Thomas Reinhold

Rüstungskontrolle für den Cyberspace – Herausforderungen und erste Ansätze

Das Konzept der Rüstungskontrolle wurde als politische Reaktion auf die Rüstungsdynamiken im internationalen Staatensystem entwickelt. Rüstungskontrolle ist dabei im Kern ein normatives Unterfangen, das vom Prinzip der Verhinderung zukünftiger Kriege geleitet wird und sich dabei auch mit den Bedingungen und Umständen befasst, die zu bewaffneten Konflikten führen. Das Konzept kann als „einseitige Maßnahmen, bilaterale und multilaterale Abkommen sowie informelle Regime (…) zwischen Staaten bezeichnet werden, um bestimmte Kategorien von Waffen oder militärischen Operationen einzuschränken oder zu reduzieren, um stabile militärische Gleichgewichte zu erreichen und so Spannungen und die Wahrscheinlichkeit von Konflikten zu verringern" (Den Dekker, 2004).

Diese Aufgabe kann dabei in drei verschiedene Teile aufgegliedert werden (Müller & Schörnig, 2006):

- Kriegsprävention und Verringerung der Konfliktwahrscheinlichkeit, Begrenzung der Beschleunigung der Rüstungsdynamik und ihrer Ursachen und Verringerung der Wahrscheinlichkeit von Präventivschlägen,
- Schadensbegrenzung bei bewaffneten Konflikten, Begrenzung des Umfangs von Leid, Tod und Zerstörung durch bestimmte Waffensysteme mit massivem Zerstörungspotenzial oder andere Waffen, die in großem Umfang eingesetzt werden können,
- Senkung der für Rüstung ausgegebenen Mittel.

Vor diesem Hintergrund betrachtet, enthalten konkrete Rüstungskontrollansätze die folgenden individuell festgelegten Maßnahmen, die in Form von Verträgen für bestimmte Waffen, Waffenteile und Waffentechnologien zwischen Staaten vereinbart werden:

- Transparenz über militärische Fähigkeiten,
- stabile und dauerhafte Kommunikation in den zwischenstaatlichen Beziehungen,
- Definition und Kontrolle quantitativer und qualitativer Grenzen für Waffentechnologien,
- Beschränkung oder Verbot der Verbreitung von Waffen, Waffenteilen oder Waffentechnologien,
- Festlegung spezifischer Überprüfungsmaßnahmen, die es Staaten ermöglichen, die Übereinstimmung anderer Vertragsparteien zu überprüfen.

Diese Ansätze sind nicht notwendigerweise kompatibel, da der Fokus in einer konkreten Situation immer von der Konfiguration und dem Niveau des politischen, wirtschaftlichen oder (erwarteten) militärischen Konflikts abhängt. Das ist auch wichtig im Hinblick auf die realistische Einschätzung der Möglichkeiten und der erwarteten Ergebnisse der Rüstungskontrolle in bestimmten Situationen. Rüstungskontrolle kann daher nicht mit Abrüstung gleichgesetzt werden, deren Ziel in jedem Fall in der konkreten Reduktion von Waffen bis hin zu deren kompletter Abschaffung liegt.

Maßnahmen der Rüstungskontrolle

Rüstungskontrollbemühungen sind fast immer ein allmählicher Prozess, dessen Erfolg oft nur vorübergehend ist und von den politischen Umständen und den verantwortlichen Akteuren abhängt. In vielen Fällen ist die Ausgangssituation geprägt von zwei oder mehr Vertragsstaaten mit einem gewissen Maß an Misstrauen oder Unsicherheiten hinsichtlich der gegenwärtigen oder geplanten militärischen Aktivitäten anderer Staaten, die als Bedrohungen wahrgenommen werden. Dazu zählen bspw. ein aggressives territoriales Verhalten sowie die qualitative oder quantitative militärische Bewaffnung. Neue militärisch genutzte Technologien und ein ggf. unzureichendes Verständnis ihrer invasiven oder zerstörerischen Fähigkeiten verschärfen solche angespannten Situationen. Die aktuellen Debatten über Cyberwaffen veranschaulichen diese Situation: Einerseits ist noch unklar, was genau Cyberwaffen im sicherheitspolitischen Kontext sind, und ob offensive militärische Handlungen im Zusammenhang mit dem Cyberspace dem üblichen Ansatz der Verwendung von „militärischer Gewalt" entsprechen. Ebenso ist international umstritten, wie militärische Cyber-Tools bewertet, verglichen und kategorisiert werden können um sie im Rahmen völkerrechtlicher Normen zu regulieren. Andererseits verdeutlichen internationale Studien die steigende Nachfrage der Streitkräfte nach Kapazitäten im Zusammenhang mit Cyber-Mitteln (UNIDIR, 2013).

