UNhörbar/UNrecht #18 Kann die UN Cyber? Über die Schattenseiten der Digitalisierung

2021, May 14

Vanessa Vohs

Herzlich Willkommen zu unserer Gemeinschaftsfolge von UNrecht und …

Franziska Sandt

UNhörbar.

Vanessa

Denn heute ist unser Thema ein sehr interdisziplinäres, wofür wir sowohl politischen, gesellschaftlichen als auch rechtlichen Perspektiven eine Stimme geben möchten. Denn wir sprechen heute über das Internet und die Regulierung dessen. Warum machen wir das ganze heute? Weil es mittlerweile vier Milliarden Internetnutzer gibt, gleichzeitig aber drei Milliarden, die keinen Zugang zum Internet haben. Daher ist natürlich das Thema „Zugang zum Internet - Entwicklung“ ein wichtiges Thema, welches Nachhaltigkeit betrifft und die Digitalisierung im Allgemeinen. Daher wollen wir heute fragen: Kann die UNO Cyber?

Dazu sprechen wir in zwei Teilen heute über das Thema und zwar gucken wir uns im ersten Teil an, was denn Gefahren im Cyberspace sind und gehen dann weiter und fragen, was man dagegen tun kann.

Franziska

Ja, und ohne nun groß vorweg greifen zu wollen. Ihr steht ja nun beide mit sehr kessen Füßen im Thema, unsere beiden Gäste heute, Matthias Kettemann und Matthias Schulze. Und ja, Matthias Kettemann, du vertrittst nicht nur gerade in Jena den Lehrstuhl für International Law, sondern du bist auch Forschungsprogrammleiter, bspw. am Leibniz-Institut für Medienforschung. Und ich glaube, jetzt wäre der Moment, wo du dich den Zuhörern einfach mal ein bisschen selbst vorstellst.

Dr. Matthias Kettemann

Hallo, mein Name ist Matthias Kettemann und ich forsche an verschiedenen Institutionen über Recht und Regeln im Internet und schaue mir dabei an, wie wir das Internet zu einem faireren, besseren Ort machen können.

Franziska

Und unser zweiter Gast, Matthias Schulze. Du bist stellvertretender Forschungsgruppenleiter der SFB-Forschungsgruppe für Sicherheitspolitik und hast auch deinen eigenen Cyber-Podcast. Erzähl doch mal!

Dr. Matthias Schulze

Jo, hallo. Danke für die Einladung! Ja, ich bin bei der Stiftung „Wissenschaft und Politik“ in der Forschungsgruppe „Sicherheitspolitik“ angestellt und beschäftige mich mit der „dunklen Seite“ der Digitalisierung, bei der SWP, aber auch auf meinem Blog und meinem Podcast www.percepticon.de – Ende des Werbeblock. Wer da vorbeischauen will, kann das gerne mal tun.

Franziska

Ja, klasse, danke schön euch beiden. Also zunächst und zum Einstieg, wir sitzen ja nicht nur bei UNrecht, sondern auch in einer „Bar“, der UNhör-bar, und in einer Bar gibt es ja auch Trinksprüche. Und deshalb, liebe Zuhörer, wird es jetzt eine kurze „Entweder-oder-Fragerunde“ geben.

Ich werden jetzt also unseren beiden Gästen drei Paare nennen, drei Begriffspaare, und sie müssen sich ganz schnell für eins von beiden entscheiden. Also sowas wie Vanille oder Schokolade.

Sinn des Spiels ist dabei maßlose Verwirrung bei allen, aber ich glaube, das wird auf jeden Fall ein lustiger Einstieg.

Also fangen wir an: Iron Man oder Capt’n America?

Matthias K.

Iron Man

Matthias S.

Oh Gott, Iron Man, war mir sympathischer.

Franziska

Gedankenlesen oder Unsichtbar machen?

Matthias K.

Gedankenlesen

Matthias S.

Gedankenlesen

Franziska

Und – Startrek oder Starwars?

Matthias K.

Ich muss Startrek sagen, das geht nicht anders.

Matthias S.

Startrek.

(Lachen)

Franziska

Ja, das war sehr aufschlussreich, würde ich sagen. Wir wissen jetzt auf jeden Fall mehr über euch. Und was wir auch wissen, dass Ihr Internet-Mythen entzaubert habt, und zwar war ich heute zur Vorbereitung auf den Podcast im virtuellen Raum unterwegs und hab ein bisschen recherchiert zu euch und hab herausgefunden, dass ihr, ja, Entzauberer seid und Internetmythen entzaubert habt. Und da haben wir uns natürlich gedacht, wollen wir gleich mal nachhaken, zu Internet-Mythen, und Mythos eins wäre: In dem Internet gilt kein Völkerrecht. Es existiert also kein internationaler Vertrag oder internationale Verträge hinsichtlich des Internets, und damit können Staaten online tun und lassen, was sie wollen, und es gibt dementsprechend auch kein Völkerrecht. Stimmt das, Matthias Kettemann?

Matthias K.

Nein, das stimmt zum Glück nicht. Was stimmt, ist, dass es keinen Internetvertrag gibt. Es gibt also keine Konventionen zum Schutze des Internet. Aber das Völkerrecht gilt dennoch online, darauf haben sich die Staaten schon lange verständigt. Völkervertragsrecht, Völkergewohnheitsrecht, die allgemeinen Rechtsprinzipien – das alles gilt online. Das Internet ist kein rechtsfreier Raum, weder für einzelne, noch für Staaten.

