Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

Krieg im Informationsraum

Bericht vom IMI-Kongress 2017

von IMI

Dass sich der jährliche Kongress der Informationsstelle Militarisierung (IMI e.V.) im November 2017 dem „Krieg im Informationsraum“ widmete, hatte verschiedene Gründe. Der augenfälligste Anlass dürfte die Aufstellung des Kommandos Cyber- und Informationsraum Mitte 2017 gewesen sein. Dem zugehörigen Organisationsbereich mit gut 13.000 Dienststellen steht ein eigener Inspekteur vor, womit er den Teilstreitkräften Heer, Marine und Luftwaffe nahezu gleichgestellt ist. Darüber hinaus zeigte sich auch in der praktischen Arbeit der IMI in den letzten Jahren verstärkt, dass gerade in der internationalen Politik und in Konflikten wie in der Ukraine und Syrien mit vielfältigen, oft manipulierten Nachrichten oder Informationen umzugehen ist. Spekulationen über die Urheber und Motive von Cyberattacken und Leaks sind Teil der Geopolitik und der verschärften Spannungen zwischen den USA und Russland geworden. Immer deutlicher zeigen sie ihr Potential, auch zu handfesten militärischen Konflikten zu eskalieren. Augenscheinlich wurden auch viele Menschen von diesen Themen angesprochen, in der Spitze fanden bis zu 140 Zuhörer*innen den Weg ins Tübinger Schlatterhaus.

Die Ausrufung des Informationskriegs...

Ein weiterer Anlass für die Themenwahl war ein wenig beachtetes Dokument, welches das Europäische Parlament (EP) im November 2016 verabschiedet hatte und das einleitend vorgestellt wurde. Darin wird die Behauptung aufgestellt, dass sowohl der Islamische Staat wie auch Russland einen „Informationskrieg“ gegen die Europäische Union führen würden und dass dieser Teil einer hybriden Kriegführung wäre, „die dazu dient, die politische, wirtschaftliche und soziale Lage von im Fokus stehenden Ländern zu destabilisieren, ohne ihnen formell den Krieg zu erklären.“ Das EP fordert mit Nachdruck auf, diesen „Informationskrieg“ anzuerkennen und Gegenmaßnahmen zu ergreifen. Diese reichen von der Finanzierung von Maßnahmen, um im russischen Informationsraum „unabhängige Medienunternehmen, Denkfabriken und nichtstaatliche Organisationen insbesondere in der Muttersprache der Zielgruppe“ zu unterstützen, bis hin zur verstärkten Mobilisierung der Geheimdienste und der Strafverfolgungsbehörden gegen die Quellen „europafeindliche[r] Propaganda“ innerhalb der EU. Sowohl bei der Beobachtung „feindliche[r] Informationsmaßnahmen“ und damit zusammenhängender Finanzströme, als auch bei der Erarbeitung von Fähigkeiten, diese zu unterbinden, sei eine enge und kontinuierliche Zusammenarbeit mit der NATO anzustreben.

Die drei anschließenden Vorträge griffen Beispiele bereits jetzt bestehender Schieflagen in der Berichterstattung durch klassische und „neue“ Medien auf. *Christopher Schwitanski* zeigte zunächst anhand einer Netzwerkanalyse von Uwe Krüger, dass führende Journalisten und Redakteure sog. Leitmedien, insbesondere der Süddeutschen Zeitung, der Welt, der Frankfurter Allgemeinen Zeitung und der Zeit eng mit NATO-eigenen oder Nato-nahen Thinktanks vernetzt sind und sich hieraus eine wohlwollende Berichterstattung zugunsten des transatlantischen Bündnisses teilweise erkläre. In der anschließenden Diskussion wurde ergänzt, dass sich viele Medienschaffende selbst als politische Akteure verstehen und dabei eher der Elite zugehörig fühlen und deren Standpunkte vertreten würden. Außerdem wurde darauf hingewiesen, dass viele Nachrichten nicht auf eigener Recherche vor Ort, sondern auf Meldungen einer sehr überschaubaren Zahl von Agenturen beruhe, was einer genaueren Betrachtung hinsichtlich dadurch entstehender Schieflagen wert wäre.

