In: IFSH (Hrsg.), OSZE-Jahrbuch 2017, Baden-Baden 2019, S. 227-240.

*Velimir Radicevic**

Die Förderung von Cyberstabilität zwischen Staaten: die Bemühungen der OSZE zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien (IKT) im Kontext globaler und regionaler Sicherheit ergeben

Einführung – der globale Status quo im Cyberspace

Als grenzenlose Ressource, die in fast allen Bereichen und Staaten eingesetzt wird, hat das Internet die Möglichkeiten für Wirtschaftswachstum, den politischen Diskurs, die Verbreitung von Informationen und für soziale Mobilität weltweit verbessert und damit die – wie sie von einigen genannt wird – dritte industrielle Revolution eingeleitet. Die rasante Verbreitung dieser Ressource ging jedoch mit neuen Herausforderungen, wie z.B. Schadsoftware, Hackerangriffen, Datenschutzverletzungen und Internetspionage, einher, was sich bereits 1988 mit dem ersten, vom „Morris-Wurm" ausgelösten dokumentierten Überlastungsangriff (*distributed denial-of-service attack*, DDoS) abzuzeichnen begann.[1] Zahl und Umfang von Cyberangriffen haben infolge der einzigartigen Kombination von hoher Rentabilität und großer Reichweite, niedrigen technischen Einstiegshürden und asymmetrischen Risiken für die Täter seitdem weiter zugenommen. Dies zeigte sich auch bei den jüngsten Cybervorfällen, z.B. der WannaCry-*Ransomware*-Attacke, den Versuchen, die Wahlen in den USA und in Frankreich zu hacken, und den Angriffen auf kritische Infrastrukturen in der Ukraine und Georgien, die allesamt große Beachtung in den Medien fanden. Der Unterschied zwischen solch weitreichenden Angriffen, alltäglicher Cyberkriminalität und der Nutzung des Internets durch Terroristen mag akademisch escheinen. Der Umfang und das hohe technische Niveau dieser Angriffe haben jedoch viele Experten davon überzeugt, dass sie nur mithilfe irgendeiner Form von staatlicher Beteiligung haben stattfinden können.
Darüber hinaus haben Staaten die Vorteile von Cyberangriffen erkannt und entsprechend damit begonnen, nicht nur ihre defensiven, sondern auch ihre offensiven Cyberfähigkeiten zu verbessern. Nach Angaben des Instituts der Ver-

---

* Die in diesem Beitrag geäußerten Ansichten sind diejenigen des Autors und geben nicht unbedingt die offizielle Position der OSZE wieder. Der Autor dankt Veronika Černá, Projektassistentin für Cybersicherheit/IKT-Sicherheit im Koordinierungsstab der Abteilung Grenzüberschreitende Bedrohungen des OSZE-Sekretariats, für ihre wertvolle Hilfe.

1 Ein DDoS-Angriff ist ein Cyberangriff, bei dem eine Person oder Gruppe versucht, einen einzelnen Computer oder ein Computernetzwerk für seine vorgesehenen Nutzer unerreichbar zu machen. Dies geschieht in der Regel durch die Überschwemmung der/des betroffenen Rechner(s) mit überflüssigen Anfragen, um so die Systeme zu überlasten und die Bearbeitung legitimer Anfragen zu verhindern.

einten Nationen für Abrüstungsforschung (*United Nations Institute for Disarmament Research*, UNIDIR) verfügen mindestens 47 Staaten über Programme zur Cybersicherheit/IKT-Sicherheit, in denen den Streitkräften eine gewisse Rolle zugeschrieben wird,[2] und einige haben den Cyberspace selbst als Sphäre möglicher militärischer Operationen definiert.[3] Das digitale Wettrüsten hat – gepaart mit der Grenzenlosigkeit des Cyberspace, den Schwierigkeiten, die Verantwortlichen hinter Cyberangriffen zu identifizieren (*attack attribution*), und den unterschiedlichen Cyberfähigkeiten der Staaten – zu Verwirrung, Ungewissheit und Fehlwahrnehmungen in den zwischenstaatlichen Beziehungen geführt. Dies wiederum kann zu eskalierenden Spannungen zwischen Staaten führen und sich potenziell in einen kinetischen, also mittels physischer Einwirkung ausgetragenen Konflikt verwandeln.

Leider gibt es nur wenige etablierte Verfahren zur Verminderung der Irritationen und zum Abbau möglicher Spannungen, die sich aus dem Einsatz von IKT ergeben. Es ist unwahrscheinlich, dass es in naher Zukunft – oder überhaupt jemals – ein Cyberäquivalent zum Vertrag über den Offenen Himmel[4] geben wird, das mittels eines multilateralen Rüstungskontrollregimes im Cyberspace Vertrauen bilden könnte. Cyber Tools sind weder sichtbar noch leicht zu lokalisieren und Server können von kriminellen Gruppen gemietet oder genutzt werden, um Angriffe von überall auf der Welt zu starten und so die Erkennung zu umgehen. Und wenn ein Angriff stattfindet, kann seine Zuordnung, selbst wenn sie schnell und zeitnah erfolgt, unter Umständen keine eindeutige Verbindung zwischen dem Täter und einem potenziellen staatlichen Akteur nachweisen, der im Verdacht steht, hinter dem Angriff zu stecken.[5]

All dies bedeutet, dass die Cybersicherheit/IKT-Sicherheit auf der Agenda der Staaten und in der Folge auch auf derjenigen internationaler, regionaler und subregionaler Organisationen innerhalb kürzester Zeit an Bedeutung gewonnen hat. Sie alle stehen vor derselben Frage: Was muss getan werden, um die globale Cyberstabilität zwischen den Staaten zu verbessern und die Spannungen zu verringern, die aus einem Vorfall im Zusammenhang mit IKT entstehen können?

