Cybersecurity

Thesen zum Referat von Stefanie Schmahl, Würzburg

I. Empirische Diagnose: Das Bedrohungspotential im Cyberspace

1. Die Anzahl schädlicher Computernetzwerkoperationen hat in den letzten Jahren exponentiell zugenommen. Zu den Opfern spektakulärer Cyberangriffe zählen etwa Estland, Georgien, der Iran, die Ukraine und die USA. Bis heute ist allerdings unklar, wer die jeweiligen Cyberoperationen zu verantworten hat.

II. Terminologische Abgrenzungen: Cybersecurity als Gegenwehr zu schädlichen Cyberoperationen

2. Obgleich nachhaltige Verwerfungen bisher nicht aufgetreten sind, geht von Cyberoperationen ein hohes Bedrohungspotential für die internationale Stabilität aus, dem sich das Recht stellen muss. Welche zulässigen defensiven und präventiven Abwehrmechanismen gegen Cyberangriffe von außen bestehen, ist die zentrale Frage der Cybersecurity. Dabei darf Cybersecurity nicht mit dem Schlagwort „*Cyberwar*“ gleichgesetzt werden; sie erstreckt sich etwa auch auf das Problemfeld des Cyberterrorismus.

3. Die bei schädlichen Computernetzwerkoperationen verwendeten Techniken sind variantenreich; im Wesentlichen lassen sich nicht-intrusive und intrusive Operationsmethoden unterscheiden. Nicht-intrusive Cybermethoden dringen nicht in das Computersystem ein, sondern verringern oder unterbinden dessen Funktionsfähigkeit. Intrusive Operationen greifen hingegen gezielt auf ein informationstechnisches System zu. Die Konsequenzen bleiben intrinsisch, wenn etwa Daten eines Computers ausgespäht werden (sog. „*Computer Network Exploitation*“). Werden Daten indes umfunktioniert oder gelöscht, zeitigt dies regelmäßig netzexterne Wirkungen, die im Extremfall destruktive Folgen für Sachwerte und Leib und Leben haben können (sog. „*Computer Network Attack*“).

4. Ungeachtet ihrer unterschiedlichen Arten und Ausprägungen haften allen Cyberoperationen strukturelle Gemeinsamkeiten an, die die bestehenden völkerrechtlichen Grundprinzipien herausfordern. Dazu zählen die rasante Schnelligkeit, die Neutralität und die Ubiquität von Datenübertragungen, die amorphe Wirkungsstruktur von Cyberoperationen und der „*dual use*“-Charakter der Informationsinfrastruktur. Probleme bereiten zudem die mangelnde technische Beherrschbarkeit mancher Schadprogramme, die quasi-staatlichen Fähigkeiten bestimmter nichtstaatlicher Akteure und vor allem die Möglichkeit, Cyberattacken anonym, technisch verschleiert und aus großer Distanz durchzuführen.

III. Rechtlicher Befund: Anwendbare Rechtsregeln im Bereich der Cybersecurity

5. Wie bei allen technischen Errungenschaften der Vergangenheit hinken positivrechtliche Normierungen und normative Einschätzungen dem komplexen Bereich der Cybersecurity hinterher. Der zur Verfügung stehende Kanon internationaler Verträge hält für die modernen Herausforderungen bislang keine maßgeschneiderte Lösung bereit. Auch ein von der Staatenpraxis getragenes *ius digitale emergens* ist (noch) nicht ersichtlich. Zu untersuchen ist daher, ob eine evolutiv-dynamische Auslegung der völkerrechtlichen Grundregeln die digitale Gefahrenlage in den Griff zu bekommen vermag oder ob selbst moderne Deutungen letztlich doch auf einem zu unbestimmten Niveau verbleiben, weshalb die Entwicklung spezieller Regeln zur Internetsicherheit notwendig sein könnte.