Franziska

Super. Und Mythos 2, den werfe ich jetzt einfach ungeschönt mit in den Raum. Zur dunklen Seite der Macht sozusagen. Der Cyberkrieg kommt, Matthias Schulze. Kurze Erklärung: Moderne Volkswirtschaften sind ja von der digitalen Welt abhängig. Ein strategischer Cyberangriff kann damit auch eine kritische Infrastruktur, z.B. Stromversorgung, weitreichende Folgen haben und Opfer fordern. Siehst du denn die Gefahr auch in naher Zukunft? Würdest du sagen, der Cyberkrieg kommt, und zwar demnächst.

Matthias S.

Ja, die Möglichkeit existiert, aber das Argument, was ich in dem Beitrag mache, ist, dass die Wahrscheinlichkeit dafür sehr gering ist. Also die Möglichkeit, die Volkswirtschaft digital auszuschalten, geht, es ist superkomplex, es zu machen, aber wenn man genügend bösen Willen sozusagen und Geld voranbringen kann, wäre es theoretisch möglich.

Das ist aber eher unwahrscheinlich, dass das tatsächlich passiert, weil die Folgeeffekte kaum absehbar sind, und Kollateralschäden entstehen, weil, ich denke an sowas wie das Bankensystem, ja, wenn der Finanztransfer nicht mehr geht, dann hätte das womöglich auch Effekte für denjenigen und diejenigen, die das auslösen, also kurzum, die Möglichkeit besteht, dass so ein Krieg kommt, ein digitaler, die Wahrscheinlichkeit eines Stand-Alone-Cyberkriegs ist wahrscheinlich übertrieben.

Vanessa

Ja, vielen Dank, Matthias Schulze. Magst du vielleicht mal weitermachen? Du hast gesagt, du beschäftigst dich mit der dunklen Seite der Macht und der dunklen Seite der Digitalisierung hier. Warum ist also Internetregulierung wichtig?

Matthias S.

Jetzt muss ich so ein bisschen Matthias Kettemann wiedersprechen. Denn so ein bisschen „Wilder Westen“ ist natürlich doch noch, also so ein bisschen „lawless space“, obwohl natürlich Rechtsprinzipien wie das Völkerrecht gelten. Im Prinzip halten sich natürlich nicht alle dran. Das sieht man einfach daran, dass Quantität und Qualität von Cyber-Angriffen, die die Vertraulichkeit und Integrität von Datensystemen treffen, zunehmen, und das schon seit den 80er Jahren. Die Kurve zeigt permanent nach oben, in Quantitäts- und in Qualitätsdimensionen. Wir haben Spionage, wir haben Angriffe auf kritische Infrastrukturen, Stichwort Wanna-Cry vor einigen Jahren, oder auch Petya, die ja zum Teil sehr destruktive Effekte hatten, also sehr mit physischen Impacts, also zum Beispiel bei der Logistikfirma Maersk, die haben z.B. Container dadurch verloren. Weil einfach ihre Infrastruktur nicht mehr ging. Und der Schiffsverkehr lag dadurch zum Teil mal still. Das sind doch sehr reale Effekte, die da passieren. Und die Kosten für sowas steigen, also für die Behebung von sowas steigen. Also der Trend zeigt nach oben. Und dann haben wir ja auch noch das nette Thema „Beeinflussung von Gesellschaften über das Internet“, Desinformation, Influence Operation. Also, da ist schon noch so ein bisschen Wildwest, was das angeht.

Franziska

Und was ja auch tatsächlich Fakt ist, dass wir wenig Kontrollmechanismen haben. Also, es gibt keinen richtigen Rüstungskontrollvertrag, keine Begrenzungssysteme, kein inhaltlich umfassendes Regime irgendwie, Regelwerk zur Eindämmung von Risiken aus dem Cyberraum allgemein. Und wenn dann all diese Kontrollmechanismen fehlen – wo liegen denn dann die großen Gefahren im Cyberspace? Also vielleicht könnt ihr das einfach noch mal so zusammentragen, was wären so die großen Punkte, die ihr nennen würdet bei den Gefahren.

Matthias S.

Ich will einfach mal weitermachen. Also zentrales Problem und auch ein Risiko und auch eine Erklärung dafür, warum so ein Vertragswerk nicht gibt, ist, dass wir ja auch eine ganze Menge nicht-staatlicher Akteure haben, die in diesem Raum Schabernack treiben, also es sind ja nicht nur Staaten, die Cyberangriffe benutzen, um Macht auszuüben. Um dich zu Verhalten zu zwingen. Um Druck aufzubauen. Und es sind eben auch nicht-staatliche Akteure, die viel Gestaltungsmacht haben. Das sind zum einen die Unternehmen, die großen Internet-Unternehmen, denen ein Großteil der Infrastruktur gehört. Das Internet ist zu großen Teilen in privater Hand. Also die physische Infrastruktur genau wie die Netzwerkkabel, aber auch die Softwareebene, ja, denken wir an die großen Microsofts, Googles und Apples dieser Welt, das heißt, die haben da viel Gestaltungsmacht im defensiven, was Sicherheit angeht, und dann haben wir auch nicht-staatliche Akteure wie Cyberkriminelle, die für ein Großteil von Angriffen verantwortlich sind, und zwar niedrigschwellige Cyberkriminalität. Und oftmals ist es halt schwer nachzuweisen, wer der Urheber von sowas ist. Also zu eruieren, wer die Verantwortung trägt. Und dadurch ist es natürlich sehr schwierig, Menschen zur Rechenschaft zu ziehen und das macht diese ganzen legalen Prinzipien, die ja auch Nachverfolgbarkeit und Verfahren usw. nach sich ziehen, schwierig. Und dazu kommt eben, dass es eine ganze Menge Akteure gibt, die da mitwirken, und das ist ein ziemlich fragmentierter Raum, der zu regulieren ist, keine einheitlichen Ansätze, eben, weil es so kompliziert ist.

