

Stellungnahme zum

**Entwurf der EU-Kommission  
zur Verordnung Nr. 428/2009  
über Exportkontrollen  
von Dual Use-Gütern**

Anhörung des Bundesministeriums  
für Wirtschaft und Energie am 27.01.2017

Eingereicht am 10. Februar 2017

**Eingereicht von:**  
Reporter ohne Grenzen e.V.  
Friedrichstraße 231  
10969 Berlin

**Ansprechpartner:**

Daniel Moßbrucker

Referent für Informationsfreiheit im Internet

030 – 6098 9533 23

[dm@reporter-ohne-grenzen.de](mailto:dm@reporter-ohne-grenzen.de) (PGP: F09F78A3)

<b>Vorwort</b> .....	<b>4</b>
<b>1. Notwendigkeit eines strengen Kontrollregimes bei Exporten von Dual Use-Gütern aus menschenrechtlicher Perspektive, insbesondere zum Schutz der Pressefreiheit weltweit</b> .....	<b>5</b>
<b>2. Fortschritte des Entwurfs zur aktuellen Rechtslage</b> .....	<b>7</b>
<b>2.1 Erweiterung des Dual Use-Begriffes</b> .....	<b>7</b>
2.1.1 Verbesserungspotenzial der neuen Definition .....	8
<b>2.2 Einführung einer EU-autonomen Liste</b> .....	<b>8</b>
<b>2.3 Allgemeine Ausfuhrgenehmigungen für Verschlüsselung</b> .....	<b>9</b>
<b>3. Kritikpunkte und Verbesserungsvorschläge</b> .....	<b>10</b>
<b>3.1 Definition des Prüfkriteriums „Menschenrechte“</b> .....	<b>10</b>
3.1.1. Human Rights Due Diligence und Human Rights Impact Assessment .....	11
3.1.2 Exportverbote bei menschenrechtlichen Risiken.....	12
<b>3.2 Ausgestaltung der Catch All-Klauseln</b> .....	<b>13</b>
<b>3.3 Transparenz- und Statistikpflichten</b> .....	<b>15</b>
<b>4. Fazit und Ausblick</b> .....	<b>17</b>

## Vorwort

Reporter ohne Grenzen (ROG) hat den politischen Prozess zur Aufnahme von Überwachungstechnologie in die Anhänge der Dual Use-Verordnung (Nr. 428/2009, im folgenden: Verordnung) im Jahr 2015 von Beginn an intensiv begleitet und Exporte solcher Technologien an autoritäre Regierungen stets scharf kritisiert.

Unter anderem hat ROG bereits 2013 in einer ausführlichen Recherche bestimmte Hersteller von Überwachungstechnologie anlässlich des World Day Against Cyber Censorship am 12. März als „Feinde des Internets“ bezeichnet und maßgeblich zu einer öffentlichen Auseinandersetzung mit Firmen wie Blue Coat, Gamma International, Trovicor und Hacking Team beigetragen.<sup>1</sup> Politisch hat ROG den Prozess unter anderem mit Stellungnahmen vor dem Unterausschuss „Abrüstung, Rüstungskontrolle und Nichtverbreitung“ im April 2013<sup>2</sup> sowie im November 2014<sup>3</sup> begleitet.

Die grundlegende Überarbeitung der Verordnung durch die Europäische Union begrüßt Reporter ohne Grenzen im Grundsatz. Ebenfalls für sinnvoll halten wir die Einbeziehung der Zivilgesellschaft durch die Bundesregierung und die damit verbundene Möglichkeit, im Rahmen dieser Stellungnahme zur Weiterentwicklung des am 28. September 2016 von der EU-Kommission vorgelegten Entwurfes (im Folgenden: Verordnung-NF) mitzuwirken.

Die Stellungnahme bezieht sich insbesondere auf die Regelungen zu Genehmigungspflichten für Technologie zur digitalen Überwachung im Sinne des Art. 2 Abs. 1 Nr. b der Verordnung-NF.

Reporter ohne Grenzen ist eine international tätige Menschenrechtsorganisation, die sich für den Schutz von Journalisten und die Stärkung der Pressefreiheit weltweit einsetzt. Vor diesem Hintergrund erkennt ROG zwar an, dass auch der Export von Dual Use-Gütern, im Speziellen von Überwachungstechnologie, im wirtschaftlichen Interesse der EU liegen kann und die Hersteller solcher Technologien grundsätzlich bestimmte Rechte wie zum Beispiel den Schutz Betriebs- und Geschäftsgeheimnissen genießen. Gleichzeitig beobachtet Reporter ohne Grenzen weiterhin Fälle und betreut diese teilweise, in denen Journalisten Ziel von digitaler Überwachung geworden sind. ROG ist daher von der Notwendigkeit eines möglichst strengen Exportregimes solcher Technologien überzeugt und hat die vorliegende Stellungnahme in diesem Lichte verfasst.

Der Schwerpunkt dieser Stellungnahme liegt auf Exportkontrollen von Überwachungstechnologie, weil Reporter ohne Grenzen hier über Expertise verfügt und in seiner Nothilfe-Arbeit mit den Gefahren dieser Technologie konfrontiert ist. Diese Fokussierung bedeutet nicht, dass ROG Gefahren für die Menschenrechte beim Export anderer Dual Use-Güter als geringer einschätzt. Im Gegenteil: Ein wirksamer Schutz von Menschenrechten durch Exportkontrollen kann nur gewährleistet werden, wenn sämtliche Dual Use-Güter einer wertebasierten Ausfuhrpolitik unterliegen, wie es die Verordnung-NF erfreulicherweise vorsieht.

# 1. Notwendigkeit eines strengen Kontrollregimes bei Exporten von Dual Use-Gütern aus menschenrechtlicher Perspektive, insbesondere zum Schutz der Pressefreiheit weltweit

Die Aufnahme von Überwachungstechnologie in die Verordnung war ein wichtiges politisches Signal, sollte jedoch bloß als Einstieg in eine fortlaufende Verbesserung der Regulierung von Dual Use-Gütern gesehen werden. Die vergangenen Jahre haben gezeigt, dass die aktuelle Rechtslage den Handel mit Überwachungstechnologie zwischen Herstellern mit Sitz in der EU und autokratischen oder bisweilen sogar diktatorischen Regimen nicht stoppen konnte.

Schon heute beobachtet Reporter ohne Grenzen in vielen Ländern der Welt, wie auf schreckliche Weise Regierungen mittels moderner Überwachungstechnologie gegen Journalisten, Aktivisten und Oppositionelle im eigenen Land vorgehen – häufig mit Software westlicher Firmen, die teilweise dorthin verkauft worden ist, als dies nach europäischem Recht noch legal war. Eine interne Auswertung der mittlerweile über 500 Nothilfe-Fälle, in denen Reporter ohne Grenzen Journalisten in Notsituationen geholfen hat, hat gezeigt, dass in über 50 Prozent der Fälle digitale Überwachung eine Rolle gespielt hat.

Beispielsweise hat die syrische Regierung nachweislich einen gewaltigen Überwachungsapparat aufgebaut, als die Proteste noch längst nicht begonnen hatten bzw. weitaus später dann im Begriff waren, sich zu einer nationalen Bewegung für mehr Demokratie zu formieren. Auch Firmen, die zumindest zu Teilen in Deutschland agieren wie z.B. Advanced German Technology, spielten bei diesen Geschäften eine zentrale Rolle.<sup>4</sup>

Anfang 2017 äußerte sich erstmals ein ehemaliger Mitarbeiter eines syrischen Geheimdienstes, der als Whistleblower im Interview mit der ARD über das Ausmaß der Überwachung in Syrien sprach. Er bestätigte, dass das Assad-Regime insbesondere Journalisten überwacht und versucht, jede Kritik im Keim zu ersticken. Mittels digitaler Überwachung werden Quellen enttarnt, Journalisten geortet, verhaftet und häufig in Foltergefängnisse gebracht, die sie nie wieder lebend verlassen. Wer sich gegen die Überwachung mittels Verschlüsselung und Anonymisierung schützen will, gilt als verdächtig.

