AG Interdisziplinäre Sicherheitsforschung

Freie Universität Berlin

Dahlemer Rundgespräche „Sicherheitsforschung“

der Freien Universität Berlin

Kontrast oder Symbiose? Sicherheitsforschung im Spannungsfeld zwischen Technik und Gesellschaft

Zusammenfassung der Ergebnisse

Datum: **20. Juni 2017, 17 Uhr**
Ort: **Einstein Zentrum Digitale Zukunft, Wilhelmstr. 67, 10117 Berlin**

Einleitung

Sicherheit ist ein universelles Gut, das sich in allen Gesellschaften manifestiert und zunehmend zentraler wird. Im Mittelpunkt der Veranstaltung standen gesellschaftliche Veränderungsprozesse unter dem Gesichtspunkt der Sicherheit. Daher adressieren die DAHLEMER RUNDGESPRÄCHE SICHERHEITSFORSCHUNG die gesamte Breite des Sicherheitsbegriffs und fördern den Diskurs über Sicherheit vom technisch Möglichen bis zum gesellschaftlich Akzeptierten.

Die DAHLEMER RUNDGESPRÄCHE SICHERHEITSFORSCHUNG fanden bereits zum zweiten Mal statt. Bei der ersten Veranstaltung im Jahr 2016 stand die Vernetzung der Akteur_innen innerhalb der Freien Universität Berlin im Vordergrund. In der zweiten Veranstaltung lag nun der Fokus auf der Vernetzung von Expert_innen der Sicherheitsforschung in der Region Berlin-Brandenburg.

Ziel der DAHLEMER RUNDGESPRÄCHE SICHERHEITSFORSCHUNG ist es, gemeinsame wie konflikthafte Positionen auf das komplexe Zusammenspiel zwischen technischen Innovationen und sozialem Wandel herauszuarbeiten und vor dem Hintergrund der in den beteiligten Disziplinen und Institutionen betriebenen Sicherheitsforschung zu reflektieren. Daneben war es ein Anliegen, allen Teilnehmenden die Möglichkeit zum Austausch zu geben und gemeinsam Synergien bei Forschungsfragen und -projekten zu entdecken.

Das Forschungsforum Öffentliