Fachschaft Informatik, Hochschulstraße 10, 64289 Darmstadt

Herrn
Prof. Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

44,0. Konferenz der
Informatikfachschaften

c/o Fachschaft Informatik
Hochschulstraße 10
64289 Darmstadt

Datum
12. Mai 2016

Sehr geehrter Herr Prof. Dr. Lammert,

die 44,0. Konferenz der deutschsprachigen Informatikfachschaften[1] schließt sich dem Appell des FIfF e.V.[2] an und fordert:

- dass Deutschland auf eine offensive Cyberstrategie verzichtet,
- dass sich Deutschland verpflichtet, keine Cyberwaffen zu entwickeln, zu beschaffen und zu verwenden,
- dass internationale Abkommen zu einem weltweiten Bann von Cyberwaffen angestrebt werden.

Wir verstehen unter einer digitalen Waffe (auch „Cyberwaffe“) eine geheimgehaltene Software, Hardware oder Methode, die dazu bestimmt ist, IT-Systeme zu stören, zu beschädigen, für fremde Absichten zu missbrauchen oder in ihrer Integrität zu beeinträchtigen. Die Herstellung einer digitalen Waffe, also eines Werkzeuges zum Ausnutzen einer Sicherheitslücke eines IT-Systems, zeichnet sich durch die Geheimhaltung und den Erhalt derselben aus.

Ein Bann schlösse die Entwicklung, Herstellung und Verwendung sowie den Besitz von Cyberwaffen ein.

Begründung

Die Schaffung einer neuen Teilstreitkraft der Deutschen Bundeswehr im Rahmen des „Projekt Digitale Kräfte“ birgt große Gefahren. Sie ist ein Schritt in einem globalen IT-Wettrüsten, welches in einen digitalen kalten Krieg zu münden droht. In einem solchen würden alle Staaten gezwungen, immer besser ausgestattete Digitalstreitkräfte auszuheben, um im drohenden Konfliktfall nicht chancenlos zu sein. Immer mehr IT-know-how würde beim Militär gebündelt. Die Erkenntnisse über IT-Systeme und ihre Schwachstellen, die diese Streitkräfte gewännen, würden nie veröffentlicht und könnten deshalb der Gesellschaft nicht dienlich sein. Zivile

[1] Siehe: Wikipedia-Artikel *Konferenz der Informatikfachschaften* (`https://de.wikipedia.org/wiki/Konferenz_der_Informatikfachschaften`) und *Was ist die KIF?* (`https://kif.fsinf.de/wiki/Was_ist_die_KIF`)

[2] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, siehe `http://cyberpeace.fiff.de`

IT-Systeme blieben weiterhin schwach und stünden im Konfliktfall nicht mehr zur Verfügung. Komplexe Computerinfrastruktur, wie sie zum Beispiel in Krankenhäusern zum Einsatz kommt, fiele einem bewaffneten Konflikt in Sekunden zum Opfer, gefolgt von Kommunikation und digitalem Leben der Bevölkerung.

Einen nicht verwerflichen Krieg im digitalen Raum zu führen, ist ausgeschlossen. Genau wie der Einsatz atomarer, biologischer und chemischer Waffen ist auch der Einsatz digitaler Waffen mit großen zivilen Opfern verbunden. Der Grund: Bei Kampfhandlungen im digitalen Raum ist, sofern der Angreifer – und davon ist bei Nation-/State-Adversaries auszugehen – nicht naiv vorgeht, unmöglich festzustellen:

- ob das angreifende oder anzugreifende Gerät von einem staatlichen oder zivilen Akteur betrieben wird, und damit, ob ein potentielles Ziel einen Kombattanten oder Zivilisten darstellt,
- ob das Gerät allein zum Zwecke des Angriffs betrieben wird oder ob es sich vielleicht um ein von Unbeteiligten betriebenes Gerät handelt, welches lediglich für Zwecke des Angriffs missbraucht wird und
- wo der geographische Ursprung des Angriffes liegt.

Wird zum Beispiel das Smartphone eines deutschen Staatsbürgers angegriffen, kann nicht ausgeschlossen werden, dass bei einem Gegenschlag gewaltige zivile Opfer entstünden, weil der Angriff zum Beispiel seinerseits von einem Krankenhaus-Server oder einem internetfähigen Auto kommen könnte, die für diesen Zweck missbraucht werden. Der Schaden, der bei einem Gegenangriff entstünde, ist unberechenbar. Da die Verletzung der Integrität eines IT-Systems gewiss eine Beschädigung eines zivilen Objektes im Sinne des Römischen Statuts des Internationalen Strafgerichtshofes darstellt, sind die allermeisten von Kombattanten durchgeführten Störungen von IT-Systemen deshalb als Kriegsverbrechen im Sinne des dortigen Art. 8 Abs. 2b iv zu betrachten.

Aus den oben genannten Gründen sollte die Deutsche Bundeswehr per Gesetz daran gehindert werden, digitale Angriffe jedweder Art zu führen. Alle staatlich unternommenen Anstrengungen im Bereich der IT-Sicherheit sollten ausschließlich der sogenannten *Härtung* staatlicher und ziviler IT-Systeme dienen und somit auf das Auffinden von Sicherheitslücken abzielen, statt IT-Systeme fremder Staaten anzugreifen.

Aufgrund der globalen heterogenen IT-Infrastruktur betreffen diese Sicherheitslücken aber nicht nur staatlich betriebene IT-Systeme, sondern auch weltweit eingesetzte Geräte des digitalen Alltags, wie zum Beispiel Smartphones und Laptops; im Zeitalter des „Internet of Things“ sind sogar Kühlschränke und Autos mit dem Internet verbunden. Deshalb müssen alle Informationen über Schwachstellen in IT-Systemen, die durch die Deutsche Bundeswehr oder durch deutsche Nachrichtendienste und Strafverfolgungsbehörden gewonnen werden, nach ihrer Entdeckung so bald wie möglich der Öffentlichkeit zugänglich gemacht werden, um ein Härten auch nicht staatlich betriebener IT-Systeme zu ermöglichen und so einen Nutzen für die ganze Gesellschaft zu erzielen.

In Anbetracht stattfindender digitaler Kriegsoperationen wie „Stuxnet“, die – zum Beispiel im Rahmen der Wirtschaftsspionage – auch zivile Ziele betreffen, würden die (auch personellen) Mittel, welche gegenwärtig für eine neue Teilstreitkraft aufgewendet werden, besser in die Förderung oder Neuschaffung von Institutionen investiert, die IT-Sicherheitsforschung unabhängig von Militär und Nachrichtendiensten betreiben, um so die Sicherheit aller IT-Systeme zu fördern, statt zum digitalen Angriff zu rüsten.

Hochachtungsvoll,

die Teilnehmer*innen der
44,0ten Konferenz der Informatikfachschaften