

PRISM: Das Leben der anderen - total

Markus Lehner, *Neue Internationale* 181, Juli/August 2013

☒ Von den bürgerlichen IdeologInnen wird gern die Geschichte vom totalen Überwachungsstaat DDR erzählt und verschiedenste Beispiele der „unvorstellbaren“ Missachtung der Privatsphäre durch die Stasi beschworen. Doch hätte sich die Stasi in ihren kühnsten Träumen das Ausmaß an technischer Überwachung von Kommunikations- und Informationskanälen weltweit nicht vorstellen können, das jetzt durch den NSA-Überläufer Edward Snowden im Ansatz deutlich geworden ist.

Snowden

Am 6. Juni veröffentlichte der „Guardian“ einen ersten Artikel mit grundlegenden Informationen über das PRISM-Programm der NSA. Die NSA (National Security Agency) ist ein Spezial-Geheimdienst der USA, der seit den 1950ern auf die Überwachung von Kommunikations- und Informationssystemen spezialisiert ist. Er hat die weltweit größte Computer-Kapazität, was Möglichkeiten der Netzwerküberwachung, der Informationsspeicherung aber auch Kapazitäten zur Entschlüsselung und Informationsanalyse betrifft.

Mit über 35.000 AgentInnen und riesigen Rechenzentren (darunter ein Mega-Storage-Komplex in Utah, wo ein Großteil der Terrabits an Daten aus der Prism-Überwachung gesammelt werden soll) ist die NSA die unbestritten größte Schnüffelorganisation in den globalen Datennetzen.

Edward Snowden kam nach einer mäßigen CIA-Karriere als „Hacker“ und Consultant zum NSA, um dort als System-Architekt für Sicherheitsfragen zu arbeiten. Wie offenbar viele andere seiner KollegInnen wurde er durch eine Schulung zum System Prism gesendet, in der der Umgang mit diesem Datensammlungs-System gelehrt wird. Das „Verbrechen“ von Snowden, für das er nun um den halben Erdball gejagt wird, bestand einfach darin, die Powerpoint-Folien dieses Lehrgangs im Guardian zu veröffentlichen. Nicht diese Veröffentlichung – der Inhalt dieses Lehrgangs ist der Skandal!

Hintergrund

„Besonders perfide an den Regelungen ist, dass die Firmen auch dazu verpflichtet werden, auf jeden Fall zu leugnen, dass sie Daten an die NSA weitergeleitet haben.“ Nach dem 11. September versuchte die Bush-Administration zunächst vergeblich, ein vollständiges Überwachungssystem von Internet und Telekommunikationssystemen, die über die USA laufen, in Gang zu setzen. Dies scheiterte zunächst an den juristischen und organisatorischen Beschränkungen, die damals noch gegeben waren. Dies änderte sich mit dem 2007 beschlossenen „Protect America Act“ und dem 2008 in Gang gesetzten „FISA Amendmend of 2008“ (FISA ist ein halböffentliches Kontrollorgan speziell für den NSA).

Der Witz an diesen Regelungen ist, das nunmehr Privatfirmen, die der NSA ihre Daten zur Verfügung stellen, sich nicht mehr irgendwelcher Datenschutzvergehen oder ähnlichen zivilrechtlichen Problemen gegenüber sehen. Das Microsoft und Co. aufgrund der Datenlecks mit Strafzahlungen zu rechnen hatten, war nämlich zunächst das eigentliche Hemmnis, nicht irgendwelche Skrupel in Bezug auf die Verletzung der Privatsphäre!

Mit dieser rechtlichen Grundlage können nun Firmen aus dem Internet- und Telekommunikationsbereich mit Sitz in den USA dazu verpflichtet werden, ihre Daten offen zu legen

und haben auch beim Auffliegen dieser Tatsache mit keiner Konsequenz zu rechnen. Besonders perfide an den Regelungen ist, dass die Firmen auch dazu verpflichtet werden, auf jeden Fall zu leugnen, dass sie Daten an die NSA weitergeleitet haben. Diese beiden Verordnungen der Bush-Regierung wurden von der Obama-Administration nicht nur übernommen, sondern auch problemlos verlängert.

Was zeigen nun die Folien der Prism-Schulung, die Snowden veröffentlicht hat? Nicht mehr und nicht weniger, dass alle großen US-Internetfirmen ihre Server dem unmittelbaren Zugriff der NSA geöffnet haben. In der Folie sehen wir, wie die NSA stolz darstellt, ab welchem Jahr jeweils welche Firma ihre Server geöffnet hat.

Wir sehen, dass Mailaccounts, die bei Google-mail o.a. Anbietern hinterlegt sind, seit mehreren Jahren gleichzeitig auf den NSA-Servern in Utah gespeichert werden. Wir sehen auch, dass Facebook-Accounts seit 2009 dort „gesichert“ werden. Seit 2011 werden auch Skype-Gespräche mitgeschnitten.

Auf anderen Folien wird dargestellt, dass tatsächlich direkt von den Servern kopiert werden kann. Auch bei Skype-Gesprächen sollte man sich nicht sicher sein: die VoIP-Payload ist ein Datenstrom wie jeder andere und kann über die entsprechenden Ports abgezweigt und im Datenspeicher hinterlegt werden.

Doch nicht nur Mail, Facebook, Skype, Google und Youtube ist von der Datensammel-Leidenschaft der NSA betroffen. Schon längst läuft das globale Telefonsystem nicht mehr auf der alten ISDN-Technik, sondern ist in seinem Kernbereich Internet-basiert (nur noch ein Teil der alten Teilnehmeranschlüsse ist noch Alt-Technik, wird aber durch SIP-Technologie ersetzt). Damit wird auch ein großer Teil des Telefonverkehrs der unmittelbaren digitalen Überwachungstechnik geöffnet.

Um auch die nicht über die USA laufenden Verbindungen mitschneiden zu können, wurde die NSA dabei offenbar von ihren britischen Kollegen des GCHQ (Government Communication Headquarters) mit deren Spezialprogramm Tempora zur Überwachung des Backbones der internationalen Glasfaserverbindungen unterstützt. Damit kann man davon ausgehen, dass NSA und GCHQ sämtliche Internet- und Telefonverbindungen samt Accounts und in der globalen Server-Wolke verbreiteten Daten in ihren Systemen haben.

Imperialistische Konkurrenz

„Niemand sollte sich in der falschen Sicherheit wiegen, dass die ungeheure Datenmenge ja gar nicht auswertbar sei.“ Es ist natürlich wenig glaubhaft, dass ein derart globales und umfassendes Überwachungssystem zum Aufspüren von vielleicht 500 islamischen Terroristen dient, die sich zumeist wahrscheinlich gar nicht dieser Technologien bedienen. Nimmt man die zusätzlich aufgedeckten Überwachungssysteme hinzu, die z.B. in Richtung EU-VertreterInnen und Regierungen eingesetzt wurden, wird deutlich, dass es hier v.a. um inner-imperialistische Konkurrenz und politische Überwachung in Zeiten der Krise und der schwindenden US-Hegemonie geht.

Vornehmlich sollen Konkurrenten der US-Konzerne abgehört werden; ebenso mögliche Konkurrenten auf weltpolitischer Ebene. Aber im Fadenkreuz sind sicher auch politische Gegner in Protestbewegungen, Gewerkschaften und der Linken. Ein besonderes Licht wirft die systematische Überwachung von Facebook auf die gleichnamigen „Facebook-Revolutionen“ und das Agieren der USA dabei.

Niemand sollte sich in der falschen Sicherheit wiegen, dass die ungeheure Datenmenge ja gar nicht auswertbar sei. Der größte Teil der Investitionen in diese Überwachungssysteme sind gar nicht die eher trivialen Mechanismen zur Datenbeschaffung und Speicherung. Der größte Aufwand wurde in den letzten Jahren in die Analyse-Systeme gesteckt. Dies reicht vom „Data-Mining“ (Methoden zur intelligenten Suche in „big data“-Systemen), über den Einsatz von Methoden der „künstlichen Intelligenz“ (wie etwa dem kontext-abhängigen Datenanalyse-Systemen von Systemen wie Watson), über „Stream“-Systeme (die direkt aus dem Datenstrom in intelligenter Weise nach „verdächtigen“ Inhalten filtern und dabei längst nicht mehr nur auf einzelne „Schockwörter“ reagieren).

Konsequenzen

Man kann davon ausgehen, dass NSA & Co die Informationen, nach denen sie suchen, in den Datenmengen auch sehr schnell finden können. Die Frage ist nur, wer in ihr Fadenkreuz gerät und für sie interessant erscheint. Manchmal werden auch völlig harmlose Liberale dabei gescannt und erledigt, wie das Beispiel einer US-Anwältin zeigt, die zufällig einen „Terror-Verdächtigen“ als Pflichtmandanten hatte, und seither systematisch ruiniert wurde.

Als Betroffene dieses Systems der totalen Überwachung müssen wir als Linke Konsequenzen ziehen. Dies reicht von der Verwendung starker Verschlüsselung bis hin zum bewusst vorsichtigen Umgang mit den „sozialen Netzwerken“ im Internet. Allgemeine Paranoia ist sicher nicht angebracht, aber in kritischen Momenten sollten wir die öffentliche Kommunikation über diese Netzwerke vermeiden. Der Umgang mit Überwachungssystemen ist in der Geschichte der Arbeiterbewegung nicht neu. Wir sollten hier auf historische Erfahrungen zurückgreifen.

„Whistleblower“ wie Edward Snowden spielen eine wichtige Rolle, um überhaupt zu erfahren, was in diesen Agenturen vor sich geht. Daher müssen wir ohne Wenn und Aber ihre Straffreiheit und Reisefreiheit verteidigen. Wir brauchen mehr Snowdens - und genau deswegen wollen ihn die Schergen des US-Systems offenbar um jeden Preis in ihre Gewalt bekommen. Dies darf ihnen nicht gelingen! Daher: Sofortiges Asyl für Snowden!

Schließlich müssen die Enthüllungen von Snowden zu einem weltweiten Protest gegen das Schnüffelsystem NSA/GHCO u.a. Staaten - nicht zuletzt auch der BRD - führen. Diese Institutionen und ihre Programme müssen sofort geschlossen werden! Alle gemeinen Unterlagen, Verbindungen, Anweisungen und Verträge von Diensten, Regierungen und Unternehmen müssen öffentlich gemacht werden. Die gesammelten Daten und Techniken müssen von ExpertInnen, die das Vertrauen der Arbeiterbewegung und der sozialen Bewegungen genießen, kontrolliert und die Datensammlungen gelöscht werden.

Bild: LATUFF

2013, <http://latuffcartoons.wordpress.com/2013/06/10/cartoon-dincao-barackobama-is-watching-you-prism/>