Pax Digitalis

In der digitalen Welt lösen sich Staatsvolk und Staatsgewalt auf, Unternehmen werden immer mächtiger. Über die Grenzen des Völkerrechts im Cyberraum

Von Maxim Asjoma und Christoph Meinel

Es ist erst wenige Jahre her, als umfassende nationale Bedrohungen durch Cyberterror und Cyberkrieg lediglich Vorlagen für die Drehbücher von Hollywood-Blockbustern waren. Heute hat sich das verändert. Immer mehr Menschen und Maschinen verbinden sich über das Internet. Diese Entwicklung ist nicht mehr aufzuhalten und nimmt seit einigen Jahren rasant zu. Im gleichen Maße vermehren sich auch die Angriffsvektoren auf Personen, Unternehmen, NGOs und Staaten. Großangelegte Hackerattacken wie diejenigen des Mirai-Botnetzwerks, das die öffentliche Infrastruktur zahlreicher europäischer Staaten lahmlegte, oder der Stuxnet-Angriff, mit dem iranische Uranzentrifugen zerstört wurden, zeigen, wie nachhaltig physische und digitale Aggressionen verschmelzen.

Krieg früher und heute

Seitdem es Staaten gibt, werden Konflikte um Territorien, Machtansprüche und Ausbeutungsrechte von Ressourcen geführt. Die Mittel, mit denen Konflikte geführt werden, transformieren sich jedoch zusehends. Während es in vergangenen Zeiten das Ziel war, das begehrte Territorium durch physische Präsenz zu beherrschen, werden in Zukunft relativ „einfache“ digitale Mittel ausreichen, um den erwünschten Effekt im Cyberraum zu erzielen.

Kritische Infrastrukturen, die an das Internet angeschlossen sind, lassen sich von überall her auf der Welt angreifen. Dazu braucht es lediglich einen Computer, eine gute Internetleitung und erfahrene Hacker. Die Kosten eines verheerenden Angriffs lassen sich so stark minimieren, und selbst kleine Staaten oder Terrorgruppen können Fähigkeiten entwickeln, die vormals nur einer gut funktionierenden Armee vorbehalten waren (zum Beispiel Zerstörung von Infrastrukturen über cyberphysische Schnittstellen oder Denial of Service-Angriffe).

Schon heute begleiten Cyberangriffe analoge Kriegsführung. Je stärker jedoch die Digitalisierung voranschreitet, desto weniger werden analoge Waffen sowie Statthalter oder Besatzer notwendig sein. Gewalt wird verstärkt über digitale Wege ausgeübt werden. Es wird möglich sein, hochdigitalisierte Staaten über weite Distanzen zu unterwerfen. Auch Propaganda- und Informationskriege verlagern sich in den digitalen Raum. Der Unterschied zu früher ist, dass auch hier die Mittel der „soften" Kriegsführung deutlich billiger geworden sind. Es braucht heute lediglich einen geschickten Hacker, um im großen Maßstab Informationsschlachten zu führen. Über das Internet kann jede Nachricht – wahr oder falsch – mit Lichtgeschwindigkeit über den Globus geschickt werden, Informationen über Feinde lassen sich auf einfachste Weise über das Web erlangen.

Kriege verlagern sich zusehends in den digitalen Raum

Ursprünge des Völkerrechts

Um die Frage zu reflektieren, wie man mit den neuen digitalen Aggressionen umgehen kann, lohnt ein Blick in die Vergangenheit. Die Menschheitsgeschichte hat zur Genüge gezeigt, dass kriegerische Auseinandersetzungen in der Natur des Menschen zu liegen scheinen. Zu allen Zeiten wurde deshalb versucht, dieser Natur entgegenzuwirken und vermittelnde Institutionen informeller und formeller Art zu schaffen, um Gewalt einzudämmen und zu kontrollieren. In diesem Prozess haben immer „große Erzählungen" wie die klassischen Mythen, philosophische Staatsentwürfe sowie Weltreligionen die Rolle eingenommen, Regeln für ein friedliches Zusammenleben zu setzen.

Der Westfälische Frieden, der 1648 den großen europäischen Bürger- und Glaubenskrieg beendete, kann in dieser logischen Folge als ein erstes wesentliches Ereignis angesehen werden, das eine moderne völkerrechtliche Ordnung definierte. Die Verträge regelten erstmals die territorialen Verhältnisse sämtlicher Großmächte und kleinerer Staaten in Europa. Der Westfälische Frieden wurde so zu einem der wichtigsten Initiale moderner staatlicher Souveränität.