Matthias K.

Ja, auf verschiedenen Ebenen wird hier Recht geschaffen und durchgesetzt, also man sieht ganz neue Akteurskonstellationen drinnen. Das Problem, das wir haben mit der Zurechnung dieser Völkerrechtsprinzipien ist dergestalt gegeben, dass wir im Völkerrecht in der Regel in Zurechnung zu einem Staat brauchen, um erst die völkerrechtliche Verantwortung überhaupt konstruieren zu können. Das ist in der Regel sehr, sehr schwierig. Und Staaten werden ja auch immer cleverer, wenn sie Cybermittel einsetzen. Um Informationsoperationen durchzuführen, machen sie das in der Regel nicht selbst, sondern holen sich da Unterstützung, teils auf dem freien Markt, teils von Akteuren, die ideologisch eben hier aufgestellt sind. Aber da mal eine Verbindung herzustellen, die belastbar ist, ist gar nicht so einfach.

Vanessa

Ja, dann wissen wir schon mal, wo hier die großen Gefahren herkommen, aus eurer Perspektive. Aber dabei wollen wir natürlich nicht bleiben, sondern schauen, was man dagegen tun kann und wie man diese Gefahren minimieren kann. Um völkerrechtliche Zurechenbarkeit zu gewährleisten und die Angriffe im Allgemeinen vielleicht auch zu verändern.

Wollen wir vielleicht als erstes mal darüber sprechen, was denn jetzt die Vereinten Nationen machen. Also, kann die UNO Cyber?

Matthias S.

Also was wir sehen, ist, dass Staaten ja durchaus nutzen, um einander Schaden zuzufügen. Oder schädliche Effekte auszuführen. Also wir sehen einen veritablen Rüstungswettlauf, dass aufgerüstet, dass das Internet militarisiert wird, kann man auch sagen. Wir haben Kriminalität, und allerlei mehr Spionage. Und jetzt ist die Frage, wie kriegt man das eingeebnet. Dass das Thema ein Problem ist, haben die Vereinten Nationen schon relativ früh gemerkt. 1998 wird im Wesentlichen darüber gesprochen, dass man mal irgendwie eine Art Regelsystem bräuchte, um zunehmende schädliche Effekte einzudämmen, die durch Informationstechnologien entstehen. Also viel weitergedacht als nur Internet – Informations- und Kommunikationstechnologien kann ja auch sowas wie Smartphones und Mobilphones sein. Heute Internet of Things-Geräte. Das dauert aber in den diplomatischen Prozessen immer super-lange, deswegen ist das so ein Schritt-für-Schritt-Prozess, der dann eingesetzt ist. 2002 gab es dann die ersten Bemühungen vonseiten der Generalversammlung, eine sogenannte Governmental Group of Experts einzusetzen, die erstmal ein gemeinsames Verständnis der Bedrohungslage entwickeln sollen. Damals war noch nicht allen klar, was für Risiken existieren. Das Thema war auch noch relativ neu und dann natürlich auch perspektivisch Verhaltensstandards zu entwickeln. Vielleicht so der Kontext dazu: 2005 fing die UN an, darüber nachzudenken, 2007 gab es die ersten größeren Cyberangriffe, die tatsächlich Medienaufmerksamkeit generiert haben, 2007 in Estland, vermutlich russischen Ursprungs, wie gesagt, die Rekonstruktion ist immer ein bisschen schwierig, da gingen dann die Regierungswebsites ein paar Tage nicht, Bankenwebsites gingen down, Infrastruktur, Medien usw. wurden gestört, und das hat dann ziemlich großen Medienhass erzeugt. Und dann 2008 im Kontext des Georgien-Krieges haben diese Erfahrungen auch eine Rolle gespielt. Und das ist so ein bisschen der Hintergrund für diese UN-Prozesse, die dann gelaufen sind, zur Entwicklung von Normen, angemessenes Staatenverhalten. Und dann geht es auch um die Frage, gilt das Völkerrecht, wenn ja, wie gilt es, wenn nein, wann gilt es nicht, aber da kann Matthias Kettemann, glaube ich, viel mehr zu sagen.

Matthias K.

Zum Glück kamen diese Gremien sehr bald zum Schluss, dass in der Tat Völkerrecht gilt. Und das war gar kein geringer Schritt, nämlich, dass wir im Konsens der Staaten jetzt festgestellt haben, dass die UN-Charta in ihrer Gänze auch im Cyberspace anzuwenden ist. Vielleicht sind wir jetzt etwas spät damit, aber wir dürfen auch nicht vergessen, dass, wenn wir von Internet sprechen, wovon wir eigentlich sprechen, was ist eigentlich das Internet, auf dass das Völkerrecht anzuwenden ist. Das geht ganz in die Richtung der Frage, die sich die Staaten bei der UNO gestellt haben. Es geht ja um die Kernressourcen des Internets. Nicht so sehr darum, was Facebook und Google machen. Das sind auch wichtige Fragen, aber da hat das Völkerrecht nicht so viel zu sagen. Hier geht es um die großen Fragen, wie Staaten sich im Internet verhalten dürfen. Wie Staaten Informations- und Kommunikationstechnologien benutzen dürfen. Wie sie mit Unterwasserkabeln umgehen dürfen. Das sind auch Fragen, wo das Völkerrecht sehr relevant wird. Man darf nicht vergessen, einer der ersten völkerrechtlichen Organisationen war der Verein, der sich mit Telegrafenmasten auseinandergesetzt hat und in den ersten Verträgen standen Dinge drin, die uns heute sehr bekannt vorkommen, z.B. Mindestaufbewahrungsdauer für Depeschen. Klingt sehr nach einer Vorratsdatenspeicherung. Übrigens auch die Chefs der Telegraphenbüros, die hatten die Verpflichtung, Depeschen zurückzuweisen, die gegen die guten Sitten verstoßen haben. Also schon damals gab es eine Zensur. Nur damals wurde sie wirklich staatlich durchgesetzt. Der Konsensbericht 2015 war für diese Gruppen ein wichtiger Schritt. 2017 kam es dann zu einer Zerfaserung der Prozesse, auf Seiten der Vereinten Nationen. Schon im Wesentlichen deswegen, weil einige Staaten nicht glücklich waren mit der Idee, dass auf nur internetbasierte Angriffe kinetisch reagiert werden dürfte. Also die meinten, etwa Kuba oder Russland, es kann doch nicht sein, dass bei einem Online-Only-Angriff, dass das gleichzuhalten ist