In dem Gespräch, das unter anderem ROG-Referent Daniel Moßbrucker führte, bestätigte der Whistleblower außerdem, dass das syrische Regime seine Überwachungstechnik noch Anfang 2012 aufwändig modernisieren konnte, als die Proteste im Land längst brutal niedergeschlagen wurden. Bis zu welchem Zeitpunkt der Whistleblower genau für die syrischen Geheimdienste tätig war, kann aus Gründen des Informantenschutzes nicht genau gesagt werden.<sup>5</sup>

Reporter ohne Grenzen sieht sich durch das traurige Beispiel Syriens in seiner generellen Kritik bestätigt, dass Überwachungstechnologie stets ein enormes Risiko für demokratische und speziell nicht-demokratische Gesellschaften darstellt und hohe Missbrauchsgefahren birgt. Der Export solcher Technologien in Länder ohne gefestigte Demokratie und ohne funktionierenden Rechtsstaat ist unverantwortlich und abzulehnen. Bis heute sind es mutige Bürgerjournalisten in Syrien, die unter Einsatz ihres Lebens unabhängige Informationen im Bürgerkrieg recherchieren und mittels digitaler Technologien der Welt zur Verfügung stellen. Dass Technologie aus westlichen Ländern diese Arbeit nahezu unmöglich macht, ist beschämend.

Hat der globale Handel mit Überwachungstechnologie vor der Reform der Dual Use-Verordnung in vielen Ländern autokratische Strukturen gestärkt, sind diese Geschäfte durch die Klassifizierung als Dual Use-Güter in der Verordnung trotzdem weiter getätigt worden. Geleakte Email-

Korrespondenzen der italienischen Firma Hacking Team haben bewiesen, dass das Unternehmen entgegen eigener Angaben auch nach der Verschärfung der Dual Use-Verordnung weiter Produkte in autokratische Länder verkauft hat.<sup>6</sup> Hochbedenklich stimmen ebenfalls Berichte der britischen Organisation Privacy International, wonach die italienische Firma Area SpA von den italienischen Kontroll- und Aufsichtsbehörden erst kürzlich eine Genehmigung zum Verkauf umfangreicher Überwachungsprogramme an Ägypten erhalten hat.

„According to a recent PI investigation, the unit to which Area SpA has been allowed to sell the internet surveillance system, the Technical Research Department, is a shadowy unaccountable government intelligence agency responsible for implementing Egypt's surveillance apparatus, and has procured equipment from numerous European countries.“<sup>7</sup>

Italienische Behörden haben übrigens dieselbe Firma, Area SpA, kurz zuvor wegen fragwürdiger Exporte nach Syrien durchsuchen lassen.<sup>8</sup> Hier zeigt sich einerseits, dass die Behörden dringend rechtliche Mittel benötigen, um solche Verkäufe aus menschenrechtlichen Erwägungen verhindern zu können. Die Initiative der EU ist daher im Grundsatz zu begrüßen.

Gleichzeitig zeigen die Beispiele aus Italien, dass bei einer Gefährdung für Menschenrechte ein Export nicht nur genehmigungspflichtig, sondern verboten werden muss. Bei menschenrechtlichen Fragen darf es Schlupflöcher für Unternehmen ebenso wenig geben wie einen Ermessensspielraum für europäische Behörden. Menschenrechte dürfen für die Europäische Union nicht verhandelbar sein. Klare rechtliche Regelungen sind letztlich aber auch im Interesse der handelnden Unternehmen, die Rechtssicherheit genießen, wenn Verkäufe in gewisse Länder generell verboten sind.

Im Interesse der Unternehmen sollte es weiterhin sein, möglichst transparent gegenüber Behörden zu handeln und kooperativ zu agieren. Leider war das in der Vergangenheit nicht der Fall. Stattdessen haben diverse Unternehmen Rechte wie den Schutz von Betriebs- und Geschäftsgeheimnissen für illegale Verkäufe missbraucht und agieren in einem intransparenten, grauen Markt am Rande der Legalität – oder gänzlich kriminell.

Auch in Deutschland sind solche Firmen beheimatet und scheren sich bis heute nicht um rechtliche Regelungen, die den Export von Überwachungstechnologie regulieren sollen. Besonders drastisch ist der Fall der Firma Wolf Intelligence, die in München sitzt und 2015 ein umfangreiches Paket an Überwachungssoftware an die Staatsführung von Mauretanien für 2,5 Millionen US Dollar verkaufen wollte.<sup>9</sup> Das Land rangierte 2015 auf Platz 55 der Rangliste der Pressefreiheit von Reporter ohne Grenzen.<sup>10</sup> ROG setzt sich dort unter anderem für den Blogger Mohamed Cheikh Ould M'Kheitir ein, der seit drei Jahren im Gefängnis sitzt und Ende 2014 wegen eines vermeintlich islamkritischen Blogeintrags zum Tode verurteilt worden war.<sup>11</sup>

Aufgrund solch illegaler Machenschaften vermeintlich integrierter Sicherheitsfirmen aus Deutschland sollten Kontrollbehörden aus Sicht von Reporter ohne Grenzen mit umfangreichen Befugnissen ausgestattet werden, um diese Firmen überprüfen zu können und illegale Geschäfte zu verhindern. Es braucht zudem Transparenzpflichten in Form von Statistiken, um eine gesellschaftliche Debatte über diese Geschäfte zu ermöglichen und Journalisten in den betroffenen Drittländern Ansätze zu geben, um zum Thema Überwachung in ihren Heimatländern recherchieren zu können.

## 2. Fortschritte des Entwurfs zur aktuellen Rechtslage

In diesem Abschnitt werden die Aspekte aus der Verordnung herausgegriffen, die aus Sicht von Reporter ohne Grenzen im Grundsatz gelungen sind und – wenn überhaupt – nur noch einer vergleichsweise geringen Überarbeitung bedürfen.

### 2.1 Erweiterung des Dual Use-Begriffes

Die Überarbeitung der Verordnung mit einem Schwerpunkt auf dem Schutz von Menschenrechten, die insbesondere auch durch den Einsatz von Überwachungstechnologie bedroht sein können, ist im Grundsatz zu begrüßen. Insbesondere ist es sinnvoll, dass die Definition von Dual Use-Gütern erweitert worden ist und Überwachungstechnologie explizit in Art. 2 Abs. 1 Nr. b der Verordnung-NF definiert wird als

„Technologie für digitale Überwachung, die für die Begehung schwerwiegender Verletzungen der Menschenrechte oder des humanitären Völkerrechts verwendet werden oder eine Bedrohung für die internationale Sicherheit oder die wesentlichen Sicherheitsinteressen der Union und ihrer Mitgliedstaaten darstellen kann“.

Diese begriffliche Erweiterung ist richtig, da sie dem besonderen Charakter von Überwachungstechnologie als Teil der Dual Use-Güter gerechter wird als die vorherige Allgemeindefinition.

Das Argument, dass damit definitorisch mit anderen Kontrollregimen gebrochen wird und die EU ihre Vorreiterrolle in der Exportpolitik verlieren könnte, überzeugt nicht. Im Gegenteil: Die bisherigen Definitionen von Dual Use-Gütern, etwa im Wassenaar-Abkommen, haben sich als überholt erwiesen und sollten nach der Initiative der EU nun ebenfalls angepasst werden, um stärker auf digitale Überwachungstechnologie abzielen zu können.

Begrüßenswert ist zudem, dass Abs. 21 des Art. 2 Verordnung-NF „Technologien für digitale Überwachung“ weiter präzisiert als

„Güter, die besonders dafür konstruiert sind, das unbemerkte Eindringen in Informations- und Telekommunikationssysteme zu ermöglichen, um Daten zu überwachen, zu extrahieren, zu sammeln und zu analysieren und/oder das betreffende System betriebsunfähig zu machen oder zu beschädigen. Dies umfasst Güter im Zusammenhang mit folgender Technologie und Ausrüstung:

- a) Ausrüstung zum Abhören von mobiler Telekommunikation;
- b) Intrusion-Software,
- c) Überwachungszentren,
- d) Systeme zur rechtmäßigen Überwachung und Vorratsdatenspeicherung,
- e) digitale Forensik“.

Insbesondere die Aufnahme von System zur rechtmäßigen Überwachung und Vorratsdatenspeicherung („law enforcement“) ist sinnvoll, weil sie bei missbräuchlicher Anwendung extrem weitreichende Folgen haben können und sich in ihrer Eingriffstiefe in die Grundrechte der Betroffenen kaum oder gar nicht unterscheiden von übriger Hacking-Software.<sup>12</sup>

Gleichzeitig scheint eine strenge Kontrolle dieser Instrumente geboten, weil immer wieder Fälle bekannt werden, in dem mit Hilfe von Programmen des „law enforcement“ auch in demokratisch verfassten Staaten unrechtmäßig gegen Journalisten vorgegangen wird. Zwei kürzlich bekannt gewordene Beispiele sind die Vorfälle in Kanada gegen Patrick Lagacé und sechs weitere Kollegen<sup>13</sup> sowie in Großbritannien gegen Jeremy Armstrong und zwei weitere Kollegen<sup>14</sup>, als jeweils mit Hilfe von Überwachungsinstrumenten Quellen von Journalisten enttarnt wurden, was einen klaren Angriff auf die Pressefreiheit darstellt.

Dies zeigt: Überwachungstechnologien sollten – wenn denn überhaupt – äußerst zurückhaltend eingesetzt werden, ihr Einsatz muss nach rechtstaatlichen Prinzipien unabhängig kontrolliert werden und auch ein Export solcher Software – egal in welches Land – sollte äußerst restriktiv gehandhabt werden. Die Versuchung für staatliche Stellen, beim Besitz solcher Technologien gegen Journalisten vorzugehen, ist naturgemäß verlockend, weshalb nur eine strenge Limitierung im Sinne des Schutzes der Pressefreiheit sein kann.

### 2.1.1 Verbesserungspotenzial der neuen Definition

Weiterer Präzisierung bedarf der Begriff der „Digitalen Forensik“, der vermutlich wegen aktueller Diskussionen im Zuge der Weiterentwicklung des Wassenaar-Abkommens in die Verordnung aufgenommen worden ist („digital forensics“). Es ist unklar, was darunter fallen soll und ob die Aufnahme des Begriffes tatsächlich geboten erscheint oder kontraproduktiv für den Schutz von Menschenrechten sein kann. Kontraproduktiv wäre die Begriffseinführung dann, wenn „Digitale Forensik“ zum Beispiel für die Aufnahme von Verschlüsselungstechnologien in die Kontrolllisten genutzt würde. Auch eine Erfassung von Programmen, mit denen Privatnutzer zum Beispiel aus Versehen gelöschte Fotos auf dem Mobiltelefon wiederherstellen können, wäre abzulehnen. Solche weitgefassten Definitionen würden letztlich wieder Rechtsunsicherheit bei den Unternehmen hervorrufen, womit entweder die Akzeptanz für das Instrument der Exportkontrolle als Ganzes sinkt oder die zuständige Behörde im Mitgliedsstaat überlastet würde.

Begrüßenswert wäre eine Interpretation im Sinne von Software, mit dem zum Beispiel Strafermittler gelöschte Inhalte auf Festplatten wiederherstellen können oder mittels Brute-Force-Methoden Passwortschutz verschlüsselter Programme umgangen werden soll. Es ist unverständlich, warum ein solch neuer Begriff wie „Digitale Forensik“ im Anhang zur Verordnung nicht weiter definiert wird. Dies sollte zwingend geschehen. Ergänzt werden könnten die Begriffsdefinitionen um eine negative Abgrenzung, wie es bereits für den Begriff Überwachungszentren in Anhang B, Kategorie 10 vollzogen worden ist. Hier sollte sich die Bundesregierung für eine weitere Präzisierung der Begriffe des Art. 2 Abs. 2 Nr. 21 Verordnung-NF einsetzen, insbesondere bei der digitalen Forensik.

Außerdem ist unklar, warum unter Punkt a) nur Ausrüstung zum Abhören mobiler Kommunikation als digitale Überwachungstechnologie gelten soll, nicht aber bei im klassischen Sinne leitungsgebundener Telefonie („Festnetz“). Auch hier sollte sich die Bundesregierung für eine weitere Präzisierung des Paragraphen in der Verordnung-NF einsetzen und die Definition ausweiten.

## 2.2 Einführung einer EU-autonomen Liste

Positiv zu bewerten ist Art. 3 Abs. 1 i.V.m. Anhang 1, Abschnitt B Verordnung-NF sowie der neue Art. 16 Abs. 2 Nr. b) Verordnung-NF, wonach der EU-Kommission die Befugnis übertragen wird, delegierte Rechtsakte zu erlassen, um die Liste von Gütern mit doppeltem Verwendungszweck in Anhang 1, Abschnitt B ändern zu können,

„wenn dies notwendig ist, weil mit der Ausfuhr solcher Güter möglicherweise Risiken im Hinblick auf die Begehung schwerwiegender Verletzungen der Menschenrechte, des humanitären Völkerrechts oder der wesentlichen Sicherheitsinteressen der Union und ihrer Mitgliedstaaten verbunden sind.“

Durch beide Regelungen entsteht die Möglichkeit, dass bei Exporten aus der EU in Drittländer schärfer kontrolliert werden kann als bisher, weil die Güterlisten umfangreicher sein können als eine Zusammenfassung der Güterlisten der übrigen vier Kontrollregime Australische Gruppe,

MTCR, NAG und Wassenaar. Diese EU-autonome Liste ist sinnvoll, um über die bisherigen Kontrollregime hinaus notwendige Anpassungen vornehmen zu können. Bei der Neuaufnahme von Gütern in Anhang 1, Abschnitt B ist ein transparenter und partizipativer Prozess seitens der EU-Kommission gefordert, in dem neben den Unternehmen mit ihren Interessen insbesondere auch die Zivilgesellschaft Einfluss nehmen kann. Sinnvoll könnte eine Kontaktstelle sein, an die sich Unternehmen, Vertreter der Zivilgesellschaft, aber auch Betroffene in den Drittländern wenden können, um auf Menschenrechtsverletzungen aufmerksam zu machen und technologische Innovationen dort melden zu können.

Mit dieser EU-autonomen Liste muss mittelbar Druck für eine transparente Überarbeitung der Kontrolllisten der anderen Ausfuhrregime entstehen, da z.B. das Wassenaar-Abkommen eine „closed group“ ist, obwohl eigentlich eine demokratischere Mitbestimmung geboten wäre. Keinesfalls darf die neue Liste des Anhangs 1, Abschnitt B ein Sammelbecken werden für Technologien, die im Wassenaar-Abkommen und den übrigen Kontrollregimen definitiv nicht hineinpassen und daher dort gar nicht reguliert werden sollen. Ferner darf die EU-autonome Liste die bisherige Struktur internationaler Exportkontrolle nicht zerstören, sondern stützen und Anreize für eine menschenrechtskonforme Weiterentwicklung gebeten. Reporter ohne Grenzen ist überzeugt, dass dies möglich ist und hält entsprechende Bedenken seitens der Industrie für übertrieben und teilweise konstruiert. Die EU muss weiterhin Vorreiter bleiben, um die Kontrollregime auf globaler Ebene zu verfeinern und hat damit durch Anhang 1 Abschnitt B ein neues Druckmittel erhalten.

### 2.3 Allgemeine Ausfuhrgenehmigungen für Verschlüsselung

Begrüßenswert ist auch, dass Dual Use-Güter aus dem Bereich der Informationssicherheit, insbesondere kryptografische Verfahren, gemäß Art. 10 Abs. 1 Nr. d) der Verordnung in Verbindung mit Anhang 2 eine allgemeine Ausfuhrgenehmigung erhalten, sofern sie nicht zu militärischen Zwecken gebraucht werden sollen. Effektive Verschlüsselung ist für Journalisten essenziell. Informanten müssen sicher sein können, dass ihre Identität geschützt bleibt und sensible Informationen in Redaktionen gut aufgehoben sind. Ist das nicht der Fall, scheuen Informanten im Zweifel die Kontaktaufnahme und der gesellschaftlich wichtige Informationsfluss zu den Medien versiegt.

Im Zuge zunehmender staatlicher Überwachung werden Verschlüsselungstechnologien für Journalisten derzeit immer wichtiger. Ein barrierefreier globaler Handel mit diesen Technologien ist begrüßenswert, um Innovationen aus Europa auch an anderen Orten der Welt wirksam werden zu lassen. Die Bundesregierung sollte sich daher dafür einsetzen, diesen Handel zu fördern, insbesondere im Bereich Open Source-Software.

### 3. Kritikpunkte und Verbesserungsvorschläge

Die grundsätzliche Stoßrichtung der Verordnung-NF ist aus menschenrechtlicher Perspektive wie beschrieben positiv, doch in vielen neu eingeführten Regelungen bedarf es besserer und umfassenderer Definitionen, um sie erst wirksam zu machen. Im Folgenden sollen die wichtigsten Kritikpunkte am Entwurf aufgeführt werden.

#### 3.1 Definition des Prüfkriteriums „Menschenrechte“

Die bisherige Definition des Prüfkriteriums „Menschenrechte“, die in Art. 14 Verordnung-NF geregelt ist, ist unzureichend. Neben dem Umstand, dass die Frage einer Genehmigung sich an den Verpflichtungen der Mitgliedsstaaten in den internationalen Nichtverbreitungsregimen und Ausfuhrkontrollvereinbarungen orientieren muss, spielen zusätzlich eine Rolle:

- „b) die Achtung der Menschenrechte und des humanitären Völkerrechts durch das Endbestimmungsland;
- c) die innere Lage im Endbestimmungsland – die zuständigen Behörden verweigern die Genehmigung von Ausfuhren, die im Endbestimmungsland bewaffnete Konflikte auslösen bzw. verlängern würden oder bestehende Spannungen oder Konflikte verschärfen würden;
- d) die Aufrechterhaltung von Frieden, Sicherheit und Stabilität in der jeweiligen Region;“

Diese Bestimmungen dürfen nicht mehr als ein erster Schritt in der Genese der neuen Dual Use-Verordnung bleiben, um nicht wirkungslos zu bleiben. Exportkontrolle ist nur dann sinnvoll, wenn sie für Regulierungsbehörden und Unternehmen praktikabel umsetzbar ist – und wenn sich die Inhaber von Menschenrechten in den betroffenen Drittländern auf ein klares Bekenntnis und eine deutliche Ausgestaltung selbiger berufen können. Derzeit finden sich nur vage Bestimmungen, dass ein Schutz der Menschenrechte geboten ist. Dies ist nicht mehr als ein Rechtstext, der in seiner derzeitigen Form wirkungslos bleiben wird.

Es ist völlig unklar, was die Bestimmungen in der Praxis für eine Relevanz erfahren sollen. Es braucht strukturierte Regelwerke, die menschenrechtliche Fragen auf die Praxis übertragen und Prüfkriterien beinhalten, anhand derer die menschenrechtliche Situation in einem Drittland bestimmt werden kann. Eine Mindestanforderung ist es, die in Frage stehenden Menschenrechte bei den betreffenden Gütern – vorzugsweise güterspezifisch in den Anhängen selbst – zu nennen und damit dezidierte Prüfkataloge zu entwickeln. Diese Idee steckt auch im Zitiergebot im deutschen Grundsatz nach Art. 19 Abs. 1 S. 2 sein, das für Exportkontrollen weiterentwickelt werden könnte.

„Soweit nach diesem Grundgesetz ein Grundrecht durch Gesetz oder auf Grund eines Gesetzes eingeschränkt werden kann, muss das Gesetz allgemein und nicht nur für den Einzelfall gelten. Außerdem muss das Gesetz das Grundrecht unter Angabe des Artikels nennen.“

So könnten im Falle von Überwachungstechnologie gemäß Art. 2 Abs. 21 Verordnung-NF besonders bedrohte Menschenrechte wie das Recht auf Privatsphäre (Art. 12 AEMR) sowie das Recht auf Meinung- und Pressefreiheit (Art. 19 AEMR) genannt werden. Denkbar ist auch eine Zitation der Europäischen Menschenrechtskonvention, wobei zumindest ein Verweis auf die Allgemeine Erklärung der Menschenrechte sinnvoll erscheint, da es bei den Exportkontrollen ja gerade um Handelsbeziehungen geht, die sich auch außerhalb der EU abspielen.

Diese explizite Nennung bestimmter, besonders bedrohter Menschenrechte würde bei der Prüfung von Anträgen den zuständigen Stellen helfen, an die Art. 14 Verordnung-NF adressiert ist. Es hätte aber gerade auch für die betroffenen Unternehmen den Vorteil, sich bei der einer Vorab-Prüfung im Zuge des Antragsprozesses auf eben diese Rechte zu konzentrieren. Dies macht den Prozess

handhabbarer, wirtschaftlicher und damit wirksamer. Zuletzt böte sich wiederum die Möglichkeit für die Zivilgesellschaft, mit der Recherche von Fällen wirksamer dazu beizutragen, besonders bedrohte Menschenrechte zu schützen und Informationen für Behörden und Unternehmen bereitzustellen.

Für Prüfungen durch Unternehmen und zuständige Stellen braucht es explizite Vorgaben, Leitfäden und Methoden. Dies scheint die Verordnung-NF auch vorzusehen, doch die Ausführungen dazu sind derart vage, dass dies nicht mit Sicherheit konstatiert werden kann. Zu empfehlen ist daher, bei der Erarbeitung solcher Leitfäden transparente Entscheidungsprozesse unter Einbeziehung der Zivilgesellschaft zu etablieren. Hierzu sollte auf die Erfahrung der betroffenen Unternehmen, Informationen von Institutionen der EU und ihrer Mitgliedstaaten, Expertise von europäischen Fachleuten sowie der Zivilgesellschaft in den betroffenen Drittländern zurückgegriffen werden. Diesen Ansatz verfehlt der Entwurf in der aktuellen Fassung völlig, da Abs. 2 des Art. 14 lediglich festhält:

„Die Kommission und der Rat stellen Leitfäden und/oder Empfehlungen zur Verfügung, um bei der Anwendung der genannten Kriterien eine einheitliche Risikobewertung durch die zuständigen Behörden der Mitgliedstaaten sicherzustellen.“

Zwar ist auch dieser Ansatz im Grundsatz wieder richtig. Mangels Bestimmtheit hält Reporter ohne Grenzen die derzeitige Ausgestaltung des „Prüfkriteriums Menschenrechte“ jedoch für verfehlt und unbedingt nachbesserungswürdig.

Die vorliegende Verordnung würde in der neuen Fassung zum Beispiel kaum verhindern können, dass Großbritannien weiterhin dutzende Exportlizenzen für IMSI-Catcher bei Verkäufen an autoritäre Regime genehmigt, wie es 2015 der Fall war – unter anderem nach China und Kuwait<sup>15</sup>, die auf der Rangliste der Pressefreiheit von Reporter ohne Grenzen auf den Plätzen 176 und 103 stehen.<sup>16</sup> Ein bloßer Verweis auf Menschenrechte in der Verordnung-NF hätte kaum zur Folge, dass die zuständige Behörde in Großbritannien eine Exportgenehmigung verweigern könnte, ohne erfolgsversprechende Klagen der Unternehmen fürchten zu müssen.

### 3.1.1. Human Rights Due Diligence und Human Rights Impact Assessment

Zweifelsfrei ist die „Gretchenfrage“ der Verordnung-NF, wie sich Menschenrechte „messen“ lassen können und in welchem Verfahren zuständige Behörden und Unternehmen solche Prüfungen vornehmen könnten. Hingewiesen sei an dieser Stelle darauf, dass diese Diskussion in anderen Politikfeldern bereits intensiv geführt wird durch die UN-Leitprinzipien Wirtschaft und Menschenrechte (Ruggie-Prinzipien)<sup>17</sup>. Human Rights Due Diligence ist Kern der zweiten Säule dieser Prinzipien und es ist daher nur folgerichtig, dass die EU diese Sorgfaltspflicht nun auch auf die Exportkontrollen von Dual Use-Gütern ausweiten soll. Dies ist begrüßenswert.

Im Zuge der Umsetzung der Ruggie-Prinzipien im Nationalen Aktionsplan Wirtschaft und Menschenrechte sind in einem (leider nicht vollständig) partizipativen Prozess Kriterien erarbeitet worden, welche die Bundesregierung nun auch in die Diskussion auf EU-Ebene einfließen lassen sollte. Auch wenn der am 21. Dezember 2017 vom Bundeskabinett beschlossene Nationale Aktionsplan insgesamt kein zufriedenstellender Kompromiss aus menschenrechtlicher Perspektive geworden ist<sup>18</sup>, bietet er doch erste Ansätze für eine praktische Umsetzung menschenrechtlicher Prüfungsmechanismen bei Exportkontrollen.<sup>19</sup>

Von zentralem Interesse muss die Diskussion um Methoden für ein Human Rights Impact Assessment (HRIA) sein. Hier hat das Dänische Institut für Menschenrechte 2016 eine umfangreiche Methodik inklusive Leitlinien und Toolbox für die praktische Durchführung solcher HRIA vorgelegt.

„In the business context, HRIA can be defined as a process for identifying, understanding, assessing and addressing the adverse effects of a business project or activities on the human rights enjoyment of impacted rights-holders such as workers and community members. (...) HRIA involves several phases or steps, all of which need to be included to ensure a comprehensive assessment. In this Guidance and Toolbox the phases have been divided into:

1. Planning and scoping
2. Data collection and baseline development
3. Analysing impacts
4. Impact mitigation and management; and
5. Reporting and evaluation.“<sup>20</sup>

Der Blick liegt hier ausdrücklich nicht auf Fragen der Exportkontrolle, sondern auf Großprojekten wie der Bau von Firmengebäuden zur Textilproduktion. Allerdings dürften die fünf Phasen grundsätzlich auf Prüfprozesse bei der Exportkontrolle anzuwenden sein, wobei ein besonderes Augenmerk bei den Punkten zwei und drei liegen dürfte. Aber auch eine mindestens stichprobenartige Kontrolle im Nachhinein und Berichtspflichten sind notwendig, um für zukünftige Entscheidungen eine bessere Entscheidungsgrundlage zu erlangen.

Zur 1. Anhörung „Human Rights Due Diligence und Human Rights Impact Assessments – Anforderungen“ am 29. April 2015 im Auswärtigen Amt hat Dr. Brigitte Hamm vom Institut für Frieden und Entwicklung (INEF) Handlungsempfehlungen für die Bundesregierung formuliert<sup>21</sup>, von denen die folgenden auch für den Prozess einer menschenrechtskonformen Exportkontrolle formuliert werden könnten:

- Klare Regeln für die Durchführung und Veröffentlichung HRIA
- Entwicklung von best practice Beispielen für die effektive Einbindung Betroffener
- Schulung von Personal in Unternehmen für die Wahrnehmung der menschenrechtlichen Sorgfaltspflicht (inklusive HRIA)
- Zeit einräumen für die Durchführung der menschenrechtlichen Sorgfaltspflicht
- Erforderliche Kontextinformationen sollten für Unternehmen leicht zugänglich, einfach und kontinuierlich abrufbar sein, bspw. durch Bereitstellung einer Datenbank

Dem letzten Aspekt kommt für Reporter ohne Grenzen eine zentrale Bedeutung bei der neuen Menschenrechts-Catch All-Klausel zu (siehe Abschnitt 3.2).

### 3.1.2 Exportverbote bei menschenrechtlichen Risiken

Menschenrechte können letztlich nur dann effektiv geschützt werden, wenn Exporte in Drittländer nicht nur genehmigungspflichtig werden, sondern gänzlich verboten sein müssen, sobald menschenrechtliche Bedenken in irgendeiner Form zum Tragen kommen. Jegliche Schlupflöcher konterkarieren den notwendigen Schutz der Menschenrechte und werden von manchen Firmen als Einladung verstanden werden, ihre bisweilen kriminellen Geschäfte voranzutreiben und sich in Werbevideos noch mit der Rechtmäßigkeit Ihres Handels brüsten. Gleichzeitig können Unternehmen, denen aus menschenrechtlichen Erwägungen eine Exportlizenz verweigert wird, stets mit rechtlichen Schritten drohen und die zuständige Behörde damit unter Druck setzen. Im Sinne der Rechtssicherheit für beide Seite sollte daher klargestellt werden, dass Exporte bei menschenrechtlichen Risiken verboten sind.

Die Bundesregierung sollte sich daher im weiteren Prozess auf europäischer Ebene in Bezug auf Art. 14 der Verordnung für eine Verschärfung der Kontrollbefugnisse, Präzisierung der Begriffe und transparente Erarbeitung der Leitfäden einsetzen.

## 3.2 Ausgestaltung der Catch All-Klauseln

Weil eine staatliche Exportkontrolle mit umfangreichen Prüflisten naturgemäß der technologischen Entwicklung und Innovation hinterherläuft, ist es sinnvoll, dass die Verordnung Catch All-Klauseln enthält. Dadurch können unter bestimmten Voraussetzungen auch Ausfuhren von Dual Use-Gütern genehmigungspflichtig sein, wenn sie nicht in der Verordnung explizit aufgeführt sind.

Zum einen ist die Ausfuhr von Gütern mit doppeltem Verwendungszweck, die nicht in Anhang 1 aufgeführt sind, gemäß Art. 4 Abs. 1 genehmigungspflichtig, wenn der Ausführer von der zuständigen Behörde des Mitgliedstaats darüber unterrichtet wird. Anhaltspunkt für diese Klassifizierung kann durch den neuen Abs. 1 Nr. d) nun auch sein, dass die Güter bestimmt sind oder sein können

„für die Verwendung durch Personen, die nach Feststellung maßgeblicher internationaler öffentlicher Einrichtungen oder der zuständigen europäischen oder nationalen Behörden im Rahmen von bewaffneten Konflikten oder im Zuge der internen Repression im Endbestimmungsland an der Anordnung oder Begehung schwerwiegender Verletzungen der Menschenrechte oder des humanitären Völkerrechts beteiligt oder hierfür verantwortlich waren, wenn Hinweise vorhanden sind, dass diese oder ähnliche Güter vom vorgeschlagenen Endverwender zur Anordnung oder Durchführung solcher schwerwiegenden Verstöße eingesetzt werden.“

Diese „Menschenrechts-Catch-All“-Klausel ist im Grundsatz wieder begrüßenswert und kohärent zur neuen Struktur der Verordnung. Ebenso wie schon in Teil 3.1 dieser Stellungnahme beschrieben, fehlt aber auch diesem menschenrechtlichen Prüfkriterium die Präzision und Bestimmtheit, um wirksam werden zu können. Im Gegenteil, der Wortlaut wird nochmals geändert und „maßgebliche öffentliche Einrichtungen“ werden unter anderem aufgeführt, wobei völlig unklar bleibt, was damit gemeint sein soll.

Dieses gilt für die Menschenrechts-Catch-All-Klausel im Falle des Art. 4 Abs. 1, wenn die Initiative gewissermaßen bei der zuständigen Behörde liegt, jedoch besonders auch für den Abs. 2, in denen die Unternehmen eine Sorgfaltspflicht abverlangt wird („due diligence“):

„Ist einem Ausführer entsprechend seiner Verpflichtung, die gebotene Sorgfalt walten zu lassen, bekannt, dass Güter mit doppeltem Verwendungszweck, die er ausführen möchte und die nicht in Anhang I aufgeführt sind, ganz oder teilweise für eine der Verwendungen im Sinne des Absatzes 1 bestimmt sind, so hat er die zuständige Behörde davon zu unterrichten; diese entscheidet, ob die Ausfuhr dieser Güter genehmigungspflichtig sein soll.“

Diese Umsetzung der UN-Leitlinien (s.o.) ist sinnvoll und folgerichtig. Gleichwohl ist die Kritik der Wirtschaft an dieser neuen Form der Catch All-Klauseln nicht zu ignorieren, weil auch hier wieder gilt: Nicht praktikable Regelungen führen zu einer geringeren Akzeptanz der Exportkontrolle als Ganzer und verfehlen damit den Zweck, die Menschenrechte zu schützen. Der Schluss, dass diese Menschenrechts-Catch-All für Unternehmen wieder aus der Verordnung-NF gestrichen werden muss, ist allerdings abzulehnen. Vielmehr gilt es, die Regelung so auszugestalten, dass sie für Unternehmen und zuständige Behörden gleichermaßen anwendbar ist und die Rechteinhaber wirksamen Schutz erhalten.

Reporter ohne Grenzen schlägt daher vor, eine gemeinsame Datenbank aufzubauen, in denen Unternehmen recherchieren können und sich über die Menschenrechtssituation im Bestimmungsland informieren können (Anlehnung an die Debatte zum Human Rights Impact Assessment siehe Abschnitt 3.1.1). Dort müssen menschenrechtlich relevante Informationen über alle Länder, in die Unternehmen aus EU-Mitgliedsstaaten exportieren wollen, verfügbar sein können. Empfehlenswert ist, diese Informationen thematisch zu gliedern, sodass zum Beispiel in einem Teil besonders auf die Meinungsfreiheit im Bestimmungsland eingegangen wird, im anderen auf die Versammlungsfreiheit usw. Dies erleichtert Unternehmen und zuständigen

Behörden bei der Prüfung wiederum die Recherche, ob beim Export bestimmter Produkten die Menschenrechte gefährdet werden können. Diese Datenbank wäre landerbasiert, könnte aber auch bestimmte Güter nennen, mit denen in der Vergangenheit bereits Menschenrechtsverletzungen begangen worden sind.

Diese Datenbank hat keine rechtlich bindende Wirkung, weil sie keine Empfehlungen für den Export bestimmter Güter in einzelne Bestimmungsländer enthält. Wichtig ist, dass die Datenbank von einer neu zu schaffenden Stelle („maßgebliche Behörde“ i.S.d. Art. 4 Abs. 1) gepflegt wird, die über die ausreichenden Ressourcen verfügt und möglichst unabhängig von der EU-Kommission gestellt wird. Dies könnte etwa in einer Rechtskonstellation ähnlich der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) geschehen. Sie sollte für die Datenbank Informationen verarbeiten (1) aus den Mitgliedsländern, (2) von den Unternehmen, (3) von unabhängigen Experten innerhalb der EU, etwa aus dem Bereich der Zivilgesellschaft und Wissenschaft, sowie (4) von regionalen Partnern, die vor Ort über Expertise verfügen. Die Informationen dieser Datenbank sollten transparent nach anerkannten methodischen Vorgaben erarbeitet werden und die Informationen sollten öffentlich verfügbar sein.

Entsteht ein solches Angebot, ist es den betroffenen Unternehmen zweifelsfrei zuzumuten, bei Exportvorhaben in Drittländer dort zu recherchieren und inhouse Kompetenz aufzubauen, um über die Notwendigkeit von Genehmigungen gemäß der Verordnung-NF i.S.d. Art. 4 Abs. 2 zu entscheiden.

EU-weit einheitliche Prüfschemata, anhand derer Produkte bewertet werden können, sind dafür zwingend erforderlich. Am Beispiel der digitalen Überwachungstechnologie sollte besonders maßgeblich sein,

- ob die Produkte im Endbestimmungsland legaldefiniert sind;
- ob rechtstaatliche Vorgänge etabliert sind, die den Einsatz erst erlauben, wie zum Beispiel eine richterliche Kontrolle;
- ob das technische Know-how in den zuständigen Behörden des Endbestimmungslandes ausreicht, um die Instrumente legal einsetzen zu können, missbrauch zu verhindern und illegale Weitergabe zu unterbinden;
- ob von digitaler Überwachung besonders häufig betroffene Gruppen wie Journalisten, Menschenrechtsverteidiger, Anwälte und Oppositionelle in der Vergangenheit Opfer von unrechtmäßiger digitaler Überwachung geworden sind;
- ob die Produkte in der Vergangenheit bereits zu Menschenrechtsverletzungen geführt haben, obwohl es beim Export selbst noch nicht absehbar gewesen ist.

Solche Prüfmuster sollten in der Verordnung-NF explizit genannt werden, um zu definieren, was unter „gebotener Sorgfalt“ zu verstehen ist – und welche Pflichten damit konkret einhergehen. Bisher haben sich diverse Anbieter von digitaler Überwachungstechnologie gerade nicht um menschenrechtliche Fragen gesorgt und die oben zitierten Fälle lassen kaum darauf schließen, dass in der Branche ein rascher Gesinnungswandel einsetzen wird.

Insofern sollte erwägt werden, für Firmen, die in der Vergangenheit bereits negativ durch Exporte von digitaler Überwachungstechnologie in autokratisch regierte Länder aufgefallen sind, eine Art Blacklist zu erstellen. Solche Unternehmen könnten dann besonders stark reguliert werden und ihre Genehmigungspflichten wären besonders hoch. Auch könnten die Kontrollmöglichkeiten erweitert werden, wodurch der Schutz von Betriebs- und Geschäftsgeheimnissen eingeschränkt würde. Durch langfristig legales Verhalten muss es dann möglich werden, von diesen Blacklists genommen zu werden. Damit werden integer agierende Unternehmen nicht zu stark belastet, ebenso bleibt der Kontrollaufwand für die zuständigen Behörden in einem vertretbaren Maß.

Gleichwohl würde die EU dem selbstgesteckten Ziel, die Menschenrechte durch die Reform der Verordnung wirksamer zu schützen, gerecht werden.

Die Bundesregierung sollte dieses Modell bei den weiteren Beratungen der Verordnung-NF auf europäischer Ebene diskutieren und sich insgesamt für eine präzisere Ausgestaltung der Catch-All-Klauseln des Art. 4 einsetzen. Keinesfalls sollte die Menschenrechts-Catch-All aufgrund der Kritik seitens der Unternehmen aus dem Entwurf der Verordnung-NF genommen werden.

### 3.3 Transparenz- und Statistikpflichten

Auch dem Entwurf zur neuen Verordnung fehlen jegliche Pflichten, dass Hersteller Transparenz über ihre Handelspartner herstellen respektive seitens der EU oder ihrer Mitgliedstaaten Statistiken veröffentlicht werden, welche Arten von Dual Use-Gütern wie häufig in welche Länder verkauft worden sind und wie viele Genehmigungen nicht erteilt worden sind. Dies ist völlig unverständlich und inakzeptabel.

Gerade der Handel mit digitaler Überwachungstechnologie findet auf einem Schattenmarkt statt, auf dem dubiose Geschäftsleute agieren und für Außenstehende nur selten nachzuweisen ist, ob illegale oder zumindest illegitime Deals abgeschlossen werden. Die Aufklärung der letzten Jahre, die maßgeblich zur Initiative der EU zur Überarbeitung der Verordnung beigetragen hat, ist insbesondere der Arbeit von Nichtregierungsorganisationen wie dem European Center for Constitutional and Human Rights, Privacy International und Reporter ohne Grenzen zu verdanken, die häufig in Einzelfällen die fragwürdigen Geschäfte nachweisen konnten. Die Hersteller digitaler Überwachungstechnologie reden sich häufig jedoch heraus mit dem Argument, dass die publik gewordenen Fälle bedauerliche Einzelfälle seien, man sich im Allgemeinen aber an alle rechtlichen und ethischen Verpflichtungen halte. Dass dies häufig nichts als Lügen sind, hat die italienische Firma Hacking Team noch 2016 in einem ARD-Interview bewiesen.<sup>22</sup>

Es ist daher zwingend erforderlich, dass Transparenz in den Handel mit solchen Technologien gebracht wird und Statistikpflichten eingeführt werden. Vorbild könnte der Rüstungsexportbericht sein, in dem so etwas möglicherweise auch als Anhang für Dual Use-Güter integriert werden könnte. Denkbar und letztlich sinnvoller wäre hingegen ein EU-weit einheitlicher Bericht, der wiederum die Exportlizenzenvergaben für die einzelnen Ländern nach bestimmten Produktgruppen aufschlüsselt. Nur so kann innerhalb Europas ein gesellschaftlicher Diskurs entstehen über die Frage, ob es akzeptabel ist, dass gerade aus der Mitte Europas Überwachungstechnologie kommt, die eine Gefahr für Menschenrechte auf der gesamten Welt darstellt. Das Ausmaß der Exporte darf nicht nur innerhalb von Kontrollbehörden bekannt sein, sondern muss Gegenstand öffentlicher Debatten und einer journalistischen Aufarbeitung sein, wofür Statistikpflichten die Mindestgrundlage sind.

Darüber hinaus stellt es für die Bevölkerung in den betroffenen Drittländern die womöglich einzige unabhängige Informationsquelle dar, von der Existenz der Überwachungsfähigkeiten der eigenen Regierung zu erfahren. Statistiken könnten somit Ansätze für Recherchen von Journalisten sein, um die Bevölkerung im eigenen Land über die Gefahren digitaler Überwachung aufzuklären und für digitale Sicherheit zu werben, was einen effektiver Schutz von Menschenrechten und Pressefreiheit darstellt.

Es reicht dafür nicht, dass gemäß Art. 20 Abs. 1 der Verordnung-NF die Maßnahmen und Vorschriften der Mitgliedstaaten an die Kommission weitergeleitet werden und im Amtsblatt der Europäischen Union veröffentlicht werden. Auch genügt es nicht, dass gemäß Art. 20 Abs. 2 der

Informationsaustausch zwischen nationalen und EU-Behörden intensiviert wird, um kohärente Kontrollmechanismen zu garantieren.

Ansatzpunkt für eine höhere Transparenz wäre der neue Art. 24, der allerdings im entscheidenden neuen Abs. 2 nicht zielführend verändert worden ist:

„Die Kommission legt dem Europäischen Parlament und dem Rat einen Jahresbericht über die Durchführung und Durchsetzung der Kontrollen in der Union und über die Tätigkeiten, Prüfungen und Konsultationen der Koordinierungsgruppe ‚Güter mit doppeltem Verwendungszweck‘ vor.“

Die in den bisherigen Jahresberichten<sup>23</sup> aufgeführten Informationen und Statistiken sind unzureichend und erfüllen nicht die Anforderungen, um sich umfassend über Art und Umfang der Dual Use-Exporte der EU-Länder zu informieren. Warum hier weiterhin dem Schutz von Betriebs- und Geschäftsgeheimnissen der Unternehmen Vorrang vor einer transparenten Exportpolitik gegeben wird, ist nicht nachvollziehbar.

Es braucht regelmäßige, mindestens jährliche Statistiken, die Dual Use-Güter in Untergruppen kategorisieren, wovon digitale Überwachungstechnik eine Untergruppe sein könnte. Dazu braucht es dann detaillierte Informationen dazu, aus welchen Ländern wie viele Genehmigungen gestellt wurden, wie viele abgelehnt und wie viele bewilligt wurden, in welche Länder wie viele Exporte vollzogen worden sind und welches Handelsvolumen sich damit ergibt. Dies wären absolute Mindeststandards für eine zufriedenstellende Statistikpflicht – wünschenswerter wäre stärkere Detailtiefe, wonach zum Beispiel Überwachungstechnologie weiter differenziert wird in den Kategorien des Art. 2 Abs. 21 Nr. a) bis e) oder sich an den Güterlisten in den Anhängen der Verordnung-NF orientiert.

Hiermit würden Betriebs- und Geschäftsgeheimnisse der Unternehmen weiterhin gewahrt, weil weder einzelne Exportgüter näher beschrieben werden noch konkrete Einzelverträge zwischen Unternehmen und Staaten erfasst und veröffentlicht würden. Vielmehr ergäbe sich die Chance für die Unternehmen, Vertrauen zurückzugewinnen und für Journalisten und Zivilgesellschaft nachvollziehbar zu machen, ob die neue Verordnung tatsächlich zu einem wirksameren Schutz der Menschenrechte beiträgt. Die Bundesregierung sollte sich dafür einsetzen, solche Transparenz- und Statistikpflichten im weiteren Gesetzgebungsverfahren auf EU-Ebene durchzusetzen.

## 4. Fazit und Ausblick

Insgesamt hat die EU-Kommission mit dem Entwurf zur neuen Dual Use-Verordnung einen Kurs eingeschlagen, der in die richtige Richtung zeigt und aus menschenrechtlicher Perspektive unbedingt beibehalten werden muss. Es ist zu begrüßen, dass nun auch in der EU-Exportkontrolle zentrale Elemente der Ruggie-Prinzipien aufgenommen werden. Menschenrechte als Prüfkriterien für Kontrollbehörden, die Menschenrechts-Catch-All-Klausel sowie eine Sorgfaltspflicht für exportierende Unternehmen sind zentrale Säulen einer menschenrechtskonformen Exportkontrolle, an denen im Gesetzgebungsprozess nicht mehr gerüttelt werden darf.

Reporter ohne Grenzen wird die Reform weiterhin konstruktiv begleiten und hat mit dieser Stellungnahme einen Vorschlag erarbeitet, wie die Verordnung-NF an den entscheidenden Stellen weiter verbessert werden sollte, um für Unternehmen handhabbarer zu werden und damit in der Praxis wirksam zu werden. Enttäuschend ist, dass Exportkontrolle laut Verordnung-NF weiterhin eine Blackbox bleiben soll, die von der Öffentlichkeit nicht kritisch begleitet werden kann. Hier kommt ein veraltetes Demokratieverständnis zum Ausdruck, das dem Ziel einer modernen Exportkontrolle zuwiderläuft. Umfassende Transparenz- und Statistikpflichten sind unverzichtbar, um den Diskurs über das Instrument der Exportkontrolle aufrecht zu erhalten – was letztlich nur im Interesse aller Beteiligten sein kann und mit dem Recht auf Wahrung der Betriebs- und Geschäftsgeheimnisse nicht im Widerspruch stehen muss.

Die Bundesregierung trägt bei den weiteren Beratungen auf europäischer Ebene eine enorme Verantwortung, weil sie aufgrund des enormen Exportvolumens der deutschen Wirtschaft großen Einfluss hat. Deutschland sollte seine Vorreiterrolle bei der Fortentwicklung der europäischen Exportkontrolle behalten und sich für die oben vorgeschlagenen Verbesserungen einsetzen. Eine rasche Umsetzung der neuen Dual Use-Verordnung ist erstrebenswert, weil sich jeder Export fatal auf die Menschenrechte auswirken kann. Insbesondere digitale Überwachung stellt ein zunehmendes Risiko für Journalisten auf der ganzen Welt dar.

Mit dieser Neuaufstellung der europäischen Exportkontrolle von Use Dual-Gütern darf die Debatte jedoch nicht abreißen. Vielmehr kann moderne Exportkontrolle nur dann gelingen, wenn sie sich ständig an die neuen Innovationen und politischen Rahmenbedingungen anpasst. Neue Herausforderungen sind dabei bereits am Horizont sichtbar. So ist die EU gerade mit Blick auf Überwachungstechnologie bei den Verhandlungen über den Austritt Großbritanniens aus der EU in der Verantwortung, die hohen Standards bilateral aufrechtzuerhalten. Bereits heute sitzen viele der oben zitierten Firmen zumindest teilweise in Großbritannien und im Falle des Brexit droht, dass etwa London als Standort für solche Hersteller wichtiger werden könnte. Hier sollte alles dafür getan werden, die Ziele der eigenen Wirtschaftspolitik zu sichern und Großbritannien zu menschenrechtskonformen Exportkontrollen zu bewegen.

Gleichzeitig ist die Pressefreiheit auch innerhalb der europäischen Union teilweise unter Druck geraten. Mahnende Beispiele sind Polen und Ungarn, in denen die Arbeit von Journalisten systematisch eingeschränkt wird. Im Handumdrehen können heute gutgläubig exportierte Überwachungstechnologien dort zu modernen Waffen umfunktioniert werden. Die EU sollte im eigenen Interesse überdenken, ob eine allzu freizügige Exportpolitik solcher Güter sinnvoll ist.

Der Hang der EU-Staaten, die eigenen Bürger und auch Journalisten stärker zu überwachen, ist eine gefährliche Entwicklung. Dies gilt auch für Deutschland. Exportkontrolle darf anlasslose und unverhältnismäßige Überwachung innerhalb der EU nicht zementieren. Wozu das führen kann, ist in vielen Teilen der Welt leider alltäglich zu beobachten. Die EU trägt dafür eine mittelbare Mitverantwortung. Umso wichtiger ist es, in Zukunft menschenrechtliches Handeln der Wirtschaft zur Maxime der eigenen Exportpolitik zu erheben.

- 
- <sup>1</sup> Reporter ohne Grenzen (2013): „*Enemies of the Internet*“, abrufbar unter: [https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Berichte\\_und\\_Dokumente/2014/Stellungnahme\\_Export dt\\_Ueberwachungstechnologie\\_17.04.2013.pdf](https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Berichte_und_Dokumente/2014/Stellungnahme_Export_dt_Ueberwachungstechnologie_17.04.2013.pdf)
- <sup>2</sup> Reporter ohne Grenzen (2013): „*Schriftliche Stellungnahme von Reporter ohne Grenzen e.V. anlässlich der Sitzung des Unterausschusses ‚Abrüstung, Rüstungskontrolle und Nichtverbreitung‘ am 17. April 2013*“, abrufbar unter: [https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Berichte\\_und\\_Dokumente/2014/141112\\_Anhoerung\\_Unterausschuss\\_Ruestungskontrolle.pdf](https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Berichte_und_Dokumente/2014/141112_Anhoerung_Unterausschuss_Ruestungskontrolle.pdf)
- <sup>3</sup> Reporter ohne Grenzen (2014): „*Schriftliche Stellungnahme von Reporter ohne Grenzen e.V. anlässlich der Sitzung des Unterausschusses ‚Abrüstung, Rüstungskontrolle und Nichtverbreitung‘ am 12. November 2014*“, abrufbar unter: [https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Berichte\\_und\\_Dokumente/2014/141112\\_Anhoerung\\_Unterausschuss\\_Ruestungskontrolle.pdf](https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Berichte_und_Dokumente/2014/141112_Anhoerung_Unterausschuss_Ruestungskontrolle.pdf)
- <sup>4</sup> Meister, Andre (2016): „*Arabischer Frühling als Jagdsaison: Wie westliche Firmen den syrischen Überwachungsstaat aufgebaut haben*“, abrufbar unter: <https://netzpolitik.org/2016/arabischer-fruehling-als-jagdsaison-wie-westliche-firmen-den-syrischen-ueberwachungsstaat-aufgebaut-haben/>
- <sup>5</sup> Dittert, Annette / Moßbrucker, Daniel (2017): „*Assads ‚elektronische Armee‘*“, abrufbar unter: <https://www.tagesschau.de/ausland/darknet-doku-103.html>
- <sup>6</sup> Omanovic, Edin (2016): „*Hacking Team’s Global License Revoked by Italian Export Authorities*“, abrufbar unter: <https://www.privacyinternational.org/node/826>
- <sup>7</sup> Privacy International (2016): *New investigation reveals Syria’s mass surveillance ambitions and the shadowy Western surveillance companies that profit from it*, abrufbar unter: <https://www.privacyinternational.org/node/1033>
- <sup>8</sup> Franceschi-Bicchierai, Lorenzo (2016): „*Italian Cops Raid Surveillance Tech Company Accused of Selling Spy Gear to Syria*“, abrufbar unter: <https://motherboard.vice.com/read/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria>
- <sup>9</sup> Franceschi-Bicchierai, Lorenzo / Formica, Federico (2016): „*The Forgotten Prisoner of a Spyware Deal Gone Wrong*“, abrufbar unter: <https://motherboard.vice.com/read/the-forgotten-prisoner-of-a-spyware-deal-gone-wrong>
- <sup>10</sup> Reporter ohne Grenzen (2015): „*Rangliste der Pressefreiheit 2015*“, abrufbar unter: [https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Ranglisten/Rangliste\\_2015/Rangliste\\_der\\_Pressefreiheit\\_2015.pdf](https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Ranglisten/Rangliste_2015/Rangliste_der_Pressefreiheit_2015.pdf)
- <sup>11</sup> Reporter ohne Grenzen (2017): „*Todesstrafe gegen Blogger nicht vollstrecken*“, abrufbar unter: <https://www.reporter-ohne-grenzen.de/mauretaniens/alle-meldungen/meldung/todesstrafe-gegen-blogger-nicht-vollstrecken/>
- <sup>12</sup> Reporter ohne Grenzen (2016): „*Vorratsdatenspeicherung endlich kippen*“, abrufbar unter: <https://www.reporter-ohne-grenzen.de/presse/pressemitteilungen/meldung/vorratsdatenspeicherung-endlich-kippen/>
- <sup>13</sup> Piontek, Helena (2016): „*Abhörskandal von Journalisten in Kanada zieht weitere Kreise*“, abrufbar unter: <https://netzpolitik.org/2016/abhoerskandal-von-journalisten-in-kanada-zieht-weitere-kreise/>
- <sup>14</sup> Committee to Protect Journalists (2017): „*UK police monitored calls of Daily Mirror and Northern Echo journalists*“, abrufbar unter: <https://cpj.org/2017/01/uk-police-monitored-calls-of-daily-mirror-and-nort.php>

---

<sup>15</sup> Cox, Joseph (2016): „*British Companies Are Selling Advanced Spy Tech to Authoritarian Regimes*“, abrufbar unter: <https://motherboard.vice.com/read/the-uk-companies-exporting-interception-tech-around-the-world>

<sup>16</sup>Reporter ohne Grenzen (2015): „*Rangliste der Pressefreiheit 2015*“, abrufbar unter: [https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Ranglisten/Rangliste\\_2015/Rangliste\\_der\\_Pressefreiheit\\_2015.pdf](https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Ranglisten/Rangliste_2015/Rangliste_der_Pressefreiheit_2015.pdf)

<sup>17</sup> United Nations (2011): „*Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*“, abrufbar unter: [http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf)

<sup>18</sup> Boll, Frederike (2017): „*Der Nicht-Aktions-Plan*“, abrufbar unter: <http://www.ipg-journal.de/schwerpunkt-des-monats/wirtschaft-und-menschenrechte/artikel/detail/der-nicht-aktions-plan-1781/>

<sup>19</sup> Bundesregierung (2016): „*Nationaler Aktionsplan 'Wirtschaft und Menschenrechte'*“, abrufbar unter: <http://www.auswaertiges-amt.de/cae/servlet/contentblob/754690/publicationFile/222786/161221-NAP-DL.pdf>

<sup>20</sup> The Danish Institute for Human Rights (2016): „*Human Rights Impact Assessment. Guidance and Toolbox*“, abrufbar unter: [http://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria\\_toolbox/hria\\_guidance\\_and\\_toolbox\\_final\\_may22016.pdf](http://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/hria_guidance_and_toolbox_final_may22016.pdf)

<sup>21</sup> Auswärtiges Amt (2015): „*Dokumentation – Nationaler Aktionsplan Wirtschaft und Menschenrechte. Human Rights Due Diligence und Human Rights Impact Assessments – Anforderungen*“, abrufbar unter: <http://www.auswaertiges-amt.de/cae/servlet/contentblob/711994/publicationFile/207809/Expertenanhoerung1.pdf>

<sup>22</sup> Katrin Matthaer (2016): „*Unkontrollierter Export: Spähsoftware made in Europe*“, abrufbar unter: <http://www.daserste.de/information/politik-weltgeschehen/europamagazin/sendung/sendung-vom-18092016-unkontrollierter-export-spaehsoftware-abhoerwanzen-geheimdienste-computer-mobiltelefone-terroristen-softwarefirmen-100.html>

<sup>23</sup> z.B. Europäische Kommission (2016): „*REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items*“, abrufbar unter: [http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc\\_154929.pdf](http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154929.pdf)