Wer sieht jetzt fern?

Die Dienstälteste: Zum Tod von Ponkie

Sie verkörperte das Gegenteil der Schauwerte einer Branche, der sie jahrzehntelang die Leviten las: Hätte man sie in einem Film besetzt, wäre sie in einer Nebenrolle aufgetreten, mit wenig Text. Beinahe lautlos erschien sie bei ihren seltenen Besuchen in der Redaktion der Münchner „Abendzeitung“ , die dennoch zu einem Auftritt wurden, eben weil sie, Ponkie, sich die Ehre gab. Häufig im Lammfellmantel, immer mit großer Sonnenbrille, die als Distanzmittel interpretiert wurde. Sie sprach leise, war humorvoll auf eine spezifisch altmünchnerische Weise.

Dummheit konnte sie schwer ertragen, Zumutungen gar nicht. Vieles, was die Öffentlich-Rechtlichen ihrer Kundschaft vorsetzen zu dürfen glauben, brachte die Sozialliberale mit SPD-Parteibuch auf die Palme. Das war kein bildungsbürgerlicher Dünkel, denn gegen gut gemachte Unterhaltung hatte Ponkie nichts. Es war die Erfahrung, die sie als Kritikerin machen musste: Bis in die siebziger Jahre sei Fernsehen ganz in Ordnung gewesen, hat sie einmal befunden, danach gewannen „Unterhaltungsschrott“, Talk-Show-Wiederkäuen, Traumstadl und Musikantenschiffe überhand. Privatsender ließ sie meist links liegen.

Wenn sie zupackte, dann richtig. Bernd Eichinger hat gestanden, der schlimmste Moment seiner Karriere sei die Lektüre von Ponkies Verriss seines Films „Letzte Ausfahrt Brooklyn“ gewesen. Münchens Liebling Helmut Dietl musste damit leben, von Ponkie nicht habituell gelobt zu werden. Auch mit Weltstars nahm sie es jederzeit auf, wie ein Blick in ihre Besprechung vom Mel Gibsons „Die Passion Christi“ zeigt. Dem Regisseur hielt sie vor, er filme „mit dem Fanatismus eines katholischen Sektierers und den Schockmethoden der Splatter-Movies, sozusagen aus dem Gaffer-Auge: Zuschauen, wenn einer totgeschunden wird.“

Begonnen hat die am 16. April 1926 in München geborene Ilse Kümpfel – den Spitznamen Ponkie spendierten ihr Kommilitonen – bald nach Ende des Weltkriegs mit Glossen und Spielberichten in einer Tennis-Zeitschrift. Den Doppelnamen Kümpfel-Schliekmann behielt sie nach der Trennung vom Vater ihrer drei Kinder, die sie fortan allein erzog. Im Alter von dreißig Jahren

Ponkie (1926–2021) Foto Picture Alliance

begann sie als Filmkritikerin bei der „Abendzeitung“. Einige Jahre später nahm sie das neue Medium Fernsehen unter ihre kritische Lupe und ließ davon auch nicht ab, als sie 1990 in den Ruhestand wechselte.

Da war sie schon längst eine Institution, und das vor allem, weil sie nie den Gepflogenheiten vieler Kritiker anhing, mit Regisseuren und Schauspielern am Set, bei Homestorys oder auf Partys vertraulichen Umgang zu pflegen. Sie saß in ihrem Haus in Solln, trank Tee, schrieb Kritiken. In der Stadtgesellschaft war sie angesehen, aber selten zu sehen. Showmaster Thomas Gottschalk zollte ihr Anerkennung und Respekt, der frühere Oberbürgermeister Ude ließ sich zu Liebesbekundungen hinreißen. Zu alldem schwieg Ponkie beharrlich, ehren ließ sie sich, wenn’s gar nicht anders ging, mit dem Schwabinger Kunstpreis, dem Grimme- und dem Wilhelm-Hoegner-Preis, einem Ehrenpreis des Münchner Filmfests.