mit einem bewaffneten Angriff, im Sinne der UN-Charta, die dann natürlich ausgelöst hätte bestimmte völkerrechtliche Verteidigungsrechte und -pflichten. Das war eher die Sicht der Vereinigten Staaten. Deswegen ist der Prozess in zwei Komitees aufgeteilt worden, langsam aber sehen wir hier eine Wiedereingliederung, es gibt zwar immer noch die Open-Ended-Working-Group auf der einen Seite, und die Group of Experimental Experts auf der anderen Seite, aber wir sehen hier gewisse Tendenzen, dass hier diese sich in ähnliche Richtungen entwickeln und vor allem konstruktive Outputs erzielen. Jetzt im März gab es ja den neuen Bericht der Open-Ended-Working-Group, da ist Deutschland auch stark beteiligt. Und in diesem Bericht wurde festgehalten, was wir ohnehin schon wussten, man kann das gar nicht oft genug hören und sagen: Ja, das internationale Recht findet auch im Cyberspace Anwendung. Wichtiger aber für mich war, dass in dem Begriff noch mal betont wurde, dass es mit dem Völkerrecht alleine getan ist und dass sich auch weitere Pflichten ergeben, wie etwa Kooperationspflichten der Staaten und auch Regeln für gutes Staatenverhalten.

Vanessa

Jetzt hast du ja schon häufiger erwähnt, Matthias Kettemann, dass das Völkerrecht Anwendung findet. Welche Prinzipien finden denn Anwendung, auf die wir uns vielleicht berufen können, vielleicht einfach aus dem allgemeinen Völkerrecht, der UN-Charta selbst vielleicht? Wir haben im UNRecht-Podcast in der Folge zum Gewaltverbot, in Folge 3, ein bisschen darüber gesprochen, wie das denn aussieht mit einem bewaffneten Angriff, der durch einen Cyberangriff ausgeführt wird, ob der auch als bewaffneter Angriff eben zählen kann oder nicht? Kannst du uns da ein bisschen mehr einführen?

Matthias K.

Das Talinn-Manual, das ist ein wichtiges Dokument, das im Nato-Kontext entstanden ist, fasst hier einige wichtige Regeln zusammen. Da wird relativ klargestellt, dass ein Internet-basierter Angriff dann gegen das Gewaltverbot verstoßen kann, wenn er bestimmte kinetische Folgen hat, wenn er also über wirklich rein internetbezogene Schäden hinweggeht. Das klassische Beispiel ist etwa ein Angriff über das Internet auf die Steuerungssoftware eines Atomkraftwerkes oder eines Dammes. Solange das wirklich nur, in Anführungszeichen „nur“, die Steuerungssoftware betrifft und nichts anderes passiert, wird das wohl noch nicht eine „Gewaltausübung“ im völkerrechtlichen Sinne sein. Hingegen muss man schon eine echte kinetische Folge verlangen, das Manual spricht da von einem „large loss of life“ oder „large loss of property”.

Matthias S.

Das ist wichtig zu nennen, weil das ist eben nicht nur eine hypothetische Möglichkeit, sondern es ist 2010/2011 tatsächlich passiert, mit dem sogenannten stuxnet, dem Computerwurm, der die iranischen Atomanreicherungstanks physisch sabotiert hat, also das ist eine Schadsoftware, die ist über nachrichtendienstliche Wege, vermutlich auf einem USB-Stick, in diese Hochsicherheitszone dieses iranischen Atomprogramms geschleust worden, basierte auf einer Siemens-Schwachstelle, in einem Siemens-Industrie-Steuerungssystem, also quasi indirekt deutsche Beteiligung mit dabei. Hat den Controller sabotiert, so dass diese Zentrifugen durchgedreht sind und physisch quasi zerstört oder beschädigt wurden. Und das war sozusagen vermutlich israelisch-amerikanischen Ursprungs, um das iranische Atomprogramm zu entschleunigen oder zu sabotieren oder die Entwicklung zu behindern und das war damals so wichtig oder hat so Eindruck hinterlassen, als das bekannt wurde, dass man gesagt hat, hier wurde jetzt der Rubikon überschritten, nämlich der Rubikon einer Schadsoftware, die in die physische Domain, in die materielle Wirklichkeit hineinreicht, und seitdem ist das im Prinzip nur mehr geworden, wir haben erst die Stromausfälle über Cyberangriffe gesehen, in der Ukraine, 2015, wir haben über Maersk / Petja gesprochen, also dass die Möglichkeit existiert. Also das Problem daran ist so ein bisschen, dass die USA seit 2015, glaube ich, und die Nato dann darauffolgend dann gesagt

haben, okay, wenn ein Cyberangriff diesen Schritt macht, nämlich in die physische Wirklichkeit hineinreicht, dann ist es ein bewaffneter Angriff und dann behalten wir uns auch vor, mit konventionellen Mitteln zu reagieren und die USA und neuerdings auch Großbritannien sehen sogar vor, nuklear zu reagieren. Also wenn ein Effekt so stark ist, dass das mit einem nuklearen Angriff vergleichbar ist, auch wenn das super-abstrakt ist, sich das vorzustellen, wie so was aussehen könnte, behalten sie sich vor, darauf zu reagieren, um ein Abschreckungsszenario aufzubauen. Also um andere Akteure davon abzuhalten, diese Schwelle zu erreichen. Ob das nun eine gute Idee ist oder ob das klappt, kann man sicher trefflich diskutieren.

Vanessa

Okay, das heißt also, das Gewaltverbot kann uns in irgendeiner Weise helfen, wenn es um kinetische, physische Auswirkungen durch Cyberangriffe geht, aber es findet natürlich nicht in der Gänze Anwendung. Daher stellt sich für mich auch so die Frage, vielleicht auch an den Völkerrechtler, Matthias Kettemann: Glaubst du, dass die allgemeinen Prinzipien des Völkerrechts, dazu gehört auch die souveräne Gleichheit, das Prinzip der Streitbeilegung, glaubst du, das alles ist ausreichend, um den Cyberspace als solches zu regulieren, oder wärst du dafür, einen völkerrechtlichen spezifischen Vertrag zu entwickeln, in diesem Bereich?

Matthias K.

Ich bin immer ein Fan von mehr Verträgen, das bedeutet mehr Verträge für meine Kolleg:innen und mich, aber unabhängig von egoistischen Interessen – ich sehe das Völkerrecht in einem ziemlich guten Zustand, was das Internet betrifft. In der Tat, du hast das angesprochen, das Gewaltverbot ist ja nur der Vorschlaghammer des Völkerrechts, wir haben ja noch viele andere Regeln, die in nicht so schlimmen Fällen anzuwenden sind, vom Prinzip der Nichteinmischung, über die Souveränität, die gerade im Internet eine große Bedeutung ausfüllt, deswegen nämlich, weil die Souveränität so schnell verbunden war mit den Grenzen. Und das einfache war, staatlichen Einfluss dort enden zu lassen, wo die Grenzen sind, die Polizei kann nicht weiterfahren als bis zum Grenzbaum. Im Internet ist das ja anders. Im Internet kann man ja relativ schnell Grenzen überschreiten. Im Internet ist jeder ein Nachbar, sagt man. Das heißt, da ist das Nichteinmischungsprinzip immer wichtiger geworden, und Souveränität im Internet neu zu verstehen ist die große Herausforderung, an der sehr viele junge Völkerrechtler:innen sitzen. Ich weiß von drei, vier Dissertationen, die sich allein dieser Frage widmen. Wie das Völkerrecht Souveränität im Internetzeitalter neu verstehen muss. Wie der Staat sich neu finden muss. Und diese Störgebilde, die wir gerade jetzt haben, etwa auch im Bereich der Plattform-Regulierung, die fußen auf diesem Problem, dass der Staat noch nicht in der Jetzt-Zeit angekommen ist. Wir haben Konstrukte aus dem vergangenen Jahrhundert oder, je nach dem, wie lange man zurückgehen möchte, aus dem 17. Jahrhundert. Und das heutige dynamische Verständnis von Gewaltausübung und Legitimierung muss erst für das Internet neu konzipiert werden.

Matthias S.

Genau, die zentrale Herausforderung dabei ist eben, dass Teile des Internets – man spricht immer von drei Schichten oder drei Ebenen – man kann auch vier sagen, nämlich die Hardware-Layer, das ist die der Kabel und der Router und der Server – und die Software-Layer, das ist die Ebene der Protokolle, die den Datentransfer regulieren, das ist aber auch die Ebene der Applikation, der Software, von Apps und Betriebssystemen und so weiter, und dann die Content-Layer, so dass was sozusagen an Inhalten, an Information drinnen ist und in sozialen Medien, was gepostet wird und gesagt wird, die Rede und so weiter, dass die insbesondere die oberen beiden Layers natürlich superschwer zu regulieren sind, weil die natürlich auf einer internationalen bzw. distribuierten Logik basieren. So wie das Internet funktioniert, sprich, diese Informationen sind dezentralisiert verteilt, die sitzen nicht an einer Stelle,

notwendigerweise, sondern sind über die Knotenpunkte des Netzwerks verteilt und das macht dann eine nationale Jurisdiktion und Regulierung schwierig, weil die Informationen also im Wesentlichen überall sein können. Die Hardware wiederum, die ist natürlich in Ländern. Die ist unter nationaler Jurisdiktion, da können Staaten drauf zugreifen, und da ist die Lage ein bisschen anders. Aber alles, was so Inhalte angeht, also Inhaltsregulierung ist einer der großen Schwierigkeiten, mit der Staaten gerade zu kämpfen haben, auch wenn wir über Desinformationen und *Hate Speech* und Verschwörungstheorien und so weiter sprechen.

Matthias K.