Joachim Guilliard verglich daraufhin die Berichterstattung über die Kämpfe um die Stadt Mossul einerseits und Aleppo andererseits. Obwohl die Stadt Mossul viel umfangreicher zerstört worden und bis heute ein Großteil der Flüchtlinge nicht zurückgekehrt sei, hätten zivile Opfer und sonstige Folgen der Luftangriffe in der Berichterstattung keine große Rolle gespielt. Die schrittweise Einnahme der Stadt durch Verbündete Deutschlands und der USA sei vielmehr mit Begriffen wie „Fortschritt“ oder „Erfolg“ konnotiert worden und Bilder siegreicher, vordringender Bodentruppen hätten dominiert. Ganz anders sei hingegen die kurz zuvor begonnene Rückeroberung Aleppos durch die syrische Armee und deren Verbündete dargestellt worden. Dass sich die Offensive nur auf den Ostteil der Stadt beschränkte, sei zum Beispiel häufig untergegangen. Im Mittelpunkt standen hier Berichte über zivile Opfer, häufig von Bildern unterfüttert, die von Organisationen wie den White Helmets geliefert wurden, die gemeinsame Sache mit den Islamisten machten. Diese radikal-islamistischen und tw. Al-Kaida-nahen Kräfte seien beispielsweise vom Spiegel als „Aleppos letzte Hoffnung“ bezeichnet worden.

Jacqueline Andres stellte anschließend eine Studie der NATO zu „sozialen Medien als Instrument der hybriden Kriegführung“ vor. Darin würden vorrangig Beispiele der Aktivitäten Russlands, seiner Verbündeten und des Islamischen Staates in sozialen Medien beschrieben. So sei es der Syrian Electronic Army gelungen, in den Twitter-Account der Associated Press einzudringen und dort eine Meldung zu veröffentlichen, nach der US-Präsident Obama bei zwei Explosionen im Weißen Haus verletzt worden sei. Obwohl die Falschmeldung schnell entlarvt wurde, gab es an der US-Börse daraufhin einen rapiden Kursverfall und Milliarden Verluste. Über vergleichbare eigene Maßnahmen berichte die NATO deutlich weniger, allerdings enthalte die Studie Angaben, die NATO habe soziale Medien auch als Quelle für die Zielortung genutzt, so seien etwa im Libyenkrieg Informationen über Truppenbewegungen von vor Ort an die NATO übermittelt worden. Abschließend wurde anhand der zwei aus verschiedenen Kontexten entstandenen Kampagnen zivilgesellschaftlicher Gruppen, „Kony 2012“ und „#BringBackOurGirls“ beschrieben, wie – vermeintlich für die Betroffenen vor Ort sprechend – Zustimmung für die umfangreiche Stationierung US-amerikanischer Truppen auf dem afrikanischen Kontinent generiert wurde.

...die Geheimdienste...

Claudia Haydt sprach anschließend über Leaks und Whistelblowing als Instrumente der Geopolitik und beschrieb zunächst die Schwierigkeit, hier auf der Grundlage gesicherter Fakten zu sprechen. Sowohl Quelle, Echtheit des Materi-

als, Wahrheitsgehalt und tatsächliche Zielgruppe seien meist unklar. Sie nannte deshalb v.a. Beispiele aus Südkorea, wo die Einflussnahme der Geheimdienste auf innenpolitische Auseinandersetzungen mittlerweile gut aufgearbeitet sei. Diese hätten im Wahlkampf 2012 mit gefälschten Leaks über Twitter und Facebook den Gegnern der konservativen Präsidentin Park die Zusammenarbeit mit Nordkorea vorgeworfen. Aufgedeckt wurde dieser Skandal u.a. von einer kleinen linken Partei, der UPP. Dieser sei daraufhin ihrerseits eine „Verschwörung zum gewalttätigen Angriff auf den südkoreanischen Staat“ vorgeworfen worden, der mit vermeintlichen Leaks untermauert worden sei. Es folgten ein Parteienverbot und die Inhaftierung führender Mitglieder. Auf der anderen Seite seien Informationen über den Ausbau einer US-Basis in Südkorea über eine US-amerikanische Plattform veröffentlicht worden, was zu massiven Protesten führte. In die internationale Öffentlichkeit hätten diese Auseinandersetzungen es kaum geschafft, dafür habe sich diese zugleich intensiv mit dem sog. Sony-Hack beschäftigt, bei dem angeblich die Produktionsfirma eines Films in den USA gehackt wurde, der den nordkoreanischen Machthaber lächerlich machte. Haydt stellte anhand dieses Beispiels die Frage, ob man nicht viele Themen und Nachrichten auch als (bewusst oder unbewusst erzeugtes) „Rauschen“ verstehen müsste, in dem relevantere Nachrichten, wie der Konflikt um den Ausbau von US-Militärbasen in Südkorea, untergehen.