Angesichts vergleichbarer Herausforderungen des Misstrauens, der Aufrüstung und der Gefahr von Konflikten durch Zufall oder aufgrund von Missverständnissen wurde bereits in der Zeit des Kalten Krieges das Konzept der *vertrauensbildenden Maßnahmen (CBM)* entwickelt. Diese Maßnahmen, die ursprünglich von der Konferenz für Sicherheit und Zusammenarbeit in Europa (KSZE) eingeführt wurden, beabsichtigen durch schrittweise und gegenseitige Zugeständnisse den Informationsaustausch und die Verringerung des militärischen Drucks eine Zusammenarbeit zwischen den Staaten herzustellen (CSCE, 1986). Ein wichtiges, niedrigschwelliges Element bildeten dabei oft unpolitische Gespräche über die technischen Aspekte der Sicherung von Waffen und der benötigten Einrichtungen, um auf diese Weise aktive Kommunikationskanäle zwischen gegnerischen Parteien aufzubauen, wobei der Schutz der jeweils eigenen Bevölkerung vor unerwünschten und zerstörerischen Auswirkungen von Waffentechnologien durch versehentliche Auslöser als kleinster gemeinsamer Nenner aller Staaten fungierte.

Neben der Anbahnung und Etablierung zwischenstaatlicher Beziehungen hängt die Stabilität von Rüstungskontrollabkommen außerdem entscheidend von Möglichkeiten ab, die Einhaltung

von Vereinbarungen gegenseitig zu überprüfen. Diese *Verifizierungsmaßnahmen* reichen dabei von Verfahren, die eine Kontrolle ohne Vor-Ort-Bewertung ermöglichen, wie Kameraüberwachung von relevanten Anlagen, Luftbildaufnahmen oder seismische Sensoren, über die strukturierte Erhebung und den Austausch von Daten zu Lagerbeständen und Handelsvolumen bis hin zu Vor-Ort-Inspektionen mit der Zählung und Messung von Lagerbeständen und der Überprüfung von versiegelten Einrichtungen.

Die Herausforderungen von Rüstungskontrollmaßnahmen im Cyberspace

Der Cyberspace als Domäne weist einige sehr spezifische Merkmale auf, die sich stark von den anderen Domänen wie Land, Luft und See unterscheiden. Dazu gehören die Virtualität dieser Domäne und der darin enthaltenen Informationen, die nicht physische Repräsentierung von Code und die nahtlose Duplizierung von Daten. Diese Merkmale stellen insbesondere für die praktische Seite von Rüstungskontrollvereinbarungen große Herausforderungen dar und unterminieren einen Großteil der etablierten Ansätze. Neben den technischen Schwierigkeiten beruhen diese Probleme auch auf den unterschiedlichen Auffassungen der Staaten hinsichtlich des Cyberspace und der Frage der staatlichen Souveränität in diesem Bereich. Unklar ist weiterhin die Frage, welchem internationalen Komitee oder Institution die Überwachung und Kontrolle der technischen Weiterentwicklung des Cyberspace übertragen werden kann, die seine langfristige friedliche Ausrichtung sicherstellt und in der die internationale Staatengemeinschaft gleichberechtigt vertreten ist. Eine ähnliche Herausforderung ergibt sich mit Bezug auf die Frage nach einer international legitimierten Institution, die mit der Untersuchung von mutmaßlichen Cyberattacken staatlichen Ursprungs betraut werden könnte, um nationale Einzelinteressen im Rahmen des *Blame-Game* auszugleichen (Davis II et al., 2017). Das derzeitige Fehlen einer international einheitlichen Klassifizierung von Cyberwaffen oder jeglicher Art von bösartigen Cyber-Hilfsmitteln verschärft diese Situation weiter, da die sich daraus ergebende Unberechenbarkeit ein „Gleichgewicht der militärischen Cybermächte" verhindert, bei dem Staaten zustimmen, militärische Fähigkeiten einheitlich und vergleichbar einzuschränken. Darüber hinaus handelt es sich bei Cyberwaffen oft um *One-Shot-Waffen*, die mit ihrem Einsatz ihre zukünftige Wirkung verlieren, indem sie ihre Angriffsvektoren offenbaren. In der Summe führt dies zu einer eher zurückhaltenden internationalen Debatte über die Offenlegung der Cyber-Kapazitäten von Staaten.