Sie selbst beschrieb sich als „Langsamdenkerin“. Das Ergebnis dieses Prozesses mündete in kurze Texte. Was auf dem Boulevard Pflicht ist, verwandelte sie pointenstark in eine Kür. Solange es ging, lieferte sie dreimal die Woche Fernsehkritiken, lange als Fax, später via Mail, immer auf Zeile. Redigiert wurde sie nicht mehr, ein Privileg für Deutschlands dienstälteste Fernsehkritikerin. Es bleibt die Erinnerung an eine Frau mit Haltung, an einen wachen Geist mit scharfem Urteilsvermögen, der es nicht nötig hatte, sich in den Vordergrund zu schieben. Am 30. Dezember ist Ponkie, wie jetzt bekannt wurde, im Kreis ihrer Familie in München gestorben. HANNES HINTERMEIER

Foto Getty

Der Digitalkrieg ist zu verhindern

2022 muss das Jahr sein, in dem das Internet eine Sicherheitsstruktur bekommt. Die Gefahr eines Cyberkriegs nimmt zu, die Kriminalität im Netz explodiert.

Von Wolfgang Kleinwächter

Am 1. Januar hat Deutschland den Vorsitz der G 7 übernommen. Neben Klimawandel und Corona-Krise soll Cybersicherheit ganz oben auf der Agenda stehen. Das ist sehr sinnvoll. Gerade die Pandemie hat gezeigt, wie sehr unsere Welt von einer sicheren digitalen Infrastruktur abhängt. Instabilität im Cyberspace ist für kommende Generationen nicht weniger bedrohlich als eine zerstörte Umwelt.

Kaum etwas hat sich in den letzten zwei Jahrzehnten mehr verändert als die Internetwelt. Aus einem Freiheits- und Wachstumsversprechen ist ein Risikofaktor geworden. Grenzenlose Kommunikation und endlose Innovation sind in den Schatten von digitalem Wettrüsten, Cyberspionage und Erpressungssoftware geraten. Im Internet scheint alles mit seinem Gegenteil schwanger zu gehen. Freiheit und Wohlstand für die einen, orwellsche Überwachung und Ausbeutung für die anderen. Das Internet räumt kreativen Entwicklern, innovativen Unternehmern und mündigen Bürgern die gleichen Chancen ein wie Hasspredigern, Pädophilen und Kriegstreibern. Und noch ist unklar, wer im Ringen zwischen „Gut“ und Böse“ die Oberhand gewinnt. Sollte ein „richtiger Krieg“ ausbrechen, sagte der amerikanische Präsident Joe Biden, begänne er wahrscheinlich mit einem Cyberangriff.

Insofern ist es mehr als gerechtfertigt, den Aufbau einer globalen Cybersicherheitsarchitektur zu einer Priorität der Diplomatie zu erklären. Die USA und China steuern auf einen kalten Cyberkrieg zu. Digitale Angriffe auf kritische Infrastrukturen häufen sich. Internetbasierte Drohnen, mit Gesichtserkennungssoftware programmiert, suchen sich zu tötende Ziele selbst. Was kann man tun?

Die gute Nachricht ist, dass Regierungen und nichtstaatliche Akteure bereits seit Jahren über Risiken und Nebenwirkungen des Informationszeitalters sprechen. 2005 fand in Tunis ein UN-Weltgipfel zur Informationsgesellschaft (WSIS) statt. Dort wurde eine „Agenda“ verabschiedet mit Leitlinien für eine auf den Menschen zentrierte friedliche und offene digitale Zukunft. Seither gibt es das Internet Governance Forum (IGF), den jährlichen „Digitalgipfel“ der UN. 2025 steht die nächste WSIS-Überprüfungskonferenz an. Und unter dem Dach der UN haben sich weitere Gremien gebildet, die sich mit Cybersicherheit, Digitalwirtschaft und Menschenrechten im virtuellen Raum auseinandersetzen. Die Welt weiß also Bescheid, welche Gefahren im Cyberspace lauern.

