Seminarbericht Helmstedt 2015
Bedrohung unserer Sicherheit: Der „gläserne“ Bürger
Geheimdienste- ihr Arbeiten und ihr Wirken
23.03.-26.03.15 an der Politischen Bildungsstätte Helmstedt

Wir wissen: Die Digitalisierung von Daten ist heute unverzichtbar geworden. Aber wissen wir auch, wie viele Gefahren für uns damit verbunden sind?
Aus der Fülle der Informationen während unseres Seminars ein Beispiel: Mitarbeiter des Verfassungsschutzes befassen sich seit Jahren schwerpunktmäßig mit Wirtschaftsspionage. Sie informieren Betriebe kostenfrei, neutral und vertraulich über Schutzmaßnahmen. Das ist nötig geworden, weil der Konkurrenzdruck unter den Firmen und Nationen weltweit immer größer, Wirtschaftsspionage durch digitalisierte Daten aber immer einfacher wird. Die gewünschten Daten sind leicht und risikoarm zu beschaffen. „Schnüffelprogramme“ können jeden Tastendruck bei der Arbeit am Rechner erfassen und leiten Daten sofort und unbemerkt an den Auftraggeber weiter. Manipulierte Hardware erfüllt denselben Zweck. Hochintelligente „Schädlinge“, von denen täglich etwa 20.000 neu auftauchen, können zerstörerisch auf die Rechner kompletter Betriebe wirken. Hacker sind in der Lage, durch Eindringen in betreffende Betriebssysteme etwa die Wasser- oder Stromversorgung ganzer Städte und Landstriche lahmzulegen. Der Verfassungsschutz empfiehlt deshalb Firmen dringend, neben großer Vorsicht im Umgang mit sensiblen Daten auch auf sicherheitsorientierte Personalauswahl zu achten. In allen Ebenen eines Unternehmens verfügen Mitarbeiter über schützenswertes Wissen, an das Nachrichtendienste oder Konkurrenten oft nur mit deren Hilfe gelangen können. Weit mehr als die Hälfte der Industriespionagefälle erfolgt durch eigene Mitarbeiter! Durch die geringe Größe der Datenspeicher ist Datenschmuggel praktisch nicht zu verhindern. Es entstehen schnell riesige Schadenssummen für die betroffenen Firmen, die Aufklärungsrate ist dagegen sehr gering.

Das Internet lässt sich auch als Waffe gebrauchen – im sogenannten Cyberwar oder treffender ausgedrückt: in elektronischer Kampfführung. Dabei wird versucht, den Gegner mit Hilfe der Steuerungstechnik zur Erfüllung des eigenen Willens zu zwingen. Dieser Gegner soll derart entwaffnet werden, dass er politisch hilflos und militärisch wehrlos ist. Bisher gibt es keinerlei internationale Verträge, die Cyberaggressivität regeln. Cyberwar kann ein bisher gültiges Paradigma in der Kriegsführung verändern, dass es nämlich einfacher ist zu verteidigen als anzugreifen. Ein Verteidiger muss alle Systeme erfolgreich verteidigen, während der Angreifer nur eine einzige Sicherheitslücke finden muss. IT Systeme aber sind zu komplex, um komplett auf Sicherheit überprüft werden zu können. Aktuell lässt sich allerdings noch kein Gegner via Internet bezwingen. Gefährlich wird es jedoch, wenn eine Cyberattacke mit konventionellen Maßnahmen (Waffen) beantwortet wird.
Einige Beispiele aus dem Bereich Cyberkriminalität, also der planmäßigen Begehung von Straftaten zu Gewinn- und Machtstreben, verdeutlichten, dass diese im Gegensatz zu elektronischer Kampfführung zurzeit die größere Gefahr darstellt. Dazu gehören Angriffe auf Industriesteuerungsanlagen oder Versorgungsnetze -wie geschehen- mit manipulierten USB-Sticks, die als Werbegeschenke (Stuxnet)verteilt worden waren. Sie haben immense Schäden verursacht. Diese Angriffe können selten strafrechtlich verfolgt werden, da die Täter in der Regel vom Ausland aus agieren.
Die Frage „Cyberterrorismus – reale Bedrohung oder Mythos?“ ließ sich nicht umfassend beantworten, da die bisherige Forschungslage zur systematisch

vorbereiteten Planung und Durchführung illegaler Vorgänge (z.B. zur Abschaffung bestehender Herrschaftsverhältnisse) nicht ausreicht.
Unsere Gesellschaft wird immer abhängiger von Informationstechnologie, aber wie sieht es mit der Datensicherheit aus? Ist der Bürger „gläsern“ geworden? Durch die alltägliche Nutzung von Handy, Smartphone oder Paybackkarte hinterlassen wir tatsächlich eine Datenspur. Trotz des Datenschutzgesetzes kann sich der Bürger nicht dagegen wehren, weil im Detail nicht nachvollziehbar ist, wer was wem weiter gegeben hat. Jeder Nutzer des Internets sollte bei der Wahl von Passwörtern und bei ihrer Verwendung Vorsicht walten lassen. Bei allen Bewegungen im Internet weiß niemand, wer vielleicht noch diese Informationen unbemerkt nutzt.

Auf unserer Tagesexkursion nach Berlin war der Bundesnachrichtendienst unser erstes Ziel. Er ist der einzige Auslandsnachrichtendienst der Bundesrepublik und arbeitet im Auftrag der Bundesregierung. Hier werden wirtschaftliche, politische und militärische Informationen gesammelt und ausgewertet, quasi als Dienstleistung für Bundesregierung, Ressorts und Bundeswehr. Der BND arbeitet oft im Geheimen und Verborgenen, doch „…stets im Rahmen der gesetzlichen Vorschriften und für die Sicherheit Deutschlands.“
Nachmittags folgte der Besuch der Gedenkstätte „Stasi-Gefängnis -Hohenschönhausen“, das bis Ende 1989 als zentrale Untersuchungshaftanstalt des Staatssicherheitsdienstes der DDR gedient hat. Die Führungen werden ehrenamtlich von ehemaligen Häftlingen vorgenommen und lassen beim Besucher noch heute die beklemmende Atmosphäre von Angst und katastrophalen Haftbedingungen entstehen. Auf dem Flur mit den zahlreichen Vernehmungsräumen herrschte sogar noch der typische DDR-Geruch. Statt mit physischer Gewalt setzte man den Häftlingen mit psychologischen Methoden zu. Sie sollten dadurch das Gefühl erhalten, ohnmächtig einem allmächtigen Staat ausgeliefert zu sein.

Abends wurde in der Kellerklause angeregt über die vielfältigen Tageseindrücke diskutiert, es gab aber auch noch weitere Programmangebote. Der auf Wunsch des DFR gezeigte Filmbeitrag über Salafismus war informativ, wirkte jedoch nicht sehr beruhigend…
Die abendliche Stadtführung durch Helmstedt war besonders auf die schönen alten Professorenhäuser und ihre ehemaligen Bewohner ausgerichtet - Zeugnisse der Zeit, in der Helmstedt mit seinem Juleum eine angesehene Universitätsstadt war.

Wie an der PBH üblich war das gesamte Seminar einschließlich der Exkursion sehr gut organisiert. Alle Referenten haben uns ihren nicht immer einfachen Stoff so anschaulich vermittelt, dass wir ihnen jederzeit gespannt gefolgt sind. Wir werden in Zukunft wohl weniger sorglos im Internet unterwegs sein oder Datenspuren hinterlassen (z.B. Paybackkarte) als vielleicht noch vor diesem Seminar. Und die neue Barbiepuppe, die im Kinderzimmer zwecks interaktiver Kommunikation Daten über ihre Besitzerin sammelt, diese aber auch an ihre Herstellerfirma weiter gibt, werden wir gewiss nicht verschenken!

Brigitte Schulz, Hameln