2 Vgl. United Nations Institute for Disarmament Research (UNIDIR), The Cyber Index. International Security Trends and Realities, New York/Genf 2013, S. 1.

3 Vgl. Tomáš Minárik, NATO Recognises Cyberspace as a „Domain of Operations" at Warsaw Summit, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 26. Juli 2016.

4 Vgl. Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), Vertrag über den Offenen Himmel, 24. März 1992, unter: http://www.osce.org/library/14127.

5 Vgl. Michael N. Schmitt/Liis Vihul, The Nature of International Law Cyber Norms, in: Anna-Maria Osula/Henry Rõigas (Hrsg.), International Cyber Norms: Legal, Policy & Industry Perspectives, Tallinn 2016, S. 23-47, hier: S. 38.

Völkerrecht und seine mögliche Anwendung im Cyberspace, Normen für das Verhalten von Staaten und vertrauensbildende Maßnahmen

Die einzelnen Staaten haben die Möglichkeit, den Zugang zum Internet und dessen Nutzung durch nationale Rechtsvorschriften zu regulieren. Der Cyberspace ist jedoch immer noch wesentlich jünger als die Dokumente, die den Kern des Völkerrechts bilden, wie z.B. die Charta der Vereinten Nationen, die Genfer Konvention, die Schlussakte von Helsinki und der Internationale Pakt über bürgerliche und politische Rechte (IPbpR). Ohne einen Vertrag oder ein Gewohnheitsrecht zur Vermittlung der Regeln und Normen für verantwortungsbewusstes Verhalten von Staaten im Cyberspace und ohne Gerichte, die auf dieser Grundlage Urteile fällen, wird die Frage nach der Anwendbarkeit der bestehenden internationalen Normen im Cyberspace zum zentralen Thema – insbesondere hinsichtlich des *ius ad bellum* und des *ius in bello*. Können sie angewendet werden oder nicht? Wenn ja: wie und unter welchen Umständen? Ab wann gilt ein Cybervorfall als Angriff, auf den Artikel 51 der Charta der Vereinten Nationen anwendbar ist? Auf der Ebene der Vereinten Nationen wurde die Frage der Anwendbarkeit 2013 durch einen Konsensbericht beantwortet, der die Anwendung des bestehenden Völkerrechts im Cyberspace empfiehlt und damit die Debatte darüber eröffnete, wie genau die Rechtsnormen des 20. Jahrhunderts auf die rechtlichen Herausforderungen des 21. Jahrhunderts übertragen werden können. Zentren wie das *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) der NATO haben sich zu diesem Thema geäußert und Stellungnahmen von Rechtspraktikern und Rechtswissenschaftlern zur Anwendung verschiedener Bestimmungen des Völkerrechts im *Tallinn Manual on the International Law Applicable to Cyber Warfare*[6] und dem *Tallinn Manual 2.0*[7] veröffentlicht.

Parallel zu den Diskussionen über rechtliche Aspekte des Cyberspace war ein weiterer Schwerpunkt die Entwicklung nicht bindender Mechanismen, die die Erwartungen der Staaten hinsichtlich eines akzeptablen Verhaltens im Cyberspace beeinflussen können. Dabei handelt es sich um Normen für verantwortungsbewusstes Verhalten von Staaten und Verfahren, die gewährleisten, dass ein solches Verhalten durch vertrauensbildende Maßnahmen (VBM) aktiv umgesetzt wird. Normen für verantwortungsbewusstes Verhalten von Staaten sollen Schlüsselbegriffe, wie z.B. „rote Linien" für die Verwendung von IKT durch Staaten, definieren. Beispielsweise sollte ein Staat nicht wissentlich zulassen, dass sein Territorium für Cyberangriffe auf ein anderes Land oder für Angriffe auf die kritische Infrastruktur eines anderen Staates oder deren IKT-gestützte Steuerungssystemen genutzt wird. Dabei geht man davon aus, dass ein solches *„Soft Law"* eine gewisse Rechtswirkung entfalten kann, indem es

6 Vgl. Tallinn Manual on the International Law Applicable to Cyber Warfare, New York 2013.

7 Vgl. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Factsheet, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2. Februar 2017.

gemeinsame Erwartungen hinsichtlich des Verhaltens eines Staates auf internationaler Ebene[8] formuliert und somit die Grundlage für ein Gewohnheitsrecht für den Cyberspace bildet. Ein Beispiel für die Festlegung solcher Normen für das Verhalten von Staaten im Cyberspace ist der 2011 von der Shanghaier Organisation für Zusammenarbeit (SOZ) vorgeschlagene internationale Verhaltenskodex für Sicherheit in der Informationstechnik (*International Code of Conduct for Information Security*), der 2015 in einer aktualisierten Fassung veröffentlicht wurde.[9]

Die Vereinbarung von Normen für verantwortungsbewusstes Verhalten von Staaten im Cyberspace ist jedoch keine Garantie für ihre Anwendung, vor allem angesichts der vorhandenen Gefahr von Missverständnissen und Irritationen in den zwischenstaatlichen Beziehungen, wenn es um den Einsatz von IKT geht. Praktische und umsetzbare Maßnahmen sind erforderlich, um die Normen so zu gestalten, dass sie die Zusammenarbeit zwischen den Staaten konstant verbessern und dauerhaft Vertrauen zwischen ihnen aufbauen können. Glücklicherweise existierte für solche Maßnahmen bereits ein Modell in Gestalt des Wiener Dokuments der Verhandlungen über vertrauens- und sicherheitsbildende Maßnahmen (VSBM) der KSZE/OSZE aus dem Jahr 1990, in dem u.a. freiwillige militärische Maßnahmen festgelegt sind, die für die Erhöhung der Transparenz und die Verbesserung der Vertrauensbildung und der Rüstungskontrolle im OSZE-Gebiet von entscheidender Bedeutung sind. Im Zuge der Anpassung an den Cyberspace wurden bei diesen Maßnahmen die eher militärischen Aspekte traditioneller VSBM zugunsten einer verstärkten Cyberdiplomatie zwischen den Staaten vermieden. Zugleich sollten dadurch gleichgesinnte und nicht gleichgesinnte Staaten leichter an einen Tisch gebracht werden. VBM zur Cybersicherheit/IKT-Sicherheit sind daher als ein entscheidendes Instrument für politische Entscheidungsträger auf allen Ebenen anerkannt – von den Vereinten Nationen über regionale Organisationen bis hin zu nationalen Regierungen.

Die Diskurse über Rechtsvorschriften, Normen für verantwortungsbewusstes Verhalten von Staaten und vertrauensbildende Maßnahmen – unabhängig davon, ob diese hierarchisch oder als gleichrangige Instrumente betrachtet werden – sind in den meisten Initiativen auf hoher Ebene zur Verbesserung der Cyberstabilität zwischen den Staaten miteinander verknüpft und verstärken sich gegenseitig.

8 Vgl. Katharina Ziolkowski, Confidence Building Measures for Cyberspace – Legal Implications, Tallinn 2013, S. 32.

9 Vgl. United Nations General Assembly Document A/69/723, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, 13. Januar 2015.

In: IFSH (Hrsg.), OSZE-Jahrbuch 2017, Baden-Baden 2019, S. 227-240.

Der Einfluss der von den Vereinten Nationen eingesetzten Gruppe von Regierungssachverständigen auf den globalen Diskurs über die Förderung der Cyberstabilität zwischen Staaten

Die herrschende Unklarheit darüber, wie die Verwendung von IKTs in zwischenstaatlichen Beziehungen normativ definiert werden kann, wird noch verstärkt durch Unterschiede in den nationalen Konzepten zur Cybersicherheit/IKT-Sicherheit, eine uneinheitliche Terminologie und voneinander abweichende Definitionen sowie durch kulturelle Unterschiede und unterschiedliche Prioritäten. Als die Vereinten Nationen sich am 4. Januar 1999 in Resolution A/RES/53/70 mit dem Thema Cybersicherheit/IKT-Sicherheit befassten, standen sie daher vor einer gewaltigen Herausforderung. Bedeutende Fortschritte wurden 2003 gemacht, als die Russische Föderation erstmals die Einsetzung einer speziellen Gruppe vorschlug, die sich mit Fragen der Cybersicherheit/IKT-Sicherheit befassen sollte. Diese Gruppe wurde kurze Zeit später mit Resolution A/RES/58/32 vom 18. Dezember 2003 eingerichtet. Die neu gebildete Gruppe von Regierungssachverständigen (*United Nations Group of Governmental Experts,* UNGGE) für Entwicklungen auf dem Gebiet der Informationstechnik und Telekommunikation im Kontext der internationalen Sicherheit setzte sich aus Staaten, die auf der Grundlage einer ausgeglichenen geographischen Verteilung ausgewählt wurden, sowie den fünf ständigen Mitgliedern des Sicherheitsrats, zusammen. Die UNGGE hatte die Aufgabe, Konsensberichte zu erstellen, in denen detailliert dargelegt wird, wie die internationale Gemeinschaft am besten gegen identifizierte Bedrohungen der Cybersicherheit/IKT-Sicherheit vorgehen kann.

Der erste Bericht der UNGGE wurde am 30. Juli 2010 als Dokument A/65/201 der Generalversammlung der Vereinten Nationen veröffentlicht. Der Bericht gab einen umfassenden Überblick über die Sicherheitsbedrohungen, denen die Staaten im Cyber-/IKT-Bereich ausgesetzt sind, sowie über mögliche kooperative Maßnahmen zu deren Entschärfung. Die Empfehlungen des Berichts enthielten auch eine Art Anleitung dafür, wie zukünftige UNGGEs mit dem Thema umgehen könnten. Im Mittelpunkt standen dabei internationale Normen für die Nutzung von IKT durch Staaten sowie vertrauensbildende Maßnahmen „zur Verminderung des Risikos von Fehleinschätzungen infolge von IKT-Störungen".[10] Der Bericht von 2010 enthält keine Diskussion über das Völkerrecht, das Thema wurde jedoch später in dem Bericht von 2013, veröffentlicht als Dokument A/68/98, ausführlich behandelt.[11] Im Abschnitt über Normen, Regeln und Prinzipien für verantwortungsbewusstes Verhalten von Staaten zitiert der Bericht das Völkerrecht und insbesondere die Charta der

10 Vgl. United Nations, General Assembly, A/65/201, 30 Juli 2010, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

11 Vgl. United Nations, General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24. Juni 2013.

Vereinten Nationen sowie die daraus abgeleiteten Normen, Regeln und Prinzipien als unverzichtbar für die Wahrung eines offenen und sicheren IKT-Umfelds. In dem Bericht heißt es weiter, dass „Staaten ihren internationalen Verpflichtungen in Bezug auf völkerrechtswidrige Handlungen, die ihnen zugerechnet werden können, nachkommen müssen".[12] Auch wenn der Bericht nicht ausführlicher auf die Anwendung des Völkerrechts auf den Cyberspace eingeht, könnte er doch als wichtiger Rahmen für zukünftige Diskussionen über dieses Thema dienen. Zu VBM als dritte Komponente der Cyberstabilität heißt es in dem Bericht, dass „freiwillige vertrauensbildende Maßnahmen das Vertrauen und die Sicherheit zwischen Staaten fördern und dazu beitragen können, das Konfliktrisiko zu verringern, indem sie die Vorhersehbarkeit erhöhen und Fehleinschätzungen verringern".[13]

Der Bericht hob auch die Rolle regionaler Organisationen wie der OSZE, des Regionalforums des Verbands Südostasiatischer Nationen (ASEAN *Regional Forum*, ARF), und der Organisation Amerikanischer Staaten (OAS) bei der Förderung der Cyberstabilität und Resilienz ihrer Mitglieder hervor. Dieser Hinweis kam nicht von ungefähr. Regionalorganisationen können ihr akkumuliertes politisches Kapital und ihre bereits etablierten institutionellen Kapazitäten dazu nutzen, nicht gleichgesinnte Staaten zusammenzubringen, um über gemeinsame Sicherheitsherausforderungen wie etwa die Verbesserung der Cyberstabilität zu diskutieren. Wie im Folgenden dargelegt wird, ist die OSZE seit 2012 in diesem Bereich führend und lässt von der gemäß Beschluss Nr. 1039 des Ständigen Rates eingesetzten offenen informellen OSZE-Arbeitsgruppe vertrauensbildende Maßnahmen erarbeiten.[14] Die OSZE und die Vereinten Nationen beeinflussen sich weiterhin gegenseitig in ihrer Arbeit: Der von der UNGGE in ihren Berichten erarbeitete theoretische Rahmen bildet die Grundlage für die Diskussionen zur Cybersicherheit/IKT-Sicherheit in der OSZE und die Erfahrung der OSZE mit vertrauensbildenden Maßnahmen beeinflusst künftige Berichte der UNGGE.

Der Bericht der GGE aus dem Jahr 2015, der als Dokument A/70/174 der Generalversammlung der Vereinten Nationen[15] veröffentlicht wurde, ging ausführlich auf internationale Rechtsvorschriften, Normen für das verantwortungsbewusste Verhalten von Staaten, vertrauensbildende Maßnahmen sowie auf internationale Zusammenarbeit und Unterstützung beim Kapazitätsaufbau als gleichwertige und wichtige Säulen der globalen Cyberstabilität ein. Die Gruppe empfahl ihre eigenen VBM, die auf eine Erhöhung der Transparenz, die Erleichterung von Konsultationen und Zusammenarbeit, die Verminderung

12 Ebenda, S. 2 (eigene Übersetzung).
13 Ebenda, S. 9 (eigene Übersetzung).
14 Vgl. Organisation für Sicherheit und Zusammenarbeit in Europa, Ständiger Rat, Beschluss Nr. 1039, Entwicklung vertrauensbildender Maßnahmen zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben, PC.DEC/1039, 26. April 2012, unter: http://www.osce.org/de/pc/90632.
15 Vgl. United Nations, General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22. Juli 2015.

des Risikos von Fehleinschätzungen, Eskalationen oder Konflikten sowie den Schutz kritischer Infrastrukturen abzielten, zur Erörterung durch die Mitgliedstaaten. Sie unterstützte außerdem weiterhin den „regelmäßigen Dialog [...] im Rahmen bilateraler, regionaler und multilateraler Foren" und würdigte „die wertvollen Beiträge zur IKT-Sicherheit, die von internationalen Organisationen und regionalen Gruppen" wie etwa der OSZE „geleistet werden".[16]
Obwohl die UNGGE das höchstrangige multilaterale Organ ist, das sich mit Themen im Zusammenhang mit Cyber-/IKT-Sicherheit und -Stabilität befasst, ist ihre Zukunft seit Mitte 2017 ungewiss. Es ist der aus 25 Mitglieder bestehenden Gruppe nicht gelungen sich auf die Erarbeitung eines neuen Konsensberichts zu einigen, der die Empfehlungen der UNGGE von 2015 vertieft. Nach Aussage des Vorsitzenden der Gruppe wird es zwar keinen Konsensbericht geben, es herrsche jedoch unter den Experten noch immer Einigkeit bei Themen wie neue Risiken, Kapazitätsaufbau und vertrauensbildende Maßnahmen, Normen, Bewusstseinsbildung bei hochrangigen Entscheidungsträgern, die Durchführung von Übungen, die Erstellung von Protokollen zur Benachrichtigung über Zwischenfälle, Warnungen bei Angriffen auf kritische Infrastrukturen sowie die Verhinderung von Cyberangriffen durch nichtstaatliche Akteure.[17]

Vertrauensbildende Maßnahmen der OSZE zur Cybersicherheit/IKT-Sicherheit und damit zusammenhängende Beschlüsse

Die Beratungen der UNGGE haben die Debatte über Cybersicherheit/IKT-Sicherheit zwar im internationalen Kontext geprägt, es wäre jedoch die Aufgabe anderer, auf nationaler, subregionaler oder regionaler Ebene arbeitender Institutionen, die Verabschiedung und Umsetzung der Empfehlungen zu ermöglichen. Im April 2012 beschloss der Ständige Rat der OSZE dementsprechend, „die individuellen und kollektiven Bemühungen um eine sichere Nutzung von Informations- und Kommunikationstechnologien (ICT) umfassend und dimensionsübergreifend [...] zu verstärken".[18] Die mit dem Beschluss ebenfalls eingesetzte offene informelle OSZE-Arbeitsgruppe wurde damit beauftragt, vertrauensbildende Maßnahmen zur Verringerung der Konfliktrisiken, die sich aus dem Einsatz von IKT ergeben, auszuarbeiten. Die Arbeit zu den VBM wurde im Ministerratsbeschluss Nr. 4/12 vom 7. Dezember 2012 gewürdigt.[19] Der Beschluss zählt Cybersicherheit/IKT-Sicherheit zu den vier wichtigsten

16 Ebenda, S. 2 und 14 (eigene Übersetzung).
17 Vgl. UN GGE: Quo Vadis?, Geneva Internet Platform, Digital Watch Newsletter, Issue 22, Juni 2017, S. 6, unter: https://dig.watch/newsletter/june2017.
18 Organisation für Sicherheit und Zusammenarbeit in Europa, Ständiger Rat, Beschluss Nr. 1039, a.a.O. (Anm. 14).
19 Vgl. Organisation für Sicherheit und Zusammenarbeit in Europa, Ministerrat, Dublin 2012, Beschluss Nr. 4/12, Bemühungen der OSZE im Umgang mit grenzüberschreitenden Bedrohungen, MC.DEC/4/12, 7. Dezember 2012, S. 1, unter: https://www.osce.org/de/mc/98315.

strategischen Prioritäten der OSZE im Umgang mit grenzüberschreitenden Bedrohungen. Ebenfalls im Jahr 2012 richtete die OSZE in ihrer neu geschaffenen Abteilung Grenzüberschreitende Bedrohungen (*Transnational Threats Department*, TNTD) den Posten eines Referenten für Cybersicherheit ein, der für alle 57 Teilnehmerstaaten sowie für die Durchführungsorgane der OSZE- als Hauptkontaktstelle für alle Fragen im Zusammenhang mit Cybersicherheit/ IKT-Sicherheit fungiert.

Nach mehreren Sondersitzungen verabschiedete der Ständige Rat am 3. Dezember in Wien den Beschluss Nr. 1106, mit dem erstmals echte vertrauensbildende Maßnahmen der OSZE im Bereich Cybersicherheit/IKT-Sicherheit geschaffen wurde.[20] Die vereinbarten Maßnahmen zielten darauf ab, das Risiko von Konflikten zwischen OSZE-Teilnehmerstaaten, die sich aus dem Einsatz von IKT ergeben, zu vermindern, indem sie dazu ermutigten, frühzeitige Beratungen durchzuführen; die OSZE als Plattform für den Dialog und den Austausch von Informationen und bewährten Praktiken, nationalen Standpunkten zu Cyberbedrohungen sowie von Papieren, Strategien und Programmen zur Cybersicherheit/IKT-Sicherheit zu nutzen; Listen mit einschlägigen Terminologien bereitzustellen und ein Netz von Kontaktstellen aufzubauen, mit dem die Koordinierung ressortübergreifender Reaktionen der Regierungen auf IKT-bezogene Zwischenfälle erleichtert wird.

Dieses erste VBM-Paket der OSZE förderte eine Transparenz, die es den Staaten ermöglichen sollte, das „Auftreten" der anderen Staaten im Cyberspace zu erkennen, erleichterten eine sinnvolle Kommunikation zwischen ihnen und erhöhten die regionale Resilienz gegenüber Cyberangriffen, um so eine stabile und sichere „Cybernachbarschaft" im OSZE-Raum zu schaffen. Mit Beschluss Nr. 1106 wurde die offene informelle Arbeitsgruppe von einem *Ad-hoc*-Arrangement in eine mindestens dreimal pro Jahr zusammentretende Arbeitsgruppe verwandelt, bei deren Treffen die Teilnehmerstaaten kontinuierlich Informationen über VBM im Rahmen etablierter OSZE-Plattformen wie des *Policing OnLine Information System* (POLIS) austauschen.

Im Laufe der folgenden zwei Jahre fanden Diskussionen darüber statt, wie auf diesen ersten VBM aufgebaut werden könnte. 2016 wurden nach langen Debatten mit Beschluss Nr. 1202 des Ständigen Rates vom 10. März 2016 fünf neue Maßnahmen eingeführt.[21] Als wichtigste Bereiche dieses zweiten Maßnahmenpakets wurden genannt: die praktische Zusammenarbeit beim Schutz kritischer Infrastruktur, der Ausbau der Krisenkommunikationskanäle sowie

20 Vgl. Organisation für Sicherheit und Zusammenarbeit in Europa, Ständiger Rat, Beschluss Nr. 1106, Vorläufiger Katalog von vertrauensbildenden Maßnahmen der OSZE zur Verminderung der mit der Nutzung der Informations- und Kommunikationstechnologien verbundenen Konfliktrisiken, PC.DEC/1106, 3. Dezember 2013, unter: https://www.osce.org/de/permanent-council/109644.

21 Vgl. Organisation für Sicherheit und Zusammenarbeit in Europa, Ständiger Rat, Beschluss Nr. 1202, Vertrauensbildende Maßnahmen der OSZE zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben, PC.DEC/1202, 10. März 2016, unter: https://www.osce.org/pc/227281.

die Verbesserung der Cyberresilienz durch Zusammenarbeit mit dem Privatsektor. Dies bedeutete, dass die OSZE mit sechzehn praktischen und umsetzbare Maßnahmen, deren Implementierung durch die Ministerratsbeschlüsse Nr. 5/16[22] und Nr. 5/17[23] unterstützt wird, in das Jahr 2017 gestartet ist.
Die grundlegenden Merkmale dieser VBM – ihre Anbindung an die Empfehlungen der Berichte der UNGGE, der Grad der politischen Unterstützung durch die Teilnehmerstaaten und ihr Potenzial für eine praktische Umsetzung – machen sie zu schlagkräftigen und einzigartigen Instrumenten nicht nur im OSZE-Gebiet: Sie sind eine Quelle bewährter Praktiken und Erfahrungen, auf die auch andere Organisationen zurückgreifen können.