Die schlechte Nachricht ist, dass bislang so gut wie nichts Konkretes vereinbart worden ist. Allein drei UN-Gremien verhandeln über Sicherheit im Cyberspace. Aber in allen drei Gruppen sind die Kontroversen größer als der Wille, sich auf einen gemeinsamen Bauplan zu verständigen. Die erste Baustelle bearbeitet eine Gruppe mit dem Namen „Open Ended Working Group“ (OEWG). Die OEWG, an der alle 193 UN-Staaten beteiligt sind, soll bis 2025 klären, was völkerrechtsgemäßes Verhalten von Staaten im Cyberspace ist. Immerhin konnte man sich 2015 darauf einigen, dass das Völkerrecht auch für die digitale Welt gilt. Aber weiter ist man nicht gekommen. Wann ist ein „Cyberangriff“ eine Anwendung von Gewalt, die nach Artikel 2, Absatz 4 der UN-Charta völkerrechtswidrig ist und das Recht auf Selbstverteidigung auslöst? Ist ein „Hack Back“ gerechtfertigt? Kann man eine Cyberattacke auch asymmetrisch mit einem Bombenangriff beantworten? Das Problem ist, dass nicht nur umstritten ist, was genau ein Cyberangriff ist, in vielen Fällen lässt sich auch der Angreifer schwer ermitteln. Wenn eine Schadsoftware in einem Kraftwerk installiert ist und erst nach einem halben Jahr aktiviert wird, ist es für den angegriffenen Staat nicht einfach, hundertprozentig zu belegen, woher der Angriff kam.

In der Arbeitsgruppe geht es auch um die Rolle nichtstaatlicher Akteure und um vertrauens- und kapazitätsbildende Maßnahmen. Ideen, wie eine ständige Ansprechstelle für Krisensituationen zu schaffen oder eine engere Kooperation zwischen technischen Experten und Diplomaten zu organisieren, sind vernünftige Schritte. Die erste Sitzung der OEWG Anfang Dezember 2021 in New York fand in einer durchaus konstruktiven Atmosphäre statt. Aber noch weiß man nicht, was bei den Verhandlungen herauskommen soll: Ein Aktionsplan? Ein Verhaltenskodex? Ein Cybernichtangriffspakt?

Gemeinsam gegen Cyberkriminalität

Auf der zweiten Baustelle geht es um die Kriminalität im Cyberspace. Für das organisierte Verbrechen ist der virtuelle Raum mittlerweile profitabler als Drogen- oder Menschenhandel. Zwar gibt es seit 2001 eine Budapester Konvention gegen Cyberkriminalität. Dieser Vertrag wurde unter dem Dach des Europarates und dem Eindruck der Terroranschläge vom 11. September 2001 ausgearbeitet. Die westlichen Länder haben dafür geworben, die Budapester Konvention zu universalisieren, aber nur ein Drittel der 193 UN-Staaten hat sie unterzeichnet. Große Internetländer wie Indien, Brasilien und China waren an den Verhandlungen nicht beteiligt und unterstützten den russischen Vorschlag, eine neue UN-Konvention auszuarbeiten. Die Sorge der westlichen Staaten ist, dass neue Verhandlungen die bestehenden Regelungen aushöhlen und den Standard der Budapester Konvention absenken.

Streit wird vor allem erwartet, wenn es um die Kriminalisierung von Informationsinhalten geht. Wie sollen sich Demokratien und Autokratien darüber einigen, welche Meinungsäußerung im Internet erlaubt ist? Die neue UN-Konvention soll bis Ende 2023 fertig sein. Ein sportliches Ziel, das aber dennoch nicht ganz unrealistisch ist. Erstens lassen sich viele Passagen der Budapester Konvention einfach übernehmen. Und zweitens ist der Leidensdruck, den die globale Cybermafia mit der Erpressung von Krankenhäusern und öffentlichen Verwaltungen, mit Angriffen auf globale Lieferketten und kritische Infrastrukturen erzeugt, mittlerweile gleichmäßig über ideologische Grenzen hinaus verteilt. Wenn sich die Verhandler in der neuen Ad-hoc-Gruppe (AHC), die Mitte Januar erstmals in New York zusammentrifft, auf das Machbare konzentrieren, wären Fortschritte nicht unmöglich.