IV. Therapiemöglichkeiten *de lege lata et ferenda*: Sicherheitsmechanismen im Cyberspace

1. Defensive Abwehrmaßnahmen

a) Selbstverteidigung und Gegenmaßnahmen

6. Bestimmte Erscheinungsformen von Cyberoperationen erfüllen den Gewaltbegriff. Denn hierfür genügt eine indirekte Schadenszufügung, die nicht in engem Wortsinne zerstörerisch sein muss. Wegen des Erfordernisses gleicher Wirkung zum Einsatz konventioneller Waffengewalt müssen aber physische (netzexterne) Objekt- oder Personenschäden auch bei Cyberoperationen unwiderstehlich zu erwarten sein.

7. Nicht jede bewaffnete Gewalt eröffnet den Anwendungsbereich des Selbstverteidigungsrechts. Damit ein bewaffneter Angriff vorliegt, müssen Ausmaß und Wirkungen der durchgeführten Aktion erheblich sein. Auf Cyberoperationen gewendet bedeutet dies, dass die eingesetzte Schadsoftware signifikante physisch-destruktive Wirkungen auf den Gegner zeitigen muss.

8. Auf Handlungen, die den Schwellenwert zum bewaffneten Angriff nicht überschreiten, aber als Verletzungen des Gewalt- oder des Interventionsverbots zu qualifizieren sind, darf nur mit Gegenmaßnahmen reagiert werden. Dies gilt prinzipiell auch bei der Akkumulation verschiedener Cyberereignisse (sog. „Cyber-Kampagnen“). Da Cyberoperationen überwiegend verdeckt erfolgen und ihre Wirkungen häufig nicht sofort ersichtlich sind, ist es schwierig, wenn nicht gar unmöglich, einen Fortsetzungszusammenhang im Sinne der Doktrin der Nadelstichtaktik substantiiert darzulegen.

9. Desgleichen kommt eine vorbeugende Selbstverteidigung gegen schädliche Cyberattacken nahezu nicht in Betracht. Unter Zugrundelegung der *Webster*-Formel genügt es nicht, dass destruktive Schadprogramme bloß auf Rechnern abgelegt sind; frühestens ihr nachweisbares Einschleusen in Datenbestände des Opferstaates kann als unmittelbar bevorstehender Cyberangriff gewertet werden. Zudem können inaktive, „schlafende“ Schadprogramme, sind sie entdeckt, isoliert oder anderweitig technisch unschädlich gemacht werden mit der Folge, dass die Gefahr gebannt und ein Rückgriff auf militärische Mittel ausgeschlossen ist.

b) Zurechnungsfragen

10. Die Frage, wer der richtige Adressat einer Abwehrmaßnahme ist, bereitet Schwierigkeiten, sofern nichtstaatliche Akteure Cyberoperationen durchführen, die nicht kraft staatlicher Ermächtigung hoheitliche Aufgaben erfüllen. Für die Zurechnung genügt zwar auch, dass ein nichtstaatlicher Akteur in einer faktischen Sonderverbindung zum Staat steht, weil er von diesem als „verlängerter Arm“ gelenkt oder kontrolliert wird. Nicht ausreichend ist aber, dass im Internet Informationen zu „*hacking tools*“ zu finden sind, auf die von individuellen Hackern in eigener Initiative zugegriffen wird. Selbst der ICTY erstreckt den gegenüber dem „*effective control*“-Test des IGH deutlich breiteren Zurechnungsmaßstab der „Gesamtkontrolle“ nicht auf einzelne Individuen oder unorganisierte Gruppen. Anderes gilt lediglich, wenn der Staat das Verhalten privater Hacker als eigenes anerkennt oder solidarisch unterstützt. Dann kann in einer Gesamtschau eine substantielle Verwicklung vorliegen und sogar eine rückwirkende Zurechnung zum „Hintergrundstaat“ in Betracht kommen.