Schwerpunkt im Jahr 2017: Fortschritte bei der Einrichtung eines OSZE-Konsultationsmechanismus für Krisensituationen

Um wirksam werden zu können, müssen die VBM vollständig operationalisiert sein. Im Anschluss an den Ministerratsbeschluss Nr. 5/16 konzentrierten sich die Bemühungen der informellen Arbeitsgruppe daher auf die Operationalisierung einer schnellen Kommunikation auf technischer und politischer Ebene, um Spannungen und Konfliktrisiken zu vermindern, die sich aus dem Einsatz von IKT ergeben. Gemäß den Beschlüssen des Ständigen Rates bedeutet dies die Einrichtung eines Konsultationsmechanismus für Krisensituationen durch die Operationalisierung der VBM 3, 8 und 13 (PC.DEC/1202).
Wenn ein Cyber-/IKT-Sicherheitsvorfall eintritt, sind die ersten Stunden die wichtigsten – höchstwahrscheinlich aber auch die am stärksten von Konfusion, Missverständnissen und Fehleinschätzungen beherrschten. Die Gefahr, die von einer solchen Konfusion ausgeht, steigt noch weiter, wenn der fragliche Vorfall Ressourcen betrifft, die für das normale Funktionieren eines Staates entscheidend sind, und der Verdacht auf einen nicht gleichgesinnten Staat oder einen regionalen Rivalen fällt. Um eine Eskalation der aus einem solchen Vorfall resultierenden Spannungen zu verhindern, ist es von größter Bedeutung, dass sichere Kommunikationskanäle zwischen den nationalen Kontaktstellen eingerichtet sind, die dem betroffenen Staat dabei helfen können, von seinem mutmaßlichen Gegner wichtige Informationen über den Angriff zu erhalten, dessen Folgen einzudämmen und die öffentliche Reaktion auf die Krise gemeinsam zu steuern.

22 Vgl. Organisation für Sicherheit und Zusammenarbeit in Europa, Ministerrat, Hamburg 2016, Beschluss Nr. 5/16, OSZE-Bemühungen im Zusammenhang mit der Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben, MC.DEC/5/16/Corr.1, 9. Dezember 2016, unter: http://www.osce.org/cio/288086.

23 Vgl. Organisation für Sicherheit und Zusammenarbeit in Europa, Ministerrat, Wien 2017, Beschluss Nr. 5/17, Verstärkung der Bemühungen der OSZE zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben, MC.DEC/5/17.Corr.1, 8. Dezember 2017, unter: https://www.osce.org/chairmanship/361561.

Die OSZE hat die Einrichtung eines Konsultationsmechanismus in die Wege geleitet, der solche Reaktionen mithilfe der VBM 3, 8 und 13 ermöglichen würde. Die drei VBM fordern die Staaten dazu auf, auf geeigneter Ebene Konsultationen durchzuführen, um Risiken zu vermindern, ein Netz von Kontaktstellen auf politischer und technischer Ebene aufzubauen und sichere Kommunikationskanäle zu nutzen, die einen solchen Kontakt erleichtern würden. Das Zusammenwirken dieser drei VBM hilft die grundlegenden Fragen zu beantworten: Wer löst wie bzw. wann welchen Mechanismus aus? Sobald das Netzwerk vollständig operationalisiert und eingerichtet ist, wird es den OSZE-Teilnehmerstaaten ein einzigartiges Instrument zur Bewältigung internationaler Cyberzwischenfälle und ihrer unvermeidlichen Folgen zur Verfügung stellen.

Wie VBM in einem durch IKT hervorgerufenen Krisenszenario eingesetzt werden können

Hervorzuheben ist, dass VBM zwar darauf abzielen, Vertrauen aufzubauen und somit das Risiko nicht intendierter Konflikte vermindern, aber keinen vorsätzlichen internationalen Cyberangriff verhindern können. Was sie in einem solchen Fall jedoch allen Beteiligten zur Verfügung stellen können, ist ein Verfahren, das es ihnen ermöglicht, umgehend über Kontaktstellen miteinander zu kommunizieren und eine weitere Eskalation der Spannungen abzuwenden. Dies kann so weit gehen, dass die OSZE in einem möglichen Streit über den Einsatz von IKT zwischen Teilnehmerstaaten vermittelt.
Die einzelnen Phasen des VBM-Prozesses lassen sich am besten an einem hypothetischen Beispiel veranschaulichen. Nehmen wir an, dass Staat A Opfer eines massiven Cyberangriffs wird, der auf seine kritische Energieinfrastruktur abzielt, und dass seinem technischen Beauftragten Hinweise auf einen ungewöhnlich hohen von Staat B ausgehenden Datenverkehr vorliegen. Ein Beobachter wird wahrscheinlich zunächst davon ausgehen, dass entweder Staat B einen direkten Cyberangriff gestartet oder aber einen Dritten mit einem solchen beauftragt hat. Zu diesem Zeitpunkt, an dem beide Staaten noch mit der Analyse der Situation befasst sind, könnten erste VBM zur Anwendung kommen. Wenn Staat B über die OSZE-Plattformen genügend Informationen ausgetauscht hat, die dazu beitragen, sich ein Bild von seinen Fähigkeiten und Aktivitäten machen zu können, können die zuständigen Stellen von Staat A möglicherweise erkennen, ob der Angriff dem üblichen Auftreten von Staat B im Cyberspace entspricht. Wenn dies nicht der Fall ist, wäre es wahrscheinlicher, dass der Angriff lediglich durch das Territorium von Staat B geführt oder ohne dessen Wissen gestartet wurde. Parallel dazu könnten die Kontaktstellen beider Staaten den OSZE-Konsultationsmechanismus für Krisensituationen dazu nutzen, wichtige Informationen auszutauschen, um Unterstützung zu bitten und eine gemeinsame Reaktion auf die sich anbahnende Krise zu planen.

In dieser hypothetischen Situation können Staaten auf eine Reihe wichtiger VBM zurückgreifen, um eine durch IKT hervorgerufene Krise zu entschärfen, mögliche Fehlinformationen aufzudecken und im Rahmen etablierter OSZE-Netzwerke zusammenzuarbeiten, um Spannungen abzubauen. Angesichts der in jüngster Zeit zunehmenden Zahl spektakulärer Cyberangriffe und -vorfälle ist es möglich, dass dieses abstrakte Szenario in naher Zukunft Wirklichkeit wird und dass dabei alle operationalisierten VBM zum Einsatz kommen.