Bei der dritten Baustelle geht es um autonome Waffensysteme. Dort wird seit 2014 unter dem Dach der Konvention zu konventionellen Waffen in einer Expertengruppe unter dem Kürzel LAWS (Lethal Autonomous Weapon Systems) über Killerroboter und Drohnen verhandelt. UN-Generalsekretär António Guterres fordert seit Jahren ein Verbot autonomer Waffen. Aber eine sehr gemischte Gruppe von Staaten – Russland, China, USA, Israel, Türkei – hat bislang selbst ein Moratorium abgelehnt. Zwar ist man sich grundsätzlich einig, Entscheidungen über Leben oder Tod nicht einem Algorithmus zu überlassen. Aber schon bei der Definition, was ein autonomes Waffensystem ist, gehen die Meinungen auseinander. Und während das Filibustern in Genf weitergeht, wird der Einsatz bewaffneter Drohnen Praxis wie in Nagorny Karabach, im Jemen, in Libyen, im Nahen Osten. Das Problem ist kompliziert. Für atomare Sprengköpfe kann man Höchstgrenzen vereinbaren, was aber ist die Grenze für einen Algorithmus? Panzer und Flugzeuge lassen sich kontrollieren, wie aber verifiziert man Bits und Bytes?

Bei den autonomen Waffensystemen stoßen die traditionellen Abrüstungsverhandlungen an ihre Grenzen. Mehr denn je bedarf es des politischen Willens der handelnden Akteure und eines Mindestmaßes an Vertrauen. Das hängt nicht unwesentlich davon ab, inwieweit erkannt wird, wie ein Krieg mit digitalen Waffen ablaufen könnte. NATO-Generalsekretär Jens Stoltenberg hat an die Zeit vor dem Ersten Weltkrieg erinnert. Die Welt sei 1914 nicht nur in einen Weltkrieg „hineingeschlittert“, die politischen Führer jener Zeit hätten auch die Wirkungen der damals neuen Technologien – vom Bomber bis zu Giftgas – völlig unterschätzt. Der spätere Chemienobelpreisträger Fritz Haber, der an der Entwicklung von Chlorgas beteiligt war, überzeugte Politiker, dass der Einsatz dieser Waffe zu einem schnellen Ende des Krieges beitrage. Das Gegenteil war der Fall. Was passiert, wenn in einem heutigen Konflikt die Dose der Pandora autonomer Waffensysteme geöffnet wird?

Und dann gibt es noch eine vierte Baustelle: den Schutz des öffentlichen Kerns des Internets. Das Funktionieren der Internetinfrastruktur und die Verfügbarkeit der Ressourcen – Root-Server, Domainnamen, IP-Adressen, Internetprotokolle – ist von solch elementarer Bedeutung wie die Wasser- und Stromversorgung. Diese Ressourcen werden von verschiedenen technischen Organisationen – ICANN, IETF, RIRs – verwaltet. Nachdem 2016 die USA – noch unter der Obama-Administration – ihre historisch gewachsene Aufsicht über den A-Root-Server des Internets an ICANN übertragen hatten, wurde vor allem von China und Russland immer wieder angezweifelt, ob diese technische Community in der Lage ist, die technischen Ressourcen im Interesse der Weltgemeinschaft zu managen.

Wenn es eines Stresstests für die Belastbarkeit des Systems bedurft hätte, dann hat ihn die Corona-Pandemie erbracht. Seit dem Ausbruch des Virus ist es zu einem exorbitanten Anwachsen der Internetnutzung gekommen. Homeoffice, Zoom-Konferenzen, Onlineshopping haben die Nachfrage nach Domainnamen und IP-Adressen explodieren lassen. Wie sich gezeigt hat, war das System in der Lage, die Herausforderung zu bewältigen. Es gab keinen Mangel an IP-Adressen oder Domainnamen. Die Root- und Name-Server funktionierten. Würde man diese technischen Ressourcen in ein strategisches Machtspiel hineinziehen, wäre das mit erheblichen Risiken verbunden. So wie es keine chinesische oder amerikanische, sondern nur saubere oder verschmutzte Luft gibt, sind die technischen Internetressourcen politisch neutral. Würden sie zum Spielball der Politik, hätten alle den Schaden. Es war daher sehr vernünftig, dass sich unter der britischen G-7-Präsidentschaft die Digitalminister dazu bekannten, die technischen digitalen Standards in den Händen der technischen Community zu belassen. Die deutsche G-7-Präsidentschaft sollte daran festhalten.