Anschließend stellte *Moritz Tremmel* verschieden Aktivitäten der westlichen Geheimdienste v.a. auf der Grundlage der Snowden-Leaks vor. Einerseits gäbe es bei westlichen Geheimdiensten die Mentalität „alles zu sammeln“, also sämtliche Kommunikation zu verfolgen und möglichst lange zu speichern. Hierzu würden einerseits Kommunikationsdienstleister wie Microsoft, Google, Yahoo etc. zur Offenlegung der Daten ihrer Nutzer*innen angehalten bzw. gezwungen. Andererseits würden zentrale Knotenpunkte weltweiter Kommunikation, wie etwa in Frankfurt, abgehört. Da es vielen Geheimdiensten untersagt sei, Daten über die „eigenen“ Bürger*innen selbst zu sammeln, würden diese Daten meist über die Kooperation der Dienste gewonnen und gegenseitig ergänzt. Selbst wenn diese Überwachung meist auf die Metadaten (Absender, Adressat, Zeit, Dauer, usw.) fokussiert und nicht die Inhalte der Kommunikation umfasst, sei dies nicht zu unterschätzen, da Metadaten viel besser automatisiert auszuwerten seien und auch diese zumindest in einigen Teilen der Welt Grundlage für Tötungsentscheidungen werden könnten. Neben dieser anlass- und verdachtsunabhängigen Massenüberwachung existiere noch das gezielte Hacking, bei dem sich Geheimdienste Sicherheitslücken zunutze machen, um in die Systeme von Gegner*innen einzudringen und dort u.a. nach belastendem oder diskreditierendem Material zu suchen. Während man sich gegen die Massenüberwachung mit Verschlüsselung recht einfach zur Wehr setzen könnte, erfordere das gezielte Hakking einen äußerst professionellen Umgang mit IT-Systemen und sei nie vollständig auszuschließen.

… und der NATO.

Ein weiterer Programmpunkt setzte sich mit der Perspektive der NATO auf den Informationsraum auseinander. Hierzu wurde von *Sven Wachowiak* einführend ein Strategiedokument aus dem Jahr 2007 vorgestellt, in dem führende Militärs im Bündnis bereits davor gewarnt hatten, dass die Mitgliedsstaaten die Kontrolle der Informationsflüsse und die Hoheit bei der Gestaltung der öffentlichen Meinung zu verlieren drohten. Durch eine eigene Informationsstrategie bzw. Informationsoperationen sei es nötig, „das Ruder wieder zu übernehmen“, um der Weltöffentlichkeit klar zu machen, dass es sich bei der NATO um „eine Macht des Guten“ handele, für die es zentral sei, nach einem Ereignis „auf den Bildschirmen präsent zu sein, bevor es der Gegner ist“.

Hieran knüpfte *Jürgen Wagner* mit Strategiedokumenten jüngeren Datums an, in denen ganz klar von „Informationen als Waffe“ die Rede ist. So habe eine eigene Konferenz stattgefunden, wie mit „Informationskampagnen“ gegen Luftkriegführung umzugehen sei. Als wichtiger Akteur werde dabei eine sog. „Lawfare-Bewegung“ ausgemacht, die den Einsatz bestimmter Waffen verbieten will und angeblich von Russland unterstützt werde, weil dieses die Überlegenheit der NATO-Luftwaffen fürchte. Auch terroristische Gruppen versuchten, Luftangriffe zu verunglimpfen, indem sie behaupteten, dass Luftangriffe viele Zivilisten töten würden. Als dritter Akteur wurden NGOs ausgemacht, von denen einige dazu tendierten, „jeglichen Einsatz von Gewalt negativ darzustellen“. Diese Konstellation sei kürzlich auch bei einer gemeinsamen Übung von EU und NATO mit dem Kürzel PACE durchgespielt worden, bei der simuliert wurde, dass die zunehmende Präsenz der jeweiligen Seestreitkräfte im Mittelmeer wachsender Kritik und Cyberangriffen ausgesetzt wären. Akteure waren hier eine an Russland angelehnte Nation namens Froterre, ein terroristischer Pseudostaat namens NEXTA und die von Froterre unterstützte Antiglobalisierungsgruppe AGG, die auf sozialen Medien gegen die NATO gehetzt und regelmäßig „Krawalle im Gewand von Demonstrationen“ vorbereitet habe. Über die Gegenmaßnahmen von NATO und EU gebe das entsprechende Szenario wenig Aufschluss, nach Angaben der Bundesregierung seien jedoch einzelne Informationsmaßnahmen der Gegner als Bündnisfall nach Artikel fünf des NATO-Vertrages behandelt worden.