Verbleibende Herausforderungen und Maßnahmen zur Implementierung von VBM

Abgesehen von den unmittelbar mit dem Konsultationsmechanismus für Krisensituationen zusammenhängenden VBM ist die nominelle Implementierungsrate für alle VBM, die dem Prozentsatz der Teilnehmerstaaten entspricht, die mindestens eine der sechzehn Maßnahmen umsetzen, mit 91 Prozent sehr hoch. Angesichts der Tatsache, dass es sich bei den VBM der OSZE zur Cybersicherheit/IKT-Sicherheit um einen freiwilligen Mechanismus handelt und ihre Anwendung auf der Anerkennung ihres praktischen Nutzens seitens der Teilnehmerstaaten beruht, ist dieser Prozentsatz sogar besonders hoch. Die Implementierungsrate lässt jedoch einiges außen vor. Beispielsweise sind zwar die meisten Teilnehmerstaaten aktiv in den Prozess eingebunden, aber nicht alle Staaten halten alle VBM für gleichermaßen wichtig – die durchschnittliche Implementierungsrate für alle sechzehn VBM liegt bei rund 40 Prozent. Zudem lässt sich durch die bloße Betrachtung der Prozentzahlen der Implementierung der VBM nicht erkennen, auf welche Hindernisse die Staaten bei der Durchführung einzelner Maßnahmen treffen.

Aus diesem Grunde war es notwendig, zunächst die wichtigsten Probleme bei der Umsetzung zu identifizieren und dabei gleichzeitig die besonderen nationalen und subregionalen Gegebenheiten zu berücksichtigen, die die Operationalisierung der Maßnahmen begünstigen oder behindern könnten. Dies wiederum erforderte sowohl eine umfassende *Open-Source*-Datenerhebung und -Analyse als auch eine neue, unvoreingenommene Perspektive. Einige Teilnehmerstaaten empfahlen daher, die OSZE solle „in Erwägung ziehen, wissenschaftliche Einrichtungen mit der Durchführung vergleichender Analysen der bei der Implementierung des ersten VBM-Pakets ausgetauschten Informationen zu beauftragen“.[24] Dieser Empfehlung und mit der Unterstützung Italiens, Deutschlands und der Schweiz rief das OSZE-TNTD gemeinsam mit dem Institut für Politik- und Sozialwissenschaften der Universität Florenz 2016 eine entsprechende Initiative ins Leben. Diese Partnerschaft wurde durch die Ein-

24 OSCE Switzerland 2014, OSCE Chairmanship Event Summary, Information and Communication Technologies (ICT) Confidence Building Measures (CBMs): Promoting implementation, supporting negotiations, CIO/GAL/238/14, 22. Dezember 2014, S. 1 (eigene Übersetzung).

richtung einer informellen akademischen Lenkungsgruppe erweitert, die sich aus wissenschaftlichen Forschungseinrichtungen aus dem gesamten OSZE-Gebiet zusammensetzt.
Aus dieser Zusammenarbeit gingen 2017 zwei Papiere hervor:

a) Ein Forschungsbericht mit dem Titel „Analyse der Implementierung des ersten Pakets vertrauensbildender Maßnahmen zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben“ sowie
b) „Vorschläge aus der Wissenschaft für einen Arbeitsplan zur Unterstützung der Implementierung von VBM“, die konkrete Instrumente, Maßnahmen und Mechanismen, einschließlich Maßnahmen zum Kapazitätsaufbau, identifizierten und auflisteten, die die Durchführung von VBM maßgeblich verbessern sollen.

Das OSZE-TNTD wird künftig zur Bewältigung der wichtigsten in dem Arbeitsplan ermittelten Herausforderungen bei der Operationalisierung von VBM, u.a. durch die Entmystifizierung von VBM durch *E-Learning*-Module und den Ausbau der Fähigkeiten politischer Entscheidungsträger durch eine Reihe umfassender, regionaler und szenarienbasierter Diskussionen, beitragen.

VBM außerhalb des OSZE-Gebiets – Andere regionale Mechanismen sowie interregionale Initiativen der OSZE im Bereich Cybersicherheit/IKT-Sicherheit

Der Aufbau von Vertrauen zur Verminderung von Spannungen und Konfliktrisiken, die sich aus dem Einsatz von IKT ergeben könnten, ist eine wahrhaft globale Aufgabe. Das bedeutet auch, dass der infolge des missbräuchlichen Einsatzes von IKT in einer Region der Welt eingetretene Vertrauensverlust die Sicherheit und Stabilität außerhalb dieser Region bedrohen kann. Umgekehrt können Maßnahmen zur Stärkung des Vertrauens und zur Förderung von Sicherheit und Stabilität in einer Region eine stabilisierende Wirkung auf Staaten in einer anderen Region haben. Darüber hinaus können regionale Organisationen und Mechanismen, wie im Abschnitt über die Arbeit der UNGGE erörtert, als optimale Instrumente für die Implementierung und Koordinierung internationaler Sicherheitsempfehlungen, einschließlich der Entwicklung von VBM zur Cybersicherheit/IKT-Sicherheit, dienen. Dies unterstreicht die Notwendigkeit, sich der Vernetzung mit anderen regionalen Prozessen bewusst zu sein und sie aktiv zu fördern. In Amerika z.B. beschloss die OAS am 10. April 2017 auf einem Treffen des Interamerikanischen Komitees gegen Terrorismus (*Inter-American Committee against Terrorism*, CICTE), eine Arbeitsgruppe

für Zusammenarbeit und vertrauensbildende Maßnahmen im Cyberspace einzusetzen,[25] und in der asiatisch-pazifischen Region billigten die ARF-Minister beim 24. ASEAN-Regionalforum am 7. August 2017 einen Vorschlag, ein ARF-Zwischentreffen zur Cybersicherheit/IKT-Sicherheit einzurichten.[26]