Doppelstrategie für den Cyberspace

Für die neue Bundesregierung ergibt sich ein weites Betätigungsfeld. Die Welt braucht auch für den Cyberspace einen fairen Multilateralismus, der sich an den universellen Werten der Charta der Vereinten Nationen und der UN-Menschenrechtsdeklaration orientiert und eingebettet ist in eine enge Kooperation zwischen Regierungen, der Wirtschaft, der Zivilgesellschaft und der technischen Community. Viele Blicke sind jetzt auf Deutschland gerichtet. Das betrifft auch die Verhandlungen zu autonomen Waffensystemen. Im Januar 2020 hatte die grüne Bundestagsabgeordnete Katja Keul die damalige Bundesregierung kritisiert, sich nicht entschieden genug für einen völkerrechtliches Verbot dieser Waffen einzusetzen. Im Koalitionsvertrag der Ampelkoalition heißt es jetzt, dass die neue Bundesregierung frühzeitig Initiativen zur Rüstungskontrolle in den Bereichen Cyber und Künstliche Intelligenz ergreifen werde. Die deutsche Sektion der Nichtregierungsorganisation Stop Killer Robots hat dies als viel zu weich kritisiert. Noch hat sich auch die EU nicht positioniert. Katja Keul ist jetzt Staatssekretärin im Auswärtigen Amt, und Deutschland hat den G-7-Vorsitz.

Joseph Nye, Nestor der amerikanischen Politikwissenschaft, hat in „Foreign Affairs“ in einem Aufsatz namens „The End of Cyber-Anarchy“ daran erinnert, dass im Kalten Krieg temporäre Zuspitzungen von Krisen und stabilisierende Vertragsverhandlungen zwei Seiten einer Medaille waren. Konzeptionelle Gegensätze über die Zukunft der digitalen Welt sollten kein Hindernis sein für punktuelle Vereinbarung zur Stabilität im Cyberspace. Auch Wolfgang Ischinger, Ex-Chef der Münchner Sicherheitskonferenz, sieht in einer Reaktivierung der Grundsätze der KSZE-Schlussakte von 1975 und der Charta von Paris von 1992 eine sinnvolle Strategie, um den neuen Gefährdungen zu begegnen.

Der Vorschlag von UN-Generalsekretär Antonio Guterres, den für 2023 geplanten UN-Zukunftsgipfel zu nutzen, um einen „Global Digital Compact“ zu verabschieden, könnte ein wichtiger Baustein für eine neue Cybersicherheitsarchitektur werden. Die vom finnischen Präsidenten Sauli Niinistö ventilierte Idee, den 50. Jahrestag der Schlussakte von Helsinki im Jahr 2025 zu nutzen, um Sicherheit und Zusammenarbeit weltweit zu stärken, findet mehr und mehr Anhänger. Noch sind viele Konzepte unklar. Sicher aber dürfte sein, dass der Baumeister eines globalen Cybersicherheitsgebäudes ein guter Kandidat für einen Friedensnobelpreis wäre.

Wolfgang Kleinwächter ist emeritierter Professor für Internetpolitik und Regulierung an der Universität Aarhus und war ein Kommissar in der Global Commission on Stability in Cyberspace.