Vielleicht auch noch zwei Punkte dazu. Das Völkerrecht ist ja ein breites Feld, ein schöner Wald mit vielen Gewächsen. Und gerade im Internet sehen wir, warum das so spannend ist. Wir sehen nämlich völkerrechtlich angehauchte, völkerrechtlich beeinflusste Normen von nicht-klassischen Völkerrechtsakteur:innen, z.B. hat vor einiger Zeit *Global Commission on the Stability of Cyberspace* getagt, die wichtige, systemisch legitimierte Akteure versammelt hat, also clevere Köpfe, und die haben ein Dokument erstellt, das haben sie „*Norm Package*" genannt, also ein Norm-Paket, aus Singapur, und da findet man dann Normen, die klassisch völkerrechtlich klingen, etwa eine Norm „*to avoid tampering*", also Staaten sollen sich verpflichten, etwa nicht „Hintertüren" in Produkte einzubauen oder eine Norm „*to avoid vulnerabilities*", also Staaten sollen sich darauf verpflichten, gemeinsam mit Entwickler:innen keine Vulnerabilitäten in Produkten zu verstecken und so sie diese finden, sofort sie bekannt zu machen und keine, wie das teilweise von Sicherheitsbehörden gemacht wird, aufzukaufen und dann zu nutzen. Das ist natürlich völkerrechtlich hochinteressant. Da gibt es allerdings noch keine entsprechende Praxis. Weil sich hier die Staaten noch zu wenig in die Karten schauen lassen wollen. Wir sehen also hier auf jeden Fall ein Aufbrechen auch der traditionellen völkerrechtlichen Akteur:innen, dass uns eine sehr spannende Zukunft verspricht.

Matthias S.

Vielleicht auch noch ergänzend dazu, dieser Beitritt von nicht-staatlichen Akteuren in diese Regulierungslandschaft, den sieht man ja auch an anderen Stellen. Es gibt da zum Beispiel so Akteure wie Microsoft, die dann so was sagen wie „wir brauchen eine digitale Genfer Konvention". Wo bestimmte Prinzipien drin sind wie, bestimmte Akteure einfach nicht anzugreifen. Dass man Sanitäter und Hilfspersonal in bewaffneten Konflikten nicht angreifen soll. Microsoft bezieht das dann auf die *Computer Emergency Response Teams* und andere. Das ist auch eine Norm, die wiederum im UN-Prozess aufgetaucht ist, nämlich dass die Hilfskräfte, die *Incident Responder*, bei einem Cyberangriff vor Ort sind und die Systeme warten und prüfen und wiederherstellen, dass die nicht zu einem Ziel von Cyberangriffen gemacht werden. Wir sehen das aber auch an anderen Initiativen, wie von Frankreich, den *Paris Call*, wo eine Initiative gestartet wurde, um das zu pushen. Wir haben auch in Deutschland mit Siemens mit der *Chart of Trust* ähnliches versucht. Und Microsoft hat auch noch so einen *Tech Accord* vorgeschlagen, also dass Unternehmen sich sozusagen verweigern, zu Handlangern von Staaten zu werden, was das Einbauen von Hintertüren in Software angeht. Was natürlich super-spannend ist, weil Hintertüren, also Hintertüren sind im wesentlichen absichtliche Schwachstellen, Software-Code von Systemen, und das ist gewissermaßen die Grundlage für Cyberangriffe, also man braucht eine Software-Schwachstelle, man braucht hierzu eine Schadstoffsoftware, die diese Schwachstelle ausnutzt. Und dann kann man mehr oder weniger unbemerkt in Systeme eindringen, insbesondere wenn man hochgradige Zero-Relais-Stellen verwendet, und wenn jetzt sozusagen Unternehmen sagen, nee, wir wollen uns da nicht zum Handlanger machen und absichtlich Hintertüren einbauen, dann hat das natürlich Signalwirkungen an Staaten, weil Staaten das wollen. Im Strafverfolgungsprozess, zum Beispiel. Auch auf EU-Ebene. Das sind nicht nur die autoritären Staaten, die dieses Verlangen haben. Vielleicht dazu noch kommentierend, eine der Tatsachen, die sich mir

aufdrängt, ist, ich bin fast schon sauer, wenn Leute mir sagen, im Internet gibt es kein Völkerrecht. Aufgrund der Vielfalt an Normen, die entstehen, die völkerrechtlichen Charakter haben. Und weil du diese „CERTs“ angesprochen hast, Matthias, diese *Computer Emergency Response Teams*, in den *Norms of Responsible States Behavior*, also in den Normen für das verantwortungsvolle Verhalten von Staaten, die eine der Ergebnisse der UNO-Komitees waren, der *Group of Governmental Experts*. Da steht zum Beispiel drinnen, dass verantwortungsvoll handelnde Staaten haben heutzutage *einfach Computer Emergency Response Teams.* Menschen, die man anrufen kann, die was tun, wenn man merkt, da kommt ein *botnet* aus Österreich. Und Staaten, die das nicht tun, die werden sich vorwerfen lassen müssen, wenn schon nicht jetzt, dann in sehr, sehr naher Zukunft, dass sie ihren völkerrechtlichen Pflichten nicht nachkommen. Denn das, was auf einem Territorium als Staat geschieht, dafür hast du die Verantwortung, und das wissen wir seit Fällen aus der Vorvergangenheit. Und so entsteht Völkerrecht heutzutage. Auf kreative, spannende, neue Art und Weise. Nicht auf Verträge warten. Schauen wir doch, was wirklich geschieht und was für neue normative, spannende Fälle hier aufmachen.

Franziska

Ja, ich denke, das ist ein richtig guter Moment, um den Staaten mal in die Karten zu schauen. Richten wir doch den Blick mal auf Deutschland. Was macht Deutschland eigentlich? Es gibt ja jetzt so ein ziemlich aktuelles Positionspapier, zur Anwendung des Völkerrechts im Cyberraum unserer Bundesregierung, vom März 2021, also brandaktuell. Frisch gedruckt und ich habe mir mal ein Zitat daraus geschrieben, und zwar, Deutschland ist überzeugt, dass das internationale Recht inkl. der UN-Charta und dem internationalen humanitären Völkerrecht ohne Einschränkung auch im Kontext des Cyberspace angewandt werden muss.“ Das ist ja generell keine neue Idee, wir hatten es gerade, ihr habt es gerade erwähnt oder angesprochen. Deutschland folgt dabei im Wesentlichen der Linie des Talinn-Manuals, aber die Bundesregierung plant eben laut eigener Aussage auch dieses Positionspapier auch auf internationaler Ebene zur Debatte zu stellen. Und wie würdest du denn diesen Vorstoß Deutschlands jetzt bewerten, Matthias Kettemann, also, ist es ambitioniert, oder ist es eher eine nette Verpackung, wie bewertest du das Engagement Deutschlands hinsichtlich Cybersicherheit, insbesondere in Bezug auf dieses Positionspapier?

Matthias K.

Deutschland setzt sich sehr konsequent für das Völkerrecht im Internet ein. Deutschland ist Mitglied von vielen internationalen Gruppen, die sich für Freiheit im Netz einsetzen, mit der Botschafterin Regine Grienberger haben wir auch eine Cyber-Botschafterin im Außenministerium, die sich sehr engagiert, die für internationale Kooperationen in den Bereichen und da auch in vielen, vielen Panels sitzt. Dieses Paper ist ein großer Wurf, ein wichtiger Wurf, auch wenn nicht alles davon neu ist. Klar, man hat vieles davon erwarten können, es findet sich aber auch wichtige Fortschreibungen des Talinn-Manuals. Und so wiederum entsteht ja auch Völkerrecht, eben ein Soft Law-Dokument, das beruht auf dem *Best of Knowledge* von Expertinnen und Experten, dann von staatlichen Akteuren kondensiert, aufgegriffen und als Staatenpraxis, oder zumindest als Opinio juris der Staatenpraxis wiedergegeben wird. Deswegen ist sowas sehr, sehr wichtig. Und es ist durchaus noch im Trend der Zeit. Inzwischen haben etwa 20 Staaten entsprechende Papiere veröffentlicht. Und da gibt es immer wieder auch spannende Sachen zu finden, z.B. England hat vor kurzem veröffentlicht ein Paper zur Geltung des Völkerrechts im Internet, zum Thema Souveränität und der Bedeutung der Souveränität, das eine durchaus überraschende Auslegung hat, der Deutschland ja nicht gefolgt ist. Deutschland hat hier Souveränität betont und gesagt, naja, die Souveränität kann in Gefahr gebracht werden, durch Aktivitäten über das Internet. Es dürfen aber nicht nur *negligible physical functions appearances se*in, das ist noch kein Verstoß gegen territoriale Souveränität, was auch wichtig ist, also es soll ja nicht jede

kleine Spam aus dem Ausland ist ja nicht gleich ein Angriff auf die territoriale Integrität, aber, die Stelle, die für mich am spannendsten war, ist die Verknüpfung von Souveränität und dem Schutz von Wahlen, des Wahlprozesses, gerade in den nächsten sechs Monaten, im Superwahljahr 2021, ist das wichtig. Und so schreibt das Außenministerium, dass *„Foreign Electrical Interference, means of malicious cyber attacks"* ist eine große Herausforderung. Und auch die Verbreitung von Desinformationen über das Internet kann, wenn es eine bestimmte Schwelle überschreitet, kann es sogar *coercion*, also ein Zwang sein, der dann gegen das Nicht-Einmischungsverbot verstößt. Das hat man so in der Form nicht in anderen Statements gelesen. Das finde ich schön, dass das so klargestellt wurde und so entwickelt sich auch Völkerrecht. Das ist schön.

Matthias S.

Wenn ich dazu noch ergänzen darf, weil, das Dokument hat natürlich noch eine weitere Funktion, nämlich die eigenen Rechtsansichten zu kommunizieren, und damit wirkt das Dokument auch als eine vertrauensbildende Maßnahme, also *confidence building measures* sind auch ein Aspekt neben dem Cybernormen, die dazu beitragen, sozusagen, dieses digitale Konfliktgeschehen zu regulieren. Das klassische Beispiel für so eine *Confidence Building Measure* ist das berühmte rote Telefon aus dem Kalten Krieg zwischen Washington und Moskau, und es gibt so eine ganze Reihe von *confidence building measures*, und eine davon ist erstmal, Begriffe zu definieren, wie versteht Deutschland bestimmte Dinge, was ist unter *Desinformation* gemeint, was ist ein Cyberangriff etc. pp., aber eben auch zu sagen, okay, was ist unsere Rechtsauffassung, wie könnten wir reagieren, wenn das und das passiert, und da ist dieses Dokument, glaube ich, ein Beitrag. Und diese *confidence building measures* werden in verschiedenen Regionalforen wie OSZE und ASEAN und so weiterentwickelt und sind ein weiterer Baustein in diesem Cyber-Regime-Komplex der Verregelung, den wir da schon versucht haben, zu skizzieren.

Franziska

Ja, dann wären wir, glaube ich, am abschließenden Punkt, was kann eigentlich jeder selber machen. Wir rufen ja gerade in der DGVN immer dazu auf, engagiert euch, ja, ihr beiden, was können wir denn selber tun, nicht unbedingt gegen das Risiko des großen Cyberwars an sich, wir sind ja jetzt nicht Captain America oder Ironmen, aber so im kleinen, also beispielsweise gegen Internetkriminalität, was kann jeder einzelne denn machen, um sich zu schützen.

