Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

Cloud-Anbieter für Bundeswehr, CIA und Pentagon

Update: Cyber Valley und Tübingens Transformation in einen Rüstungsstandort

von Christoph Marischka

Anfang Juli veröffentlichte die Informationsstelle Militarisierung eine Analyse, in der gewarnt wurde, das Projekt Cyber Valley werde die Stadt Tübingen und die umliegende Region in einen Rüstungsstandort transformieren. Diese Warnung wurde von Sprecher_innen des Cyber Valleys und dem Redaktionsleiter des Schwäbischen Tagblatts (ST) zurückgewiesen[1]. Wenige Wochen später berichtete das ST über die Kundgebung zum Antikriegstag am 1. September 2018.[2] Ein dort gehaltener Redebeitrag unterstrich, dass Bundeswehr und das Verteidigungsministerium bei der Cyber-Kriegführung und im IT-Bereich massiv auf externe Expertise angewiesen seien und diese auch bei kleinen und mittelständischen Betrieben sowie über Beraterverträge einkaufen würden. In diesem Kontext nannte der Bericht des ST auch das – bereits zuvor von der IMI angesprochene – Tübinger Unternehmen Syss, das auf Penetrationstests spezialisiert ist und die Bundeswehr auf seiner Homepage als „Referenz“ nannte.

Ambivalent: Syss

In der Folge veröffentlichte das ST ein wohlwollendes Interview mit dem Geschäftsführer der Firma Syss, in dem dieser angab, mit dem Militär habe das Unternehmen so gut wie nichts zu tun. In dem Interview positionierte sich der Geschäftsführer der Firma zugleich gegen Cyberkriegführung und eine entsprechende Aufrüstung der Bundeswehr.[3] Konkret sprach er sich gegen staatliches Hacken und das Horten von Sicherheitslücken aus, was die Voraussetzung für offensive Cyber-Kapazitäten darstellt. Im Anschluss kontaktierte er die IMI und lud Vertreter*innen zum Gespräch. In diesem Gespräch nannte er als Ziel seines Unternehmens, „den Kunden den Rücken zu stärken“. Außerdem verwies er auf die Problematik, Rüstungsunternehmen von anderen Unternehmen zu unterscheiden. Die Tätigkeit seines Unternehmens für die Bundeswehr habe lediglich in zwei oder drei Vorträgen bestanden, die er selbst vor einigen Jahren gehalten habe; unter den tausenden Unternehmen, für die man arbeite, sei dies marginal. Von unserer Seite wurde daraufhin kritisiert, dass die Bundeswehr als marginaler Geschäftspartner unter tausenden trotzdem auf der ausgewählten Liste der Referenzen geführt wird. Dies bestätigt aus unserer Sicht einerseits das militärische Interesse an einer Zusammenarbeit mit IT-Firmen und normalisiert diese zugleich: Wenn es sich nur um wenige Vorträge gehandelt habe, müssten diese ja nicht ausgerechnet als Referenz genannt werden. Die Liste der Referenzen sei ohnehin veraltet und werde überarbeitet, wurde uns zugesagt, knapp zwei Monate später wird die Bundeswehr hier aber aktuell immer noch genannt.

ATOS: Verwalter der Bundeswehr-IT

Wie bei Syss, so handelt es sich auch bei ATOS – soweit ersichtlich – nicht um einen offiziellen Partner des Cyber Valleys. Anders als beim Tübinger Start-Up Syss ist ATOS jedoch ein großer, transnationaler Konzern mit engen Bindungen an die Rüstungsindustrie. ATOS hat sich Mitte 2016 – wenige Monate vor der Gründung des Cyber Valleys – durch die Übernahme des Tübinger Start-ups Science&Computing einen Standort in Tübingen erschlossen. Die Kompetenzen der Tübinger Niederlassung von ATOS bestehen seither u.a. in High-Performance-Computing und Messdatenmanagement. Die vorangegangene Übernahme des Tübinger Unternehmens entspricht der Strategie von ATOS, Firmen, Patente und Kompetenzen im IT-Bereich aufzukaufen und sich dadurch ein Quasi-Monopol bei der Systemintegration für IT-Projekte von Regierungen und Unternehmungen in vergleichbarer Größenordnung zu schaffen. Denn vielmehr noch als Bauprojekte erfordern große IT-Projekte v.a. Überblick über die am Markt verfügbaren Angebote in unterschiedlichen Bereichen: Speicher- und Rechenkapazität, Software und ihre verschiedensten Komponenten, Datenübertragung und Verschlüsselung sowie ein Management der Zugriffsrechte der hunderten bis tausenden Beteiligten. ATOS beobachtet diese Aktivitäten und kauft Unternehmen auf diesem Markt in großem Maßstab ein. ATOS wurde dabei massiv unterstützt durch die EU-Forschungsprogramme FP7 und Horizon2020, als deren fünft-größter Nutznießer der Konzern gilt. Die idealtypische Struktur dieser Projekte besteht darin, verschiedene Sensoren miteinander zu vernetzen, erfasste Ereignisse mit Einträgen aus bestehenden Datenbanken anzureichern und in einem oder mehreren Lagezentren für Menschen verständlich darzustellen – sowie die jeweilig dazugehörende sichere Datenübertragung.