Russlands Drohung

DJV fordert Reaktion von Baerbock

Der Deutsche Journalisten-Verband (DJV) fordert die Bundesregierung auf, den russischen Botschafter wegen dessen Äußerungen zu deutschen Journalisten in Russland einzubestellen. Außenministerin Annalena Baerbock (Grüne) müsse klarstellen, dass Drohungen gegen deutsche Journalisten, die in Russland arbeiteten, nicht akzeptiert würden. Der DJV bezog sich auf Äußerungen des russischen Botschafters, Sergej Netschajew, der mit Blick auf die Einschränkungen für den russischen Staatssender RT in Deutschland angedeutet hatte, dass von einer Reaktion Russlands deutsche Journalisten in dem Land betroffen sein könnten. „Eine solche unverhohlene Drohung darf nicht unbeantwortet bleiben. Die Außenministerin muss endlich ein deutliches Zeichen in Richtung Russland senden“, forderte der DJV-Bundesvorsitzende Frank Überall. „Die Schikanen gegen die dort tätigen Kolleginnen und Kollegen nehmen immer mehr zu.“ Zuletzt hatte Russland ein Gesetz verabschiedet, das medizinische Zwangsuntersuchungen von Auslandskorrespondenten vorschreibt. RT DE, so der Name des deutschen Ablegers des russischen Staatssenders, war am 16. Dezember mit einem Live-Programm über Satellit und im Netz gestartet. Am 22. Dezember wurde die Übertragung per Satellit nach Intervention der Aufsichtsbehörden gestoppt. Wenige Stunden nach Sendestart hatte Youtube den neuen Kanal von RT DE blockiert. Über seine eigene Website ist der deutschsprachige Nachrichtenkanal weiter zu sehen. KNA/F.A.Z.

Hacker greifen Israel an

Seite der „Jerusalem Post“ gekapert

Proiranische Hacker haben am Montag die Website der israelischen Zeitung „Jerusalem Post“ sowie das Twitter-Konto von „Maariv“ vorübergehend lahmgelegt. Statt der Nachrichteninhalte war ein Modellbild des israelischen Atomreaktors in der Wüstenstadt Dimona zu sehen, das mit einer Rakete zur Explosion gebracht wird. Die Rakete wird von einer zur Faust geballten Hand aus einem Ring abgefeuert, wie ihn der vor genau zwei Jahren bei einem amerikanischen Drohnenangriff im Irak getötete iranische General Ghassem Soleimani trug. Daneben steht auf Englisch und Hebräisch: „Wir sind nah an euch dran, wo ihr nicht daran denkt.“ Inzwischen sind die Website der Zeitung und das „Maariv“-Konto wieder in ihrem normalen Zustand. Es sei unklar, ob die Hacker sich in Iran aufhielten oder aus einem anderen Land heraus agierten, schrieb die „Jerusalem Post“. Ebenfalls sei nicht deutlich, ob sie in staatlichem Auftrag unterwegs seien. Die Zeitung war schon in der Vergangenheit Ziel proiranischer Hacker gewesen. Im Mai 2020 war auf der Website ein Bild der brennenden Stadt Tel Aviv erschienen. Darauf war dargestellt, wie der damalige israelische Regierungschef Benjamin Netanjahu im Meer nach einem Rettungsring greift – mit der Überschrift „Seid bereit für eine Überraschung“. dpa/F.A.Z.

Förderung für die Zeitung?

BDZV-Chef Döpfner gibt sich optimistisch

Der Präsident des Verlegerverbands BDZV, Mathias Döpfner, ist zuversichtlich, dass sich die Verlage mit der neuen Bundesregierung auf eine Förderung der Zeitungszustellung einigen. Nach ersten Gesprächen sei er „optimistischer denn je“, schrieb Döpfner in einer Neujahrsbotschaft. Die Zeitungsverleger fordern seit Jahren eine staatliche Förderung der Zustellung. Damit sei eine Unterstützung der Verlage möglich, ohne direkt Journalismus zu finanzieren. Eine von der Großen Koalition geplante Presseförderung war im April 2021 wegen rechtlicher Bedenken gescheitert. Zuversichtlich äußerte sich Döpfner auch, im Disput über presseähnliche Onlineangebote der Öffentlich-Rechtlichen mit der ARD weiterzukommen. Zugleich erneuerte er seine Kritik am von der EU geplanten Digital Markets Act. Für alle „Gatekeeper“ müssten gesetzliche Verpflichtungen gelten, Marktteilnehmern einen diskriminierungsfreien Zugang zu ihren Diensten zu geben. F.A.Z.