Erste Ansätze der Rüstungskontrolle im Cyberspace

Über die letzten Jahre ist das internationale Verständnis der Gefahren einer unkontrollierten Militarisierung des Cyberspace und der Notwendigkeit von Cyber-Rüstungskontrollmaßnahmen gewachsen. Nachfolgend sollen einige der Ansätze vorgestellt werden, die verschiedene Akteure auf verschiedenen Ebenen der zwischenstaatlichen Zusammenarbeit unternommen haben.

1. Die Wassenaar-Exportkontrollvereinbarung und ihre Erweiterung von 2013

Das *Wassenaar-Übereinkommen über die Kontrolle der Ausfuhr konventioneller Waffen sowie Güter und Technologien mit doppeltem Verwendungszweck* ist ein multilaterales System zur Kontrolle von Rüstungsexporten. Es wurde 1996 mit dem Ziel gegründet, die Transparenz des Handels mit Rüstungsgütern zwischen den inzwischen 42 Vertragsstaaten zu verbessern (Wassenaar, 2011). 2009 wurde die Regulierungs-Liste um solche Güter erweitert, die sowohl für zivile als auch für militärische Zwecke verwendet werden können. Die Mitgliedsstaaten verpflichten sich, den Export dieser kritischen Güter zu kontrollieren, Ausfuhranfragen zu prüfen und im Verdachtsfall wegen des Potenzials für sicherheitskritische oder menschenrechtsgefährdende Anwendung abzulehnen. Handelsdaten werden zweimal jährlich zwischen den Mitgliedstaaten ausgetauscht. Ende 2013 wurde die Vereinbarung durch die Aufnahme von *Intrusion-Software* (als eine Zusammenfassung von Überwachungs-, Spionage- und Sabotage-Software) in den Katalog der kritischen Güter erweitert. (Wassenaar, 2013). Eines der Probleme des Wassenaar-Abkommens ist jedoch seine Umsetzung, die in die Souveränität und Verantwortung jedes Mitgliedstaats fällt und unabhängig voneinander erfolgt. Entscheidungen und Ausfuhrkontrollen werden in den Mitgliedstaaten nicht einheitlich gehandhabt und für standardisierte Verfahren besteht keine Verpflichtung. Die kollektive Kontrolle der internationalen Verbreitung kritischer Güter, ein wesentlicher Bestandteil der klassischen Rüstungskontrollvereinbarungen, ist daher nur eingeschränkt möglich und erreicht keine allgemeine Gültigkeit. Dennoch könnte der Ansatz als Blaupause für einen potenziell globalen Ansatz zur Regulierung betrachtet werden, wenn er mit konsequenten und harmonisierten nationalen Ausfuhrgesetzen kombiniert und einer internationalen Kontrollinstanz wie einer UN-Organisation unterstellt wird.

2. Der Vorschlag des EU-Parlaments für eine EU-Verordnung zur Kontrolle der Ausfuhr von Gütern mit doppeltem Verwendungszweck von 2018

Auf der Grundlage des Wassenaar-Abkommens hat die Europäische Kommission begonnen, die weitere Regulierung solcher Waren im Rahmen eines einheitlichen Systems der Ausfuhrkontrolle für die EU-Länder zu erörtern (EU-Kommission, 2016a) voranzutreiben. Der Standpunkt des EU-Parlaments folgt dabei den Grundsätzen des Wassenaar-Abkommens über die Regulierung von Technologien, die zur Cyberüberwachung und Menschenrechtsverletzungen eingesetzt werden können (EU-Kommission, 2016b). Bei der Bewertung der Ausfuhrgenehmigung müssen die Mitgliedstaaten jedoch über die mutmaßliche Verwendung der Güter hinausgehend das Risiko einer Umgehung der festgelegten Regeln berücksichtigen. Die geplante Verordnung verfolgt außerdem einen Ansatz der *Catch-All-Kontrolle,* der die Regulierung auch für nicht explizit gelistete Technologieelemente ermöglichen sowie die Kontrolle zukünftiger, aktuell noch nicht berücksichtigter Entwicklungen umfassen soll. Neben dem Ansatz eines EU-weiten gemeinsamen Ausfuhrkontrollgesetzes wird ein System der Sorgfaltspflicht für Exportstaaten und den Exporteur selbst, sowie die Zuständigkeit für standardisierte Berichte über nationale Exportkontrollmaßnahmen vorgeschlagen. Dies soll die Schwäche des Wassenaar-Ansatzes aufheben, einer nationalen

Souveränität in Bezug auf die spezifischen Exportvorschriften und Berichterstattungsverfahren. Der Vorschlag des EU-Parlaments wird derzeit mit dem Rat der EU diskutiert.