(Un-)Sagbarkeit von Widersprüchen

Den Samstag beendete der Bildende Künstler *Franz Wanner* mit einem videografischen Vortrag, der Ausschnitte seiner Filme einbezog. Wanner hatte sich mit mehreren Rüstungsunternehmen und militärischen Forschungseinrichtungen auseinandergesetzt und war nach eigenen Angaben dabei

sehr schnell „an Grenzen gestoßen“, solange er sich „an herkömmliche Quellen gehalten“ hatte. Am Beispiel des Ludwig Bölkow Campus in Ottobrunn bei München zeigte er, wie die nationalsozialistische Geschichte und der militärische Charakter des Ortes verschleiert werden. Während der Campus öffentlich damit werbe, Studiengänge für „grüne Luftfahrt“ anzubieten, die in Wirklichkeit nicht existierten, würden hier u.a. Bundeswehrpilot*innen ausgebildet und an militärischen Drohnen geforscht. Grundsätzlich gehe er der Frage nach, wie es gelinge, „sich als Gesellschaft selbst als friedfertige Demokratie zu erleben und gleichzeitig einen ganz expansiven Militarismus zu betreiben, der sehr viele Felder betrifft.“ In diesem Zusammenhang verwies er darauf, dass NATO und Bundeswehr bereits seit Jahren versuchten, eine „Battle Management Language“ zu entwickeln, eine Sprache für Mensch-Maschine Systeme, die keine Mehrdeutigkeiten und keine Widersprüche erlaube bzw. kenne.

Cyberwar...

Der Sonntag widmete sich zunächst im engeren Sinne der militärischen Sicht auf Cyberkrieg und Kommunikationstechnik. *Hans-Jörg Kreowski*, emeritierter Professor für theoretische Informatik, gab zunächst einige Beispiele für erfolgte Cyberattacken, etwa im Kontext des Georgienkrieges oder Stuxnet, der iranische Gaszentrifugen manipulierte. In diesen Fällen legt der konkrete Kontext eine Urheberschaft – einmal Russlands, einmal der USA – nahe; grundsätzlich ließe sich diese jedoch kaum eindeutig nachweisen. Der Cyberwar bzw. die Vorbereitung hierauf setze voraus und beinhalte, dass mit viel Geld Sicherheitslücken aufrechterhalten und gehandelt werden. Die Folgen reichten von Unbequemlichkeiten etwa durch Verschlüsselungstrojaner auf Privatrechnern bis hin zu Angriffen „in dramatischem Umfang“ und mit enormen Ausmaßen, auch hinsichtlich „der Vernichtung von Menschenleben“. Die hierfür notwendigen Fähigkeiten müssten entwickelt werden und prägten bereits teilweise das Fach Informatik. „Die ganze Welt rüstet gigantisch auf“, so Kreowski. Demgegenüber warb er für das Konzept des „Cyberpeace“. Voraussetzung hierfür wäre, dass die Fähigkeiten und Ressourcen, die aktuell in die Vorbereitung des Cyberkriegs fließen, für die Beseitigung von Sicherheitslücken aufgebracht würden. Das würde sowohl Gesellschaften und kritische Infrastrukturen wie auch private Anwender*innen vor militärischen, staatlichen und kriminellen Angriffen schützen. Abschließend ging Kreowski auf die Begriffsgeschichte ein. Spionage und Propaganda habe es immer gegeben, im Zweiten Weltkrieg hätte das Ver- und Entschlüsseln elektronisch übermittelter Daten an Bedeutung gewonnen und die Grundlage heutiger Geheimdienste gelegt. Die Absicherung von und Angriffe auf militärische Führungssysteme wären bis in die 1990er Jahre unter der Bezeichnung „Informationskrieg“ und dann als „Cyberkrieg“ bezeichnet worden. Heute kehre der Begriff des Informationskrieges zurück und meine neben der Absicherung militärischer Kommunikation zunehmend auch Aktivitäten, die auf die Beeinflussung der öffentlichen Meinung zielen.

