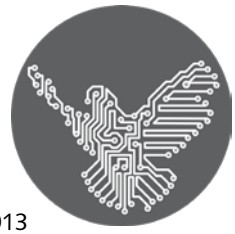
Hallo. Ich bin **Thomas Reinhold**, seit einigen Wochen Campaigner der Cyberpeace-Kampagne des FIfF, und möchte mich an dieser Stelle gern näher vorstellen. Ich bin Diplom-Informatiker mit einem Nebenfachstudium der Psychologie und beschäftige mich seit vielen Jahren mit den Themen Cyberpeace und den Problemen einer Militarisierung des Cyberspace. Seit 2009 bearbeite ich dieses weite Feld als wissenschaftlicher Fellow des Instituts für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH). Um mir die notwendige Flexibilität für eine solche Arbeit zu sichern, habe ich mich 2012 als freiberuflicher Software-Entwickler und Consultant selbstständig gemacht. Erfahrungen in politischen und öffentlichkeitswirksamen Kampagnen konnte ich unter anderem durch mein Engagement in diversen politischen und regionalen Initiativen (u. a. für Amnesty International und Pro-Asyl) sammeln. Darüber hinaus habe ich 2012 im Rahmen einer Projektanstellung im deutschen Büro von Greenpeace gearbeitet. Die Zeit im Elbspeicher hat es mir ermöglicht bei den „Kampagnenprofis" in die Lehre zu gehen und wichtige Kontakte zu knüpfen, die ich nun einbringen kann. Wer sich im Übrigen mehr für meine wissenschaftliche Arbeit interessiert, dem möchte ich die Seite *cyber-peace.org* empfehlen. Dort versuche ich wichtige Ereignisse dieses Themenfelds zu kommentieren und eine Datenbank mit Analysen und Hintergrundinformationen aller relevanten „Cybervorfälle" aufzubauen.

Ich freue mich, dass ich nun den FIfF bei seiner Kampagne unterstützen und mein Wissen einbringen kann und bin gern Ansprechpartner für Ideen, Fragen, Anregungen und Kritik.

Auf bald

Thomas / *thomas.reinhold@fiff.de*

Thomas Reinhold



Betrifft: Cyberpeace

Auswirkungen der Wassenaar-Kontrolle von Cyberwaffen

Seit den Erkenntnissen über *Stuxnet* und angesichts der NSA-Enthüllungen werden international wieder verstärkt die Möglichkeiten für die Kontrolle der Verbreitung von *Cyberwaffen* debattiert. Angesichts der zunehmenden Ausweitung der geheimdienstlichen und militärischen Aktivitäten auf den Cyberspace sind solche Maßnahmen ein wichtiger Bestandteil der politischen Einhegung des Konfliktpotenzials in den Kommunikationsnetzen und der internationalen Vertrauensbildung. Ein erster Schritt in diese Richtung wurde Ende 2013 mit der Erweiterung des *Wassenaar-Abkommens* gegangen, indem unter anderem *intrusion software* in den Katalog, der im Rahmen des Abkommens regulierten kritischen Güter aufgenommen wurde. Das *Wassenaar-Abkommen für Exportkontrollen von konventionellen Waffen und doppelverwendungsfähigen Gütern und Technologien*, dem mittlerweile 41 Mitgliedsstaaten beigetreten sind, wurde 1996 als Nachfolger des aus den Zeiten des kalten Krieges stammenden COCOM-Abkommens verabschiedet. Das Ziel des Übereinkommens ist die Vergrößerung der internationalen Transparenz und der Regulierung des Handels sowie die Eingrenzung der Verbreitung ursprünglich ausschließlich konventioneller Rüstungsgüter. 2009 wurde das Regelwerk um den Bereich der *Dual-Use*-Güter erweitert, als Produkte, die neben zivilen Zwecken auch für die Rüstung eingesetzt werden können. Die Mitgliedsstaaten des Abkommens verpflichten sich, den Export dieser kritischen Güter im Rahmen bestimmter Grenzen zu kontrollieren, Exportanfragen zu prüfen und bei Verdacht auf eine sicherheitspolitisch kritische oder menschenrechtsgefährdende Anwendung abzulehnen. Die Handelsdaten werden zwischen den Mitgliedsstaaten zweimal pro Jahr ausgetauscht.