Zur Basis für das in der Folge entstehende Völkerrecht wurde die vom österreichischen Philosophen und Juristen Georg Jellinek entwickelte „Drei-Elemente-Lehre", nach denen nur Institutionen als Staaten gelten, die ein Staatsgebiet, ein Staatsvolk und Staatsgewalt haben. Auf der Grundlage, dass Staaten diejenigen Institutionen sind, die Kriege zu führen in der Lage sind, wurden weitere völkerrechtliche Normen entwickelt, wie die Haager Landkriegsordnung, die Genfer Konvention, das Seerechtsübereinkommen, die Charta der UN, der ABM-Vertrag sowie sämtliche ABC-Waffen-Vereinbarungen. Die meisten Staaten sind in der Folge auch Mitglieder der Vereinten Nationen und verhandeln globale Sicherheitsfragen.

Mit zunehmender Digitalisierung treten nun ganz neue und bisher unbeachtete Phänomene auf, die die Wirkung des Völkerrechts, wie wir es heute kennen, grundsätzlich infrage stellen.

(a) Das Staatsgebiet: Die aktuell gängige völkerrechtliche Praxis geht davon aus, dass Cyberangriffe von denjenigen Territorien ausgehen, wo die Server stehen, die zum Angriff genutzt werden. Eine Zurechnung von Verantwortung möglicher Cyberaggressionen erfolgt demnach über die physische Lokalität der

zur Aggression genutzten Hardware. Ein solcher Rückschluss ist allerdings nicht zulässig, denn das Internet zeichnet sich durch seine millionenfache Vernetzung von Servern in unterschiedlichen Staaten rund um den Globus aus. Der letzte Durchgangspunkt eines Cyberangriffs sagt also technisch keineswegs etwas darüber aus, von wo der Angriff tatsächlich initiiert wurde.

Mehr noch, infolge der digitalen Transformation verlieren räumliche Distanzen ihre Bedeutung. Im Cyberspace kollabiert der Raum, alles ist dort gleich weit „entfernt". Wenn räumliche Ausdehnung keine Rolle mehr spielt, dann hat das direkte Auswirkungen auf unser Verständnis von Staaten, die nach Jellinek vor allem über ihre Territorien definiert sind. In einem „Nicht-Raum" haben Staaten nach klassischer Auffassung keine Basis und Wirkmächtigkeit.

Im Cyberspace kollabiert der Raum

b) Das Staatsvolk: Die Digitalisierung stellt auch die hergebrachte Vorstellung vom Staatsvolk grundsätzlich infrage. Im digitalen Raum kann es allein schon aufgrund seiner Nicht-Örtlichkeit keine Staatsbürger, geschweige denn ein „Volk" im tradierten Verständnis des Wortes geben. Im Internet gibt es digitale Plattformen und Services, die von Menschen aller Herren Länder genutzt werden. So ergibt sich die Frage, an wen sich ein Völkerrecht im digitalen Raum richtet. Derzeit werden Zuschreibungen von digitalen Identitäten unterschiedlicher Dienste an real existierende Personen über IP-Adressen versucht. Aber genauso schwierig wie die Zuordnung von Servern zu Staaten ist die Zuordnung von IP-Adressen zu Individuen.

Was ist im digitalen Zeitalter Staatsvolk, was Staatsgebiet?

Digitale Identitäten verweisen zwar auf real existierende Personen, allerdings haben diese verschiedene Identitäten. Sie entstehen bei jeder Einrichtung eines Accounts bei einem Service im Internet. Im Cyberspace ist es geradezu üblich, unter verschiedenen digitalen Identitäten gleichsam „parallele" Leben zu führen und seine Loyalität zu teilen. Wie identifiziert man in der digitalen Welt Staatsbürger, wenn es keine physischen Merkmale gibt, die einer digitalen Identität anhaften? Wer oder was ist hier also das Völkerrechtssubjekt?

Gleichzeitig stellt sich die Frage, ob einer digitalen Identität überhaupt „Gewalt" angedroht und diese „entwürdigt" werden kann. Einer digitalen Identität im Cyberraum kann Gewalt nur angetan werden, wenn diese mit der realen Person in einer so engen Verbindung steht, dass ein Angriff auf die digitale Identität eine Verletzung in der analogen Welt zur Folge hat. Hier haben Staaten prinzipiell die Pflicht, ihre Staatsbürger zu schützen. Das Problem dabei ist jedoch, dass digitale Dienste und Identitäten nicht auf ein Staatsgebiet beschränkt werden können. Räumlichkeit spielt im Digitalen keine Rolle mehr. Staatliche Zugriffsmöglichkeiten sind deshalb per se eingeschränkt, sodass man zur Durchsetzung des Schutzes von Bürgern im Digitalen auf andere Akteure setzen muss. Insgesamt stellt sich also die Frage, ob eine digitale Identität in Rückkopplung auf die physische Person staatsbürgerliche Rechte erhält oder ob umgekehrt nicht vielmehr die Staatsbürgerlichkeit einer Person insgesamt durch die digitale Entgrenzung erodiert.

Bild nur in Printausgabe verfügbar

c) Die Staatsgewalt: Auch das dritte Merkmal eines souveränen Staates steht durch die Digitalisierung immer häufiger in Frage. Gängige politische und institutionell-ökonomische Theorien sehen in der Herstellung des staatlichen Gewaltmonopols die erste Aufgabe, die ein Staat verwirklichen muss, um überhaupt Staatlichkeit zu erlangen. Das Gewaltmonopol ist gleichzeitig die Voraussetzung, handlungsfähig zu sein und Politik durchsetzen zu können. Immer mehr stellt sich heute die Frage, ob sich dieser Machtanspruch, der in der analogen Welt gut erprobt ist, auch auf den digitalen Raum übertragen lässt. Fakt ist, dass die digitale Transformation technologisch weltweit von privaten Unternehmen getrieben wird. Die Verfügbarkeit digitaler Infrastruktur sowie die Mittel zur Interaktion im Digitalen und zur digitalen Machtausübung liegen also nicht mehr in der Hand der Staaten.

Prominente Beispiele zeigen, wie sich das Verhältnis zwischen Staat und Wirtschaft neu sortiert. 2016 weigerte sich der US-Konzern Apple, mit der amerikanischen Bundespolizei zusammenzuarbeiten und die Verschlüsselung von iPhones offenzulegen. Die amerikanischen Behörden waren selbst nicht in der Lage, das iPhone eines Attentäters zu entschlüsseln. Es gelang erst mit Hilfe eines israelischen Cybersecurity-Unternehmens, Zugang zur digitalen Identität des Subjekts der Strafverfolgung zu erlangen.

In Deutschland sind Digitalkonzerne, vor allem Social-Media-Plattformen wie Facebook, YouTube und Twitter, seit 2018 verpflichtet, rechtswidrige Inhalte (zum Beispiel Hassrede und Copyright-Verstöße) in ihren Netzwerken zu verfolgen und zu löschen. Mit diesem Gesetz übertragen Behörden die genuin staatliche Aufgabe zu bestimmen, was rechtlich zulässig ist und diese Entscheidung dann auch selbst zu vollstrecken, an Privatunternehmen. Es liegt keine Häme darin, wenn man feststellt, dass die Befürworter des Netzwerkdurch-

setzungsgesetzes im Kern Recht haben. Die digitale Transformation beschleunigt globale Prozesse unserer Gesellschaft in einem solchen Maße, dass die Grenzen zwischen öffentlichen und privaten Aufgaben neu vermessen werden müssen, wenn es überhaupt noch klare Grenzen geben kann. Sicherheit im digitalen Raum wird über Technologie hergestellt. Da es staatlichen Akteuren an dieser Kompetenz fehlt, stellt sich die Frage, wer dann für die Sicherheit in der digitalen Welt, für den Schutz digitaler Identitäten und digitalen Besitzes zuständig ist. Derzeit übernehmen diese Aufgabe jedenfalls Privatunternehmen.

Der Staatsgewalt entgleitet die Kontrolle der digitalen Welt

Wenn in der Vergangenheit feindliche Staaten eine Institution in einem anderen Land angriffen, dann war es die Aufgabe des Militärs, die Verteidigung zu organisieren. 2008 beauftragte der georgische Staat die Deutsche Telekom, den russischen Hackerangriff auf die zivile und militärische Infrastruktur abzuwehren.

Schon diese Beispiele zeigen, wie der Staatsgewalt die Kontrolle und Handlungsfähigkeit im digitalen Raum langsam entgleiten. Welche neuen völkerrechtlichen Probleme ergeben sich daraus?

Die Grenzen zwischen Krieg, Terror und Verbrechen verschwimmen

Es ist heute gänzlich ungeklärt, ab wann ein Cyberangriff als kriegerische Handlung einzustufen ist. Es fehlt im Ansatz jede Verständigung darüber, wer analog zur Haager Landkriegsordnung als Kombattant gilt. Cyberkonflikte werden meist hybrid geführt. Staaten und Konfliktparteien attackieren selbst und beauftragen Private, um zu hacken. Analoge Kriegshandlungen werden inzwischen häufig von Cyberangriffen vorbereitet und begleitet. Wo verlaufen da die Grenzen zwischen Verbrechen, Terrorismus und Krieg? Da es im Vergleich zu früheren Zeiten keine große Kriegsindustrie, komplizierte Kommandostrukturen oder stehende Heere braucht, können bereits kleine Gruppen von Cyberangreifern enorme Schäden herbeiführen. Wenn Staaten private Personen und Unternehmen anheuern, um Angriffe auszuführen, ist das dann eine Kriegshandlung?