… und militärische Landschaften.

Hieran anschließend stellte *Christoph Marischka* v.a. anhand historischer Beispiele und mit einem räumlichen Ansatz die Kommunikationsinfrastruktur von Bundeswehr und NATO vor. Dabei zeige sich, dass diese bereits in der Vergangenheit einen hybriden Charakter aufgewiesen habe, indem sie öffentliche Infrastruktur, wie Kabel und Richtfunkstrecken der Bundespost genutzt und durch zusätzliche eigene Richtfunkstrecken ergänzt habe. Außerdem sei auch der Strategiewechsel von NATO und Bundeswehr an der Infrastruktur der Kommunikation erkennbar. So sei das Führungssystem der Luftwaffe früher deutlich defensiver ausgerichtet gewesen und habe darauf abgezielt, eindringende Flugzeuge von Osten zu erkennen und von im Westen Deutschlands gelegenen Kommandozentralen Gegenmaßnahmen einzuleiten. Heute würde versucht, die Führungssysteme der verschiedenen Teilstreitkräfte und NATO-Mitgliedsstaaten zu vereinheitlichen und diese über Satelliten aus der Ferne zu koordinieren. Auch in diese offensive Kommunikationsstruktur seien privatwirtschaftliche Unternehmen wie Airbus und das Deutsche Zentrum Luft- und Raumfahrt (DLR), das sich gerne einen zivilen Anstrich gibt, eingebunden.

Andreas Seifert stellte sich daraufhin der Frage: „Wer verdient eigentlich am Cyberkrieg?“ und fokussierte sich dabei auf eher kleinere und unbekannte Firmen. Hierzu stellte er zunächst den Branchenverband AFCEA vor. In Deutschland präsentiere sich dieser als „Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung“, eigentlich stehe die Abkürzung jedoch für „Armed Forces Communications and Electronics Association“. Viele der beteiligten Unternehmen befänden sich neben dem Großraum München in Köln und Bonn. AFCEA veranstalte pro Jahr 20 bis 30 Messen, Konferenzen und Fachforen, an denen sich Menschen aus dem Militär, der Politik, der Forschung und der Wirtschaft beteiligen. Kürzlich etwa habe ein solches Forum unter dem Titel „Automatisierte Meinungsbeeinflussung – Manipulation in offenen Medien“ stattgefunden. Vorgetragen hätten u.a. ein Vertreter des Verfassungsschutzes zu Social Engineering und ein Soldat des Zentrums für Operative Kommunikation zum Thema „Bundeswehr und Katzenvideos – Social Media als militärisches Wirkmittel“. Tatsächlich seien bei AFCEA neben den Produzenten von Hardware und eingebetteten Systemen auch Firmen vertreten, die kleinteilige Dienstleistungen im Bereich der Prüfung, des Managements und der Kommunikation für die Bundeswehr erbringen, wie Seifert an vielen Beispielen veranschaulichte. Am Beispiel der Drohne Eurohawk und eines mit DLR und Airbus durch Satelliten erstellten Höhenmodells der Erde wurde jedoch auch auf IT-Großprojekte eingegangen, mit denen Unternehmen auf einen Schlag hunderte Millionen Euro verdienten. Bei einer drastischen Erhöhung des Rüstungsetats sei v.a. auch davon auszugehen, dass viel Geld in die Ausbildung und zusätzliches Personal fließen dürfte. Dies bedeute angesichts der Suche nach neuen Formen der Rekrutierung und des angestrebten „atmenden Personalkörpers“ eben auch die engere Zusammenarbeit mit teilweise kleinen Unternehmen, die besser – und verstärkt auch personell – einbezogen werden sollten.