11. Davon zu trennen sind diejenigen Konstellationen, in denen ein Staat Cyberangriffe von selbständig handelnden „*hacktivists*“ auf seinem Territorium nicht unterbindet, ihm also lediglich ein Unterlassen seiner aus dem völkerrechtlichen Schädigungsverbot folgenden Schutzverpflichtung vorge-

worfen wird. Anders als bei der unmittelbaren Zurechnung aufgrund positiven Tuns ist hier der erforderliche Maßstab für die staatliche Verantwortungsübernahme bloß die sog. „*due diligence*“. Danach müssen die Staaten angemessene Präventions- und Repressionsmaßnahmen bereithalten, um schädliche Cyberoperationen unter ihrer jeweiligen Gebiets- und Personalhoheit nach Möglichkeit zu unterbinden und zu ahnden. Verstöße gegen diese Pflicht schaffen ein eigenständiges staatliches Unrecht, auf das mit Gegenmaßnahmen reagiert werden darf. Ein Recht auf militärische Gegenwehr muss jedoch ebenso ausscheiden wie eine über den erwähnten Sorgfaltsmaßstab hinausgehende striktere Haftung. Eine „*obligation of result*“ oder der Standard des „*should have known*“ würde die Staaten schlichtweg überfordern, da ihnen nicht zumutbar ist, jede schädliche Datenbewegung auf ihrem Hoheitsgebiet zu kennen oder zu ermitteln.

12. Sind weder Beteiligung noch Duldung des Staates nachweisbar, darf der Opferstaat seine Abwehrmaßnahmen nur in außergewöhnlichen Notstandssituationen auf das Territorium des Aufenthaltsstaates ohne dessen Billigung ausdehnen. Anderes gilt allerdings im Blick auf die gewaltsame Bekämpfung von Cyberterroristen und ihrer Einrichtungen. Der IGH hat in seinem *Mauer-Gutachten* noch einmal die Notwendigkeit einer staatlichen Zurechnung betont, um eine Selbstverteidigungslage zu begründen.

c) Beweisstandards

13. Anonyme oder verdeckte Informationsangriffe stellen den Regelungskomplex der Abwehrmaßnahmen vor besondere Herausforderungen. Denn jede Art defensiver Gegenwehr setzt voraus, dass Angriff und Angreifer eindeutig identifizierbar sind. Nach den völkerrechtlichen Zurechnungsprinzipien trägt der angegriffene Staat hierfür die Beweislast.

14. Das Vertrauen darauf, dass künftige technologische Entwicklungen die Identifizierung des Angreifers ermöglichen werden, ist, rechtlich besehen, nicht zufriedenstellend. Ebenso wenig kann die Ansicht überzeugen, wonach bei Cyberoperationen eine Abweichung vom Erfordernis der „*reasonable certainty*“ zugunsten von widerlegbaren Vermutungen angezeigt sei. Ein derartiger Dispens von Kausalitätssträngen und Beweisregeln findet weder im Gewohnheits- noch im Vertragsrecht eine Stütze. Die Schutzpflichtenlehre darf mit dem Recht der Abwehrmaßnahmen nicht verknüpft werden. Der irrtümlichen Ausübung des Selbstverteidigungsrechts insbesondere gegen einen unrichtigen Adressaten wohnt ein hohes Eskalationspotential inne; auch der willkürliche Rückgriff auf Gegenmaßnahmen birgt Gefahren für die internationale Sicherheit.

2. Offensiv-präventive Sicherheitsmaßnahmen

15. Anstelle der Anwendung defensiver Rechtsinstitute, die bei Verschleierung der Urheberschaft einer Cyberoperation an Wirksamkeit verlieren, bietet sich die Heranziehung des dem internationalen Umwelt- und Technikrecht bekannten Vorsorgeprinzips an, das auf generelle Gefahrenlagen und Situationen des Nichtwissens reagiert und der Risikominimierung im Vorfeld dient. Derartige Vorsorgemaßnahmen sind auch dem humanitären Völkerrecht geläufig.