Vor diesem Hintergrund ist es wenig überraschend, dass ATOS als Hauptauftragnehmer des „Projektes zur Harmonisierung und Migration der Führungsinformationssysteme (HaFIS) der Bundeswehr“ fungiert und bereits jetzt die zentralen Rechen- bzw. Datenzentren der Bundeswehr betreut. Kurz gesagt: ATOS ist der bzw. ein unumgänglicher Anbieter für die Cloud-Dienste der Bundeswehr, also für die Bereitstellung jener Strukturen, über die zukünftig die Kräfte im Feld mit ihren Kommandos und die autonomen Systeme im Einsatz zur Entscheidungsfindung mit Datenbanken verbunden sein werden.

AMAZON: Cloud-Verwalter der CIA und zukünftig des Pentagons

Anders wiederum als ATOS handelt es sich bei Amazon um einen offiziellen Partner des Cyber Valley. Amazon stellt (zumindest) seit 2013 Cloud-Dienste für den US-Auslandsgeheimdienst CIA bereit – soweit bekannt beträgt das Auftragsvolumen 600 Mio. US$. Damit gilt Amazon als unangefochtener Favorit bei der Vergabe des nächsten, wirklich großen Projekts des Pentagons, der „Joint Enterprise Defense Infrastructure“ – kurz JEDI. Das Volumen des Vertrages wird auf 10 Mrd. US$ geschätzt – die daraus bereits mittelfristig entstehenden Profite dürften deutlich höher liegen. Denn JEDI ist nicht einfach nur ein neues Kommunikations- und Infrastrukturprojekt des Pentagons, sondern auch ein Beispiel dafür, dass die Digitalisierung des Krieges nicht ohne (pseudo-)private Konzerne machbar ist. Ein Konzern, der alltäglich in großem Maßstab Daten über seine Nutzerinnen und seine Arbeitnehmer in beispielloser

Weise überwacht, managt zugleich die Datenverwaltung für Militär und Geheimdienste. Zugleich stellt er offenbar die von ihm gesammelten Daten dem Cyber Valley zur Verfügung, wo man darauf hofft mit deren experimenteller Verarbeitung Sprunginnovationen im Bereich der Künstlichen Intelligenz zu realisieren. So berichtet das ST über die Vorteile der Beteiligung von Amazon am Cyber Valley: „Wissenschaftler, die wie die Tübinger Max-Planck-Forscher über Algorithmen forschen, [müssen] diese an großen Mengen von Realdaten testen können. Die gibt es insbesondere bei Firmen wie Amazon oder Google, die über ihre Geschäftskunden Daten sammeln. Alleine um diese Realdaten zu erhalten – wenn auch in hochaggregierter und anonymisierter Form – schließen viele wissenschaftliche Einrichtungen Kooperationen mit Firmen ab, so Ferdi Schüth, Vize-Präsident der Max-Planck-Gesellschaft.“[4]

Fazit

Eine Antwort darauf, wie das Cyber Valley verhindern will, dass entsprechende (auch aus unseren Nutzer*innendaten gewonnene) Erkenntnisse wiederum Eingang in die militärische Datenverarbeitung finden, die von ATOS und Amazon angeboten wird, bleiben die Beteiligten schuldig. Knapp zwei Jahre nach der Gründung des Cyber Valley und nur wenige Monate nach einer ersten kritischen Auseinandersetzung ist unbestreitbar, dass die wichtigsten Anbieter von Cloud-Services der Bundeswehr, des CIA und des Pentagons in der überschaubaren Stadt Tübingen Niederlassungen etabliert haben. Wer dennoch keine „Transformation zum Rüstungsstandort“ erkennen will, sei aufgerufen, dies zu begründen.

Anmerkungen

1 Christoph Marischka: Das Cyber Valley in Tübingen und die Transformation zum Rüstungsstandort, IMI-Analyse Nr. 18/2018. Zur Reaktion des Tagblatts und der Antwort des Autors hierauf: „Offener Brief an Gernot Stegert, Redaktionsleiter des Schwäbischen Tagblatts, betreffend der Berichterstattung zum Cyber Valley“, www.Tueinfo.org vom 27.7.2018.
2 „Aufrüstung schadet allen“, Schwäbisches Tagblatt vom 3.9.2018.
3 „‚Hände weg von Cyber-Kriegen‘“, Schwäbisches Tagblatt vom 6.9.2018.
4 „Max-Planck-Forscher und Firmen wollen Innovations-Ökosystem für künstliche Intelligenz schaffen“, Schwäbisches Tagblatt vom 2.5.2018.