Spontan wurde das letzte Panel durch einen Beitrag von *Emanuel Matondo* erweitert, der die Folgen des Exports von Überwachungstechnologie aus Deutschland nach Angola sehr persönlich veranschaulichte. Seit 2005 habe die angolanische Regierung die zunehmenden Aktivitäten von Zivilgesellschaft, Opposition und Journalist*innen zunehmend mit Sorge betrachtet. 2008 sei dann die technische Infrastruktur des Militärgeheimdienstes spürbar ausgebaut worden und es sei immer wieder die Rede von deutschen Ingenieur*innen gewesen, die Installationen und Schulungen in Angola durchführten. Seit dieser Zeit würde auch der Mobilfunk im Umfeld des Präsi-

denten gestört, was die Bevölkerung frustriere. Mittlerweile werde davon ausgegangen, dass Siemens / Nokia Networks und Rohde & Schwarz aus München führend am Ausbau des Überwachungsapparates in Angola beteiligt seien. Die Menschen in Angola wären spürbar eingeschüchtert, gingen seither bei Telefonaten davon aus, abgehört zu werden, und fühlten sich auch bei ihren Aktivitäten in sozialen Netzen eingeschränkt.

Widerstand und Gegenöffentlichkeiten

Zum Abschlusspodium „Widerstand im Zeitalter von Cyberwar und Strategischer Kommunikation“ waren Personen geladen, die im weiteren Sinne als Medienschaffende zu bezeichnen wären. *Anna Hunger*, von der Wochenzeitung „Kontext“, beschrieb die eher klassische journalistische Arbeit in einer Redaktion, die allerdings klein ist und somit den engen persönlichen Austausch innerhalb der Redaktion ermögliche. Auch aus finanziellen Gründen habe diese keine Agenturen abonniert und suche sich ihre Themen deshalb neben der sonstigen Presse auch durch Anrufe und Schreiben von Leser*innen aus, denen dann nachgegangen werde.

Judith Lauterbach, vom freien Radio Wüste Welle, sah den Unterschied zu herkömmlichen Medien darin, dass in den Sendungen des freien Radios unmittelbar betroffene und aktive Menschen zu Wort kämen. Dadurch sei die Berichterstattung vielleicht einseitig bzw. parteiisch, aber auch authentisch und glaubwürdig. Auf sog „soziale Medien“ sei zumindest sie dadurch gar nicht angewiesen und damit auch nicht so stark gefährdet, Falschmeldungen aufzusitzen. Freie Radios seien ein „Mitmach-Medium“ und damit Teil einer Demokratisierung der Öffentlichkeit.

Tobias Pflüger als IMI-Vorstandsmitglied, Aktivist und Bundestagsabgeordneter bezeichnete gründliche Recherche als Voraussetzung politischer Arbeit, die eben häufig in der Aufbereitung von Informationen bestehe. Es sei auch immer wichtig, sich Standorte und Firmen vor Ort anzusehen. Andererseits müsse man auch als Informationsquelle damit rechnen, von Medien instrumentalisiert zu werden und sich genau überlegen, wem man z.B. Interviews gibt.

Dass man auch kreativ mit Informationen umgehen kann, zeigte anschließend ein Aktivist auf, der über *Adbusting* sprach. Dabei werden Werbeplakate manipuliert, um ihre ursprüngliche Nachricht umzukehren oder zu pervertieren. Die Bundeswehr sei hierfür ein sehr dankbarer Kooperationspartner, sobald sie an die Öffentlichkeit gehe. Sie operiere mit sehr einfachen Slogans auf der Grundlage positiv besetzter Begriffe wie „verteidigen“. Würden diese mit negativ konnotierten Begriffen wie „Ausbeutung“ kontrastiert, wäre das zwar eine Verfälschung der eigentlichen Nachricht, die der Wirklichkeit aber vielleicht sogar näher kommt. Als Quelle seien die Aktivist*innen auf alternative Medien angewiesen und das Adbusting könne diese auch nicht ersetzen, da es auf sehr kurze, prägnante Aussagen angewiesen wäre, die nicht als Grundlage für politisches Handeln ausreichten oder den persönlichen Kontakt ersetzen könnten.