16. Ein umfassendes Entwicklungs- und Einsatzverbot für Cyberoperationen kommt nicht in Betracht. Arten und Ausprägungen von Cybermethoden sind viel zu weit gefasst, und die wirksame Kontrolle eines solchen Verbots ist nicht möglich. Der jüngst von Russland, China und anderen Staaten vorgelegte Entwurf einer „*Convention on International Information Security*“ sieht zwar von einem voll-

ständigen Verbot ab, birgt aber Risiken einer Eindämmung der individuellen Meinungs- und Informationsfreiheit.

17. Der Gedanke der Vorsorge ist allerdings nicht auf ein Verbot von risikobehaftetem Verhalten beschränkt. Das Vorsorgeprinzip umfasst auch niederschwellige Maßnahmen und bezieht darüber hinaus den Initiator der Gefahrenlage mit ein. Aus dem Vorsorgeprinzip können deshalb Sorgfaltspflichten erwachsen, die sich an alle Staaten richten. Eine solche gemeinsame „*duty to prevent cyber attacks*" ist konzeptionell entwickelbar, indem z.B. Verhaltensmaximen wie gegenseitige Pflichten zu Information, Konsultation, Risikoabschätzung und Rechtshilfe etabliert werden. In dem Maße, wie derartige Verhaltensstandards vereinbart werden, können *erga omnes* wirkende Verpflichtungen entstehen, die bei Verletzung sogar eine Duldungspflicht gegenüber Gefahrenabwehrmaßnahmen anderer Staaten begründen.

V. Synthese und Fazit: Das internationale Recht der Cybersecurity als Querschnittsmaterie

18. Das internationale Recht der Cybersecurity ist eine Querschnittsmaterie, die eine ganze Palette von Regeln und Prinzipien des Völkerrechts auf den Prüfstand stellt und vor allem wegen ihrer technologischen Herausforderungen auch auf interdisziplinäre Erkenntnisgewinnung angewiesen ist. Aus völkerrechtlicher Perspektive ist freilich festzuhalten, dass ein grundlegender Paradigmenwechsel im Sinne der Erarbeitung neuer materiell-rechtlicher Parameter zur Internetsicherheit nicht angezeigt ist. Die tatbestandlichen Voraussetzungen von schädlichen Cyberoperationen lassen sich nur schwer konsentieren; nicht von ungefähr lässt selbst die *Cybercrime*-Konvention des Europarates den Vertragsstaaten einen weiten Beurteilungsspielraum.

19. Die neuen informationstechnischen Bedrohungen sind prinzipiell auf dem Boden des gegenwärtigen Rechtsinstrumentariums zu bewältigen, das schon deswegen seine Berechtigung hat, weil es der Konfliktvermeidung dient. Termini wie „Intervention", „Gewalt" oder „bewaffneter Angriff" können so evolutiv-dynamisch interpretiert werden, dass sie auf die Realität der modernen Informationsgesellschaften passen.

20. Selbst die für das Internet typische Anonymität und Verschleierungsmöglichkeit führt nicht dazu, dass die Grundprinzipien des Völkerrechts obsolet würden. Defizite im Tatsächlichen, gerade bei der Frage der Identifikation und Zuordnung, sind auch anderen Bereichen wie etwa dem internationalen Terrorismus und der asymmetrischen Kriegführung bekannt. Diesen Schutzlücken können und müssen die Staaten, deren Bedeutung als Garanten für den virtuellen Raum beständig wächst, mit einer Intensivierung der zwischenstaatlichen Kooperationsbemühungen zur konkretisierenden Ausgestaltung der bestehenden Sorgfalts- und Vorsorgepflichten entgegenwirken. *Erga omnes* geltende Verhaltensmaximen zur Minimierung des Risikos schädlicher Cyberoperationen sind anders als materielle Rechtsregime vergleichsweise schnell verhandelbar und dürften auch der rasanten technologischen Entwicklung standhalten.