3. Empfehlungen der Gruppe der Regierungsexperten der Vereinten Nationen aus dem Jahr 2015

Die Generalversammlung der Vereinten Nationen befasst sich seit 1999 in mehreren Beschlüssen mit dem zunehmend relevanten Thema des Cyberspace, seinem Potenzial für wissenschaftlichen und technologischen Fortschritt sowie seiner Nutzung für bösartige Zwecke. 2003 wurde dazu die Einrichtung einer Expertengruppe (UN GGE) beschlossen, die sich mit den Bedrohungen dieses Bereichs, aber auch den Chancen und Möglichkeiten der internationalen Zusammenarbeit im Bereich der Informations- und Kommunikationstechnologie befassen soll. Die letzte erfolgreiche Gruppe aus dem Jahr 2015 hat eine Reihe freiwilliger, unverbindlicher Normen für verantwortungsbewusstes Staatsverhalten empfohlen (UN GGE, 2015). Dabei wurde einerseits die staatliche Souveränität im Cyberspace betont, andererseits aber auch auf die staatliche Verantwortung bei Cyber-Aktivitäten verwiesen, die vom jeweiligen Staatsgebiet ausgehen:

Die Normen empfehlen den Staaten zusammenzuarbeiten, um schädliche IKT-Praktiken zu verhindern. Staaten sollten nicht wissentlich zulassen, dass ihr Territorium für international rechtswidrige Handlungen mit IKT verwendet wird. Kein Staat sollte IKT-Aktivitäten durchführen oder wissentlich unterstützen, die die Nutzung und den Betrieb kritischer Infrastruktur absichtlich beschädigen. Staaten dürfen die Informationssysteme der autorisierten Notfallteams eines anderen Staates nicht beschädigen oder ihre eigenen Teams nutzen, um sich an böswilligen internationalen Aktivitäten zu beteiligen. (Auszug aus UN GGE, 2015)

Diese unverbindlichen Normen wurden von der UN-Generalversammlung angenommen und mit dem Aufruf an ihre Mitgliedsstaaten verbunden, sich daran bei der Nutzung von Informations- und Kommunikationstechnologien zu orientieren. Auch die G20 hat ihren Staaten empfohlen, diese Empfehlungen umzusetzen (UNODA, 2017).

4. Vorschläge der OSZE für vertrauensbildende Maßnahmen

In den letzten zwei Jahren hat die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) zwei Entscheidungen erlassen, die sich auf „vertrauensbildende Maßnahmen zur Verringerung der durch die Nutzung von IKT bedingten Konfliktrisiken" beziehen. Die dafür von der Organisation entwickelten Maßnahmen sollen die „zwischenstaatliche Zusammenarbeit, Transparenz, Vorhersehbarkeit und Stabilität verbessern und (…) das Risiko von Fehlwahrnehmung, Eskalation und Konflikten verringern". Die Maßnahmen sind freiwillig, aber die OSZE hat ihre Mitgliedstaaten angewiesen, ihre politischen Entscheidungen, Gesetzgebung und ihr Verhalten auf diese Prinzipien zu stützen. Die meisten Vorschläge betreffen zwischenstaatliche Konsultationen, die Definition einer gemeinsamen Terminologie für den Cyberspace und seiner Bedrohungen sowie den Informationsaustausch in Bezug auf die Sicherheit und Nutzung von IKT sowie insbesondere die Risiken für kritische nationale und internationale IKT-Infrastrukturen und deren Integrität (OSZE, 2016). Obwohl diese Vorstöße *nur* das politische Verhalten von Staaten betreffen, sollten die Bemühungen als äußerst wertvoll angesehen werden. Die OSZE spielt als internationale Organisation eine wichtige Rolle, die Staaten verbindet, indem sie eine wichtige und etablierte Plattform für Dialog und Entscheidungsfindung bietet, die als Grundlage für Verhandlungen und weitere Vereinbarungen dienen kann.

