheit, sind heute nicht mehr nur Sache staatlicher Entitäten. Private und zivilgesellschaftliche Akteure nehmen eine zunehmend aktive und wichtige Rolle ein, wenn es um die Verabschiedung globaler Cyber-Sicherheitsnormen geht.

3 Martha Finnemore / Kathryn Sikkink, «International Norm Dynamics and Political Change», *International Organization* 52, Nr. 4 (1998), S. 887–917.

Die NCS 2018–2022 merkt dazu in treffender Weise an: «Die Herausforderungen im Umgang mit Cyberrisiken sind gross, und sie werden weiter virulent bleiben. Umso wichtiger ist es, dass alle Akteure gemeinsam und koordiniert diese Herausforderungen angehen. Eine möglichst effektive Zusammenarbeit aller kompetenten Stellen und eine systematische internationale Vernetzung sind entscheidend für die Schaffung eines sicheren Umfeldes für die [fortlaufende] Digitalisierung der Gesellschaft und Wirtschaft».[4]

4 Bundesrat, *Nationale Strategie,* S. 2.