Mit der neuerlichen Erweiterung von 2013 fällt erstmals Software in diesen Bereich staatlicher Rüstungskontrolle. Der Begriff der *intrusion software* wird spezifiziert als all jene Software, die für das verborgene Agieren entwickelt wurde, in der Lage ist, Daten zu entwenden oder zu modifizieren sowie ein Computersystem in seinen Ausführungsroutinen zu manipulieren oder zur Ausführung fremder Anweisungen zu bewegen. Diese Definition erscheint angesichts der Probleme, den etwas überstrapazierten Begriff der *Cyberwaffe* einzugrenzen, vordergründig sinnvoll gewählt. In erster Linie wird der Funktionsumfang einer Anwendung als hinreichendes Kriterium herangezogen, und weniger die möglichen Schäden oder das konkrete Einsatzumfeld berücksichtigt. Damit fallen jedoch auch Software-Tools unter die Regulierungsanforderungen, die für rein zivile Zwecke wie IT-Sicherheitsüberprüfungen und Penetrations-Test benötigt werden, also ausschließlich friedlichen Zwecken dienen. Die Etablierung von Prüfverfahren für den Export von *Dual-Use*-Gütern ist jedoch eines der wichtigsten Aufgabenfelder des *Wassenaar-Abkommens*, wird in den Handlungs- und Prüfrichtlinien umfassend behandelt und in Form von *Best-Practice*-Richtlinien kontinuierlich weiterentwickelt. Die Umsetzung dieser Maßgaben liegt in der Hoheit und Verantwortung der Mitgliedsstaaten, die jeweils unabhängig entscheiden. Für die Prüfung von Exportanfragen ist in Deutschland das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) beauftragt worden. Die deutschen Kontrollkriterien unterscheiden sich dabei hinsichtlich des Ziellands eines geplanten Exports. Exporte in EU-Mitgliedsstaaten, NATO-Staaten oder Staaten mit einem ähnlichen Status werden grundsätzlich genehmigt, sofern

nicht besondere politische Gründen dagegen sprechen. Exporte in andere Staaten werden grundsätzlich in Frage gestellt und mit Blick auf den potenziellen Käufer, den möglichen offenen und versteckten Einsatzzweck sowie die politische Lage und Stabilität im Zielland geprüft.

Eine Ankündigung der in Frankreich ansässigen Firma *Vupen* von Ende 2014 macht indessen deutlich, dass die Erweiterung des Regelwerks tatsächlich praktische Konsequenzen hat. *Vupen* ist eines der bekanntesten Unternehmen weltweit, die sich auf den Handel mit Schwachstellen und Sicherheitslücken in Software spezialisiert haben, und eigenen Aussagen zufolge ausschließlich staatliche Institutionen beliefern. Das Unternehmen, zu dessen Kunden zwischen 2011 und 2014 auch das BSI im Rahmen eines *Threat protection programs* gehörte, hatte nach der Erweiterung des Abkommens noch verkündet, ihre Aktivitäten den neuen Regularien anzupassen und die friedenspolitischen Ziele zu unterstützten. Mittlerweile hat *Vupen* jedoch beschlossen seinen Stammsitz aus Frankreich zu verlegen, da die „Verzögerungen französischer Behörden nicht länger [für uns] hinnehmbar, weil inkompatibel mit der Geschwindigkeit des Geschäftes [sind]". Die Deutlichkeit, mit der *Vupen*-Geschäftsführer Chaouki Bekrar die aus seiner Sicht störenden Genehmigungen als eine „Überdosis Bürokratie" abtut, deutet darauf hin, dass die französischen Behörden ihre Aufgabe ernst nehmen und die neuen Regularien greifen. Da in Frankreich genauere Kontrollen erst bei Exporten in Länder außerhalb der EU vorgesehen sind, weist dies möglicherweise auch auf den Kundenkreis von *Vupen* hin. Es ist jedoch strittig, ob diese Entwicklung wünschenswert ist.

Es ist für ein Unternehmen, dessen Wirtschaftsgut vor allem aus immateriellen Gütern und technischem Wissen besteht, leichter den Firmensitz zu verlegen, als dies für klassische Rüstungsfirmen mit umfangreichen Fertigungs- und Entwicklungsanlagen der Fall ist. Damit wird das Problem jedoch nur verdrängt und in Regionen ausgelagert, die sich einer effektiven Kontrolle entziehen. Im Fallen von *Vupen* wird der neue Stammsitz wohl in Singapur eingerichtet werden. Singapur ist kein Mitgliedsstaat des *Wassenaar-Abkommens* und *Vupen* unterhält dort bereits Zweigstellen. Neben diesem Effekt wird das Abkommen noch aus weiteren Gründen kritisiert. Zum einen liegt es in der Hoheit und Verantwortung jedes Mitgliedsstaates, die Regelungen und Vereinbarung konkret in nationales Recht umzusetzen und Kontrollziele, Verfahren und Prioritäten zu definieren. Damit fehlt dem Abkommen eine rechtliche Verbindlichkeit, und die unterschiedlichen nationalen Regelungen bilden keine einheitliche Bewertungs- und Rechtsgrundlage. Andere Mitgliedsstaaten haben bei Entscheidungen über Exporte keine Veto-Möglichkeiten und werden stets nur im Nachhinein über erfolgte Exporte informiert. Auch die Formulierung der *intrusion software* lässt offen, ob beispielsweise der Handel mit dem reinen Wissen über Sicherheitslücken unter das *Wassenaar-Abkommen* fällt, wenn es sich bei dem Export nicht um eine konkrete Software handelt, in der ein solches Wissen in Form eines *Exploits* eingebaut ist. Schließlich stehen internationale Abkommen der Rüstungskontrolle stets vor dem Problem der Handelsverschiebungen in den Schwarzmarkt, eine Tendenz die im Falle von immaterieller Software sehr viel einfacher umzusetzen und umso schwerer zu kontrollieren ist.

Zusammen genommen ist festzustellen, dass mit dem *Wassenaar-Abkommen* keine effektive Rüstungs- und Proliferationskontrolle möglich ist. Gleichwohl deuten die Bemühungen in eine richtige Richtung und die Erfahrungen mit dem Unternehmen *Vupen* zeigen, dass eine staatliche Kontrolle in jedem Fall wünschenswerter ist, als ein unkontrollierter Handel mit diesen *Cyberwaffen*.

FIfF e. V. – Pressemitteilung

Ganz großes Staatstheater

Die Geister, die ich rief, ich werd sie nicht mehr los

26. November 2014 – In dieser Woche wird im Deutschen Bundestag ein Staatstheater der besonderen Art aufgeführt, das es an Überheblichkeit und Wichtigtuerei mit Goethes *Zauberlehrling* aufnehmen kann. Die Beamten des Bundesnachrichtendienstes (BND) werden unseren [illegible] destag vorführen, wer sich ihrer [illegible] nicht zu verantworten, aber stets [illegible]

Am 28. November 2014 soll nach dem gegenwärtigen Stand im Deutschen Bundestag über die Haushaltsmittel beraten werden, mit denen der BND das Wissen von Kriminellen über geheim gehaltene Software-Schwachstellen – sogenannte *Zero-Day-Exploits* – aufkaufen will. Daraus soll Schadsoftware entwickelt werden, um Computersysteme im Ausland anzugreifen und zu sabotieren. Der BND hat bereits erklärt, „man müsse jetzt auf Augenhöhe mit anderen Diensten operieren". Dass NATO-Rechtsexperten eine staatliche Computersabotage als militärische Aggression mit erheblichen Eskalationsgefahren werten, wird seitens des BND verschwiegen.

Diese Woche soll dem *Focus* zufolge die Bundesanwaltschaft die Untersuchungen zur Überwachung des Handys der Bundeskanzlerin einstellen – mangels Beweisen. Bemerkenswert ist, dass weder die *Deutsche Telekom* noch das Telekommu- *logne* jene Sicherheitslücken in en konnten, durch die die NSA temen beider Unternehmen ab- dies durch die aktuellen Veröffentlichungen über den Trojaner *Regin*, der zu 28 % auf Backbones von Telekommunikationsunternehmen aufgetaucht ist und die Funktionalität hat, Aktivitäten und Daten in der infizierten Infrastruktur aufzeichnen und an den GHCQ bzw. an die NSA übermitteln soll. Die Telekom bestreitet laut *Spiegel-Online*, dass sie von *Regin* betroffen war. Dieses Dementi kommt verdächtig schnell. „Eine solche Analyse braucht deutlich mehr Zeit" kommentiert Kai Nothdurft, IT Sicherheitsexperte im FIfF-Vorstand.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de