Im analogen Bereich gab und gibt es viele Beispiele von Kaperei, Terrorfinanzierung durch Staaten und weiteren indirekten schädigenden Handlungen, die nicht als Kriegshandlung klassifiziert wurden. Es war außerdem relativ einfach, in der analogen Welt Kriegswaffen zu identifizieren, nachzuverfolgen und Abrüstung zu organisieren. Auch konnte man physisch sehen, was zerstört wurde und eine Ahnung davon bekommen, was in industriellen Großanlagen produziert wird. All das wird im Internet ungleich schwieriger. Es gibt für Digitalwaffen keine Fabriken, die sich von normalen Büros unterscheiden. Für den Cyberraum muss die klassische Staatsdefinition von Jellinek dringend überarbeitet werden. Obwohl es sich für uns heute so anfühlt, als wären Staaten „schon immer da gewesen“, sind sie menschheitsgeschichtlich doch eine recht späte Innovation. Wir sind es gewohnt, in staatlichen Systemen zu denken, aber vielleicht stehen wir heute an einem Punkt, an dem diese Vorstellung überkommen ist und wir soziale Organisation neu denken müssen. Überall, wo wir mit der digitalen Transformation in Berührung kommen, spüren wir, dass

etwas mit der gewohnten alten Sichtweise nicht stimmt und diese sich noch vollkommen unverstanden verändert. Die ehemals in staatlicher Hand liegenden Informationssysteme werden heute von wenigen privaten Unternehmen entwickelt, betrieben und gehen weit über den Wirkkreis von Staaten hinaus. Dazu kommt noch, dass es sich dabei um ganz junge Unternehmen handelt, die vor 30 Jahren noch nicht gegründet waren.

Pax Cyber: Völkerrecht im digitalen Zeitalter

Es ist gewiss eine ungewohnte und beunruhigende Vorstellung, dass die staatliche Macht im Zuge der Digitalisierung erodiert und schwindet. Kein Staat kann heute ohne das Know-how der großen Digitalunternehmen seine Bürger schützen. Diese global betriebenen privaten Plattformen übernehmen Aufgaben, die vormals ausschließlich Staaten vorbehalten waren. So verlassen sich Nutzer digitaler Plattformen schon lange nicht mehr darauf, von der Polizei oder anderen Behörden im digitalen Raum geschützt zu werden, sondern vertrauen die Sicherheit ihrer Daten mehr und mehr Plattformunternehmen an. Sie können daher in den Fragen der Herstellung von internationaler Sicherheit und internationalem Recht nicht mehr ausgeklammert werden.

Private Plattformunternehmen agieren wie Staaten

Diese Überlegungen werfen Fragen nach notwendigen Regulierungen der Plattformmärkte auf. Wie kann das Völkerrecht im digitalen Raum – eine „Pax Cyber“ – gestaltet werden, ohne dabei zu wissen, was uns die neue Welt alles bringen wird? Fest steht jedenfalls, dass nationale Ansätze zu kurz greifen und dass Staaten nicht mehr die einzigen Player sind, wenn es um Sicherheit und Frieden, den technologischen und gesellschaftlichen Fortschritt sowie um die Wohlstandsmehrung geht. Auch wenn der Gedanke heute noch sehr fremd ist, Privatunternehmen als Akteure im Völkerrecht mitzudenken, wird man überstaatliche Vereinbarungen bis hin zur Verhinderung aggressiver Auseinandersetzungen ohne private Player als Technologiespezialisten wohl nicht erreichen können. Große Plattformunternehmen fungieren zunehmend als suprastaatliche und machtvolle Institutionen, die im Internationalen Recht, sofern sich dieses auf den Cyberraum erweitert, als souveräne Akteure begriffen werden müssen. Da Konflikte immer mehr digitale Aspekte beinhalten, werden Staaten bei Auseinandersetzungen, Friedensregelungen und der Setzung internationaler Standards Unternehmen am Tisch akzeptieren müssen. Nur – „Völkerrecht“ wird man ein solches Arrangement dann nicht mehr nennen können. Wie dann?

Dr. Maxim Asjoma ist Referent der Geschäftsleitung des Hasso-Plattner-Instituts für Digital Engineering (HPI) an der Universität Potsdam.

Prof. Dr. Christoph Meinel ist Direktor und Geschäftsführer des HPI und Dekan der Digital Engineering Fakultät der Universität Potsdam.