iBorderCtrl – EU erprobt künstliche Intelligenz zur Grenzüberwachung

Mit der Technologisierung der Grenzüberwachung geht auch eine kontinuierliche Einbindung von maschinellem Sehen und Hören einher. Etliche Staaten verwenden bereits KI zur Grenzüberwachung: u.a. die USA, Südkorea, Indien, Simbabwe und Israel. Die EU probt zurzeit das mit 4,5 Millionen Euro finanzierte System iBorderCtlr, an dessen Entwicklung sich auch die Leibniz Universität Hannover beteiligt. Das mittlerweile auch als „Lügendetektor“ betitelte Projekt ist jedoch vielmehr als das. Es gliedert den Grenzkontrollablauf in zwei Phasen: Die erste erfolgt noch vor der Abreise durch ein Online-Gespräch mit einem virtuellen Grenzschutzbeamten. Dieser stellt u.a. Fragen zu dem Inhalt des Gepäcks und der Reisemotivation. Die Stimme und das Gesicht der reisenden Person werden dabei analysiert und gespeichert. Die notwendigen Reisedokumente werden gescannt und ebenfalls zu ihrer Überprüfung hochgeladen. Die zweite Phase erfolgt bei dem Grenzübertritt selbst. Sollte die erste Phase einen Verdacht geweckt haben, wird die einreisende Person intensiver von Grenzschützer_innen untersucht und befragt. Zwar wertet das Programm bis zu 38 Mikroausdrücke, u.a. Mikromuskelbewegungen, aus, um mit Hilfe von auf Künstlicher Intelligenz basierender Programme zur Mustererkennung ein auffälliges Verhalten zu identifizieren, welches laut Entwickler_innen des Projekts als Indikator für eine Lüge dienen könne.

Alleine diese Prämisse sei laut dem Kriminologen Bennett Kleinberg vom University College London „pseudowissenschaftlich“, denn das Erkennen einer Beziehung zwischen nonverbalen Mikroexpressionen und dem Erzählen einer Lüge sei sehr umstritten. Doch abgesehen von diesem Automatic Deception Detection System (ADDS), umfasst das Projekt auch zwei biometrische Module: Fingerabdrücke und Handvenenerkennung, bei der das in den Händen verlaufende Venenmuster durch Nahinfrarotlicht gescannt wird. Erstere biometrische Daten werden dann mit bereits bestehenden Datenbanken abgeglichen und mit den Venenmustern wird eine „baseline“ Datenbank angelegt. Eingebunden in das Projekt ist auch das Face Matching Tool – das Werkzeug zum Gesichtsabgleich –, mit dem die vor der Abreise erfolgten Bild- und Videoaufnahmen mit denen am Grenzübergang verglichen werden. Weitere Bestandteile beinhalten das Document Authenticity Analytics Tool (DAAT) zur Überprüfung der Dokumente sowohl vor der Einreise als auch bei der Einreise selbst, um ihre Echtheit zu überprüfen. Interessant ist auch das Hidden Human Detection Tool (HHD), welches versteckte Menschen – vermutlich mit Hilfe eines Radars – in Fahrzeugen, Zugwaggons und Containern aufspüren will. Erschreckend ist auch die beabsichtigte Einbindung einer Auswertung der von der kontrollierten Person benutzten sozialen Medien und die im SIS II (Schengener Informationssystem II) gespeicherten Daten. Bis jetzt gibt es keine genaueren Informationen, was eine solche Überprüfung der sozialen Medien beinhaltet, welchen Zeitraum diese Überprüfung umfasst und wie dies mit dem Datenschutzrecht zu vereinbaren ist.

Kurzum, das iBorderCtrl-Projekt sammelt sensible Daten von Migrant_innen, die sich gegen diese Erhebung schlecht wehren können und droht die Überquerung von Grenzen, die für viele Menschen überlebensnotwendig ist, von bislang stark fehlerhaften Algorithmen abhängig zu machen und das natürliche Phänomen der Migration zu einem computerisierten Verfahren zu reduzieren, indem die beteiligten Sicherheitsbehörden ihre Verantwortung an solche Systeme abtreten können, deren Fehlerquote im Falle von iBorderCtrl bislang bei 24% liegt. Es zeichnet sich eine hochgefährliche Entwicklung ab, die einerseits die für viele Menschen überlebenswichtige Klandestinität erschwert und andererseits droht, die Verantwortung für Entscheidungen, die ebenfalls lebenswichtig für die Betroffene sind, an Algorithmen abzutreten, denen eine gewisse Neutralität und Intelligenz unterstellt wird, obwohl sie eine hohe Fehlerquote aufweisen und ethisch stark bedenklich sind.

Jacqueline Andres