Matthias K.

Oder wonder women, um ein bisschen equality of super heroes einzuführen. Ja, es gibt etwas, was Staaten machen können, und was Individuen machen können. Und das ist übrigens auch von der Expert Group und auch vom Norm Package empfohlen wird: *Cyber hygiene*, also Cyberhygiene. Das heißt, das klingt ein bisschen komisch gerade, in dem Corona-Kontext Hygiene. Ja, einfach sich clever verhalten, im Kleinen. Das beginnt ja beim Passwörterschutz, bei der Zwei-Faktor-Identifizierung zu haben, und es beginnt, und für Unternehmen bedeutet es auch, Mitarbeiter:innen entsprechend zu schulen, dass sie eben nicht hineinfallen auf E-Mails vom Chef oder der Chefin, der sagt plötzlich, auf gebrochenem Deutsch oder Englisch, du, ich brauch mal Geld, hol mir das aus dem Company Account.

Matthias S.

Was Staaten natürlich auch noch machen können, ist, diese digitale Hygiene zu stärken und das ist dann sozusagen Regierungsauftrag an die neue Bundesregierung, die dann irgendwann mal kommen wird, wir brauchen digitale Bildung an Schulen. Wir brauchen Programmierkenntnisse an Schulen, damit wir genügend Expert:innen in diesem Bereich haben, die auch dann wiederum rekrutiert werden können, die *Incident Response Teams* zu bestellen oder auch die Security an Unternehmen

hochzufahren. Daran mangelts oft, da haben wir Fachkräftemangel. Und wir brauchen natürlich auch *media literacy*, um Desinformation besser zu erkennen, wir brauchen sozusagen Digitalkompetenzen im Umgang mit dem Internet, von klein auf. Das ist natürlich Individualauftrag an alle Eltern, die da zuhören, aber besser wäre es, glaube ich, wenn es im schulischen Kontext stattfinden würde, neben den ganzen individuellen Maßnahmen wie „bitte benutzt sichere Passwörter", „nutzt die Passwörter nicht über verschiedene Accounts hinweg", „sichert eure wichtigen Accounts mit Zwei-Faktor-Identifizierung ab", und so weiter und sofort. Software-Updates installieren, nicht vergessen.

Matthias K.

Und da sich niemand 80 Passwörter merken kann, einen guten Passwort-Manager, da gibt es auch entsprechend gute, noch ein kleiner Hinweis, da ich selbst Elternteil bin, natürlich ist es wichtig, dass wir unsere Kinder erziehen, aber wir sehen es im Bereich Desinformation, es sind nicht so sehr die Kinder etwa, die viel Desinformation teilen. Es ist so die Generation 40+, das heißt lebenslanges Lernen ist ganz wichtig, Desinformation geht nur dann, wenn die Gesellschaft nicht resilient ist, wir brauchen also auch einen Resilienzaufbau für die Gesellschaft, wir brauchen aber auch, jenseits des Internets, eine Verpflichtung der Gesellschaft auf bestimmte gemeinsame Werte, auf Zusammenhalt, das ist etwas, was langfristig auch der Gesellschaft gut tut, da kann das Völkerrecht auch nur so weitgehen, da sind so einige interne gesellschaftliche Entwicklung ja auch wichtig.

Vanessa

Ja, vielen Dank an euch beide für diese schöne Zusammenfassung hier am Ende, nochmal, was jeder Einzelne von uns tun kann. Und damit sind wir auch schon so ziemlich am Ende unserer Folge angelangt. Und ich würde hier vielleicht gern noch mal so ein wenig zusammenfassen und euch am Ende noch mal eine kurze Frage stellen. Und zwar haben wir gesehen, ja es gibt eine dunkle Seite der Digitalisierung, nicht alles ist gut, nicht alles ist super und wir müssen regulieren, müssen Menschenrechte schützen, und das Völkerrecht findet eben Anwendung. Und, das haben wir gesehen, im Konsensbericht der *Group of Governmental Experts* auf UN-Ebene, auch Deutschland beschäftigt sich aktiv mit der Weiterentwicklung durch Völkerrecht, ein jüngst veröffentlichtes Arbeitspapier, und gerade, wie ihr schon gesagt habt, jedes Individuum kann was machen, indem wir unsere Passwörter ordentlich schützen, indem wir, ja, auch auf der Ebene von Bildung an unsere Kinder was weitergeben, aber natürlich auch uns selbst immer weiter damit beschäftigen. Und da der Titel dieser Folge ja war, „Kann die UNO Cyber?", vielleicht, auch hier eine kurze Ja/Nein-Frage: Kann die UNO Cyber?

Matthias S.

Ja, aber unbedingt.

Matthias K.

Ja- Nein, ich wollt gerade sagen, aber Cyber heißt ja steuern, also klar kann die UNO steuern, also: Ja.

Franziska

Ja, ihr beiden, herzlichen Dank, dass ihr unsere Gäste wart, und uns heute über Cybersicherheit und Cyberkriege informiert habt. Und mit uns gesprochen habt, darüber, was es denn für Bedrohungen gibt, und was man dagegen tun kann. Das war heute eine Kooperationsfolge von UNrecht mit Vanessa und UNhörbar mit mir, Franziska, und wir hoffen, ihr hattet alle viel Spaß und wir hören uns bald wieder. Also, auf Wiederhören.

Vanessa

Dankeschön

Matthias K.

Danke

Matthias S.

Gerne.

Matthias, das Schlusswort war super, ich hatte so ein bisschen Pipi in den Augen, das war so schön zusammengefasst.

Franziska

Ist die Aufnahme aus, ja…