OSZE-Kooperationspartner und praktische Zusammenarbeit

Die OSZE selbst erstreckt sich in Gestalt ihrer langjährigen Kooperationspartner in Asien und im Mittelmeerraum – Afghanistan, Australien, Japan, der Republik Korea und Thailand einerseits und Ägypten, Algerien, Israel, Jordanien, Marokko und Tunesien andererseits – über die euroatlantische Region hinaus. Im Laufe der Zeit haben sich die Partner und die 57 OSZE-Teilnehmerstaaten in zahlreichen Dokumenten wie z.B. in dem am 2. Dezember 2003 verabschiedeten Beschluss Nr. 571 des Ständigen Rates dazu verpflichtet, verschiedene Bereiche der Zusammenarbeit ausfindig zu machen. Der Beschluss ermutigt die Kooperationspartner, „freiwillig die OSZE-Normen, -Prinzipien und -Verpflichtungen umzusetzen", und ruft dazu auf „zu erkunden, in welchem Umfang eine umfassendere Weitergabe der OSZE-Normen, -Prinzipien und -Verpflichtungen möglich ist".[27] Im Bereich Cybersicherheit/IKT-Sicherheit hat dies zu gemeinsamen Anstrengungen zur Identifizierung neuer Wege der Zusammenarbeit, zum Austausch von bewährten Praktiken und Erfahrungen sowie zur Harmonisierung paralleler VBM-Prozesse über regionale Trennlinien hinweg geführt. Zu diesen Aktivitäten gehören seit 2016:

- *Konferenzen mit den Kooperationspartnern in Asien*: Im Rahmen der vom 6.-7. Juni 2016 in Bangkok tagenden OSZE-Asienkonferenz fand eine Nebenveranstaltung zur Stärkung der Cybersicherheit/IKT-Sicherheit, zur Neugestaltung der gegenwärtigen Dynamik im OSZE-Gebiet, zur Bekräftigung der Rolle regionaler Organisationen und zur Sondierung möglicher Wege der konkreten Zusammenarbeit mit den Partnern in Asien statt. Diese Themen wurden auf der interregionalen IKT/Cybersicherheitskonferenz, die vom 4.-5. April 2017 in Seoul stattfand, weiter vertieft.
- *Initiative auf dem Global Forum for Cyber Excellence (GFCE)*: Am 31. Mai 2017 riefen die OSZE und Deutschland eine gemeinsame Initiative

25 Vgl. Inter-American Committee against Terrorism (CICTE), Establishment of a Working Group on Cooperation and Confidence-Building Measures in Cyberspace, CICTE/RES.1/17, 10. April 2017.

26 Vgl. 24th ASEAN Regional Forum, Chairman's Statement, Partnering for Change, Engaging the World, Manila, Philippinen, 7. August 2017, S. 7.

27 Organisation für Sicherheit und Zusammenarbeit in Europa, Ständiger Rat, Beschluss Nr. 571, Fortsetzung des Dialogs und der Zusammenarbeit mit den Kooperationspartnern und Erkundung des möglichen Umfangs für die umfassendere Weitergabe der OSZE-Normen, -Prinzipien und -Verpflichtungen an andere, PC.DEC/571, 2. Dezember 2003, unter: http://www.osce.org/pc/18297.

ins Leben, die darauf abzielt, die aktuellen Diskussionen über regionale Foren hinausgehend miteinander zu verbinden, die Implementierung von VBM zu beschleunigen und den konzeptionellen Zusammenhang zwischen den Normen für verantwortungsbewusstes Verhalten von Staaten im Cyberspace und dem Aufbau von Kapazitäten und Vertrauen weiter zu erkunden. Dies soll durch aktive Partnerschaften mit regionalen Organisationen wie der OAS, den ARF-Mitgliedstaaten und der Afrikanischen Union (AU) erreicht werden.

Fazit

Mit der zunehmenden Verbreitung der IKT wird der Bedarf an einem stabilen, widerstandsfähigen, berechenbaren und sicheren Cyberspace voraussichtlich weiter steigen. Bedrohungen der Cybersicherheit/IKT-Sicherheit, die ihrem Wesen nach transnational sind, erfordern ein größeres Engagement der internationalen Gemeinschaft, wenn ihnen wirksam begegnet und die Eskalation von Spannungen und den damit verbundenen Risiken vermieden werden soll. Gleichzeitig ist es, obwohl die Gefahr auf der Hand zu liegen scheint, weniger einfach, Mittel zu finden, sie zu bekämpfen. Dies erfordert das Zusammenwirken zahlreicher Akteure mit unterschiedlichen Prioritäten und Agenden, die Beantwortung ungelöster völkerrechtlicher Fragen, Normen für verantwortungsbewusstes Verhalten von Staaten und Maßnahmen zur Vertrauensbildung zwischen Staaten. Wie die jüngste UNGGE gezeigt hat, gibt es selbst für den umfassendsten Ansatz im Zusammenhang mit diesem Thema keine Erfolgsgarantien.

Innerhalb der OSZE befindet sich der VBM-Prozess in vieler Hinsicht noch immer im Anfangsstadium – wichtige Maßnahmen müssen noch operationalisiert, Implementierungsprobleme müssen gelöst und die interregionale Zusammenarbeit im Bereich Cybersicherheit/IKT-Sicherheit muss institutionalisiert werden. Die OSZE hat jedoch dank des Engagements ihrer Teilnehmerstaaten und Kooperationspartner seit 2012 durch die Beschlüsse 1039, 1106 und 1202 des Ständigen Rates, die Ministerratsbeschlüsse 5/16 und 5/17 und die kontinuierliche Arbeit der informellen Arbeitsgruppe und des Referenten der OSZE für Cybersicherheit messbare Fortschritte erzielt. Die OSZE und das TNTD bleiben dem VBM-Prozess und der Verbesserung der Cyberstabilität und -resilienz im OSZE-Gebiet und darüber hinaus verpflichtet.