Einen größeren Raum nahmen auch sog. Verschwörungstheorien, die oft von rechten Spektren verbreitet und vermarktet werden, ein und wie diese von „verschleierten Wahrheiten“ unterschieden werden könnten. Wenn Darstellungen Angst machen, Hilflosigkeit vermitteln und eine kleine Gruppe von Menschen für alles verantwortlich machen, wären das tendenziell Hinweise auf eine Verschwörungstheorie, so etwa Hunger. Zugleich handele es sich hier auch um einen Kampfbegriff, der Positionen und Personen diskreditieren kann und manchmal auch soll. Mehrdeutigkeit sei jedoch – anders als vom Militär gedacht – ein wesentliches Merkmal menschlicher Sprache und deshalb der Umgang hiermit eine Notwendigkeit und ein Teil der Medienkompetenz, die man u.a. in demokratischen Medien wie freien Radios erlernen kann, wie Lauterbach ergänzte. Dass auch staatliche Repression mittlerweile spürbar in den öffentlichen Diskurs einwirkt, sprach Pflüger am Beispiel des Internetportals „Linksunten“ an. Das vage Konstrukt eines nicht existierenden Vereins, der dann verboten wurde, sei mit Berichten über vermeintliche Waffenfunde flankiert worden. Die zugrunde liegende Argumentation, dass strafrechtlich relevante Aussagen hier geduldet wurden, wäre ebenso z.B. auf Facebook anzuwenden, wo Aufrufe zur Gewalt gerade auch aus der rechten Ecke alltäglich wären, niemand aber jemals ein Verbot in Betracht ziehen oder gutheißen würde.

Überraschende Gemeinsamkeiten

In der anschließenden Diskussion wurde u.a. dazu aufgerufen, das existierende Bild von Medien auf den Kopf zu stellen und dass sich jeder Mensch als Journalist*in fühlen sollte. Dem wurde allerdings auch im Sinne einer notwendigen Qualitätssicherung widersprochen. Natürlich konnte die Abschlussdiskussion keine endgültige Klärung dahingehend bringen, wie Widerstand in Zeiten des Informationskriegs zu gestalten sei, jedoch gelang es das gegenseitige Verständnis von Medienschaffenden und Aktivist*innen zu erhellen. Auch was das Thema „Krieg im Informationsraum“ anging, wurde während des gesamten Kongresses mehrfach betont, dass die IMI nur erste Ansätze zu dessen Verständnis sammeln wollte und konnte. Trotzdem zeigten sich unabgesprochene und überraschende Parallelen zwischen den einzelnen Zugängen, von denen einige hier abschließend genannt werden sollen:

1. Dass Gegner, denen Propaganda bzw. Informationskrieg vorgeworfen wird, identifiziert werden, setzt die Annahme einer eigenen moralischen Überlegenheit und Wahrheitstreue voraus, die inhaltlich kaum unterfüttert, sondern eben durch den Verweis auf die Manipulation durch den Gegner ersetzt wird.

2. Obwohl sich die aktuell mit dem Begriff des Informationsraums vollzogene Fusionierung von Cyberkrieg und Propaganda bereits länger vollzieht, werden die Aktivitäten des IS und Russlands derzeit als wesentliche Legitimationsfigur verwendet, wobei keine qualitative Differenzierung zwischen beiden Akteuren erfolgt. Westliche und internationale zivilgesellschaftliche Akteure und ihre Argumente werden in frappierender Klarheit als deren Komplizen und Werkzeuge dargestellt und als Feinde im Informationsraum identifiziert.

3. Argumente gegen die eigene Regierung, die EU oder die Nato werden als bezahlte und gesteuerte Propaganda der Gegner disqualifiziert und in keiner Weise inhaltlich adressiert.

4. Die Strategische Kommunikation (Propaganda) von EU und NATO wird eher als „Rauschen“ wahrnehmbar, das Akteure kontinuierlich positiv oder negativ konnotiert und von Ereignissen größerer Relevanz ablenkt.

5. Beim „Cyber“- und „Informationsraum“ handelt es sich um eine hybride Infrastruktur, die bereits seit ihrem Entstehen von einem Wechselspiel staatlicher, privatwirtschaftlicher und zivilgesellschaftlicher Akteure geprägt ist. Der Krieg im Informationsraum politisiert diese Akteure im Sinne Carl Schmitts: Wer nicht für uns ist, ist gegen uns und wir (egal wer) sind die Guten.