5. Staatsgetriebene Vorschläge für staatliche Normen und Verantwortlichkeiten im Cyberspace

Neben den genannten multilateralen Ansätzen haben in den letzten Jahren auch verschiedene Staaten Vorschläge für verbindliche Normen und Regeln für das Verhalten von Staaten im Cyberspace entwickelt. Diese Vorschläge sind dabei jedoch zum Teil von nationalen außenpolitischen Prioritäten bestimmt oder spiegeln nationale Ansichten und Bedenken hinsichtlich der Souveränität des Staates und der inneren Sicherheit wider.

Ende Oktober 2018 unterbreiteten sowohl Russland als auch die USA jeweils zusammen mit anderen unterstützenden Staaten dem Ersten Ausschuss der Generalversammlung der Vereinten Nationen zwei getrennte Vorschläge zur Weiterentwicklung von Normen und Verantwortlichkeiten für das Verhalten von Staaten im Cyberspace. Beide Vorschläge betonen, dass Staaten Informationstechnologie nicht dazu verwenden sollten, Aktivitäten durchzuführen, die der Aufrechterhaltung des Weltfriedens und der internationalen Sicherheit entgegenstehen oder in die inneren Angelegenheiten anderer Staaten eingreifen. Der russische Vorschlag (UN, 2018a), der von 26 anderen Ländern, einschließlich China, unterstützt wird, bekräftigt dabei explizit die Empfehlungen der UN-GGE und definiert eine umfassende Liste an Grundsätzen für verantwortungsvolles Verhalten. Eine Besonderheit dieses Vorschlags besteht darin, dass er die staatliche Souveränität über den nationalen Anteil des Internets unterstreicht und daraus ein Recht der Staaten ableitet, alle Informationen prüfen und regulieren zu dürfen, die innerhalb nationaler IT-Systeme und IT-Netzwerken geteilt, übertragen, gespeichert und verteilt werden. Auch der von den USA geführte Vorschlag (UN, 2018b), der von 35 Nationen unterstützt wird, bestätigt Ergebnisse der UN-Expertengruppen. Er fordert dabei jedoch eine weitere Konzentration auf die Frage, wie das Völkerrecht auf die Nutzung von ITK durch den Staat angewendet werden kann, ohne dabei neue Räume nationaler Souveränität zu definieren, die mit der Redefreiheit und anderen Menschenrechten in Konflikt stehen.

Abschließend sollen zwei weitere Vorschläge erwähnt werden, die beide 2018 veröffentlicht wurden. Zum einen der von der französischen Regierung vorgestellte *Pariser Aufruf für Vertrauen und Sicherheit im Cyberspace* (France-Gov, 2018). Der unverbindliche Aufruf zielt darauf ab, bestehende institutionelle Mechanismen zur „Begrenzung von Hacking- und Destabilisierungsaktivitäten" im Cyberspace zu fördern und konzentriert sich auf Hauptaufgaben: Regulierung staatlicher Aktivitäten auf der Grundlage von Normen, staatliche Souveränität im Cyberspace und Schutz der Bürger. Das Dokument fördert eine umfassende und koordinierte Regulierung des Cyberspace, insbesondere die

Wahrung von Frieden und Sicherheit auf internationaler Ebene mit einer stärkeren Steuerung durch UN Gremien. Es erkennt die Anwendbarkeit des humanitären Völkerrechts auf den Cyberspace an, einschließlich der Menschenrechte und des Völkergewohnheitsrechts. Die Rolle und Verantwortung der staatlichen Akteure in Cyber-Konflikten soll gestärkt werden und aktive Cyber-Abwehrmaßnahmen von Unternehmen sollen ausgeschlossen werden. In gleicher Weise werden „offensive Operationen nichtstaatlicher Akteure" und der Einfluss ausländischer Staaten auf demokratische Prozesse wie Wahlen verurteilt. Das Dokument fordert, dass der „öffentliche Kern des Internets" vor feindlichen Akteuren geschützt wird, und fordert von der Industrie ein stärkeres Engagement für „Sicherheit durch Design" in Produkten und Dienstleistungen. Eine zweite Erklärung, die ähnliche Ziele verfolgt, ist die *Commonwealth Cyber Declaration* (Commonwealth, 2018), die auf dem Treffen der Regierungschefs aller Commonwealth-Staaten 2018 verabschiedet wurde. Die Erklärung ist im Hinblick auf die vielen kleineren und wirtschaftlich weniger relevanten Staaten relevant, die darin die Bedeutung des Cyberspace für ihre Nationen betonen, die Unversehrtheit dieser Domäne fordern und ein Mitbestimmungsrecht an deren Entwicklung zum Ausdruck bringen. Die Commonwealth Cyber Declaration ist daher zusammen mit den Maßnahmen der OSZE eines der stärksten zwischenstaatlichen Signale für eine friedliche Entwicklung des Cyberspace. Beide erkennen den Cyberspace als Grundlage nationaler wie internationaler sozialer, wirtschaftlicher und politischer Entwicklung an und betonen die Gefahren einer Destabilisierung des Cyberspace durch einseitige verdeckte Aktivitäten einzelner staatlicher Akteure.

Referenzen

Commonwealth. (2018) Commonwealth Cyber Declaration.

CSZE. (1986) Document of the Stockholm Conference on Confidence- and Security-Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Madrid Meeting of the Conference on Security and Co-operation, iss. 2. Retrieved from https://www.osce.org/fsc/41238?download=true

Davis II, John S., Boudreaux, Benjamin, Welburn, Jonathan William, Aguirre, Jair, Ogletree, Cordaye, McGovern, Geoffrey, & Chase, Michael S. (2017) Stateless Attribution: Toward International Accountability in Cyberspace. Rand. Retrieved from http://www.rand.org/pubs/research_reports/RR2081.html

EU-Kommission (2016a) Commission proposes to modernise and strengthen controls on exports of dual-use items

EU-Kommission (2016b) Regulation setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast). Retrieved from http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf

France-Gov (2018) Paris Call for Trust and Security in Cyberspace

Müller, H., & Schörnig, N. (2006) Rüstungsdynamik und Rüstungskontrolle: Eine exemplarische Einführung in die internationalen Beziehungen (Vol. Aussenpolitik und internationale Ordnung). Nomos. Retrieved from http://books.google.com/books?id=yphePQAACAAJ

OSCE (2016) Beschluss Nr. 1202 – Vertrauensbildende Massnahmen der OSZE zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben PC.DEC/1202. Retrieved from http://www.osce.org/de/pc/228501?download=true

Reinhold, Thomas, & Reuter, Christian (2019) Arms Control and its Applicability to Cyberspace. In Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 207–231). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4_10

UN-GGE (2015) Consensus report 2015 – Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – A/70/174 . Retrieved from http://undocs.org/A/70/174

UN (2016) Resolution adopted by the General Assembly on 23 December 2015. Retrieved from https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf

UN (2018a) Draft resolution by Russia and other states concerning the developments in the field of information and telecommunications in the context of international security

UN (2018b) Draft resolution by the USA and other states on advancing responsible State behaviour in cyberspace in the context of international security

UNIDIR (2013) The Cyber Index – International Security Trends and Realities. Retrieved from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Wassenaar (2011) Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies – Guidelines & Procedures,including theInitial Elements. Retrieved from http://www.wassenaar.org/guidelines/docs/5 – Initial Elements.pdf

Wassenaar (2013) The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies – List of dual-use goods and technologies and munitions list. Retrieved from https://www.wassenaar.org/app/uploads/2019/consolidated/WA-LIST%20%2813%29%201.pdf

Thomas Reinhold

Thomas Reinhold hat Informatik und Psychologie studiert und ist seit 2004 als Wissenschaftler und Freelancer für Software-Sicherheit tätig. Seit 2010 ist er Non-Resident Fellow am IFSH in der Projektgruppe IFAR² mit dem Forschungsschwerpunkt der Konsequenzen einer Militarisierung des Cyberspace und der Entwicklung von praktischen Maßnahmen der Friedenssicherung in dieser Domäne. 2015 leitete er die bundesweite Cyberpeace Kampagne des Vereins *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung* (FIfF e. V.). Als Experte für die Gefahren des Cyberwar und die Herausforderungen für Cyberpeace wurde er 2017 als Mitglied des *Transatlantischen Cyber-Forums* der *Stiftung Neue Verantwortung* sowie in die *Research Advisory Group* der *Global Commission on the Stability of Cyberspace* berufen. Darüber hinaus ist er seit vielen Jahren im Forschungsverbund *Naturwissenschaft, Abrüstung und internationale Sicherheit* (FONAS e. V.) aktiv und Mitglied der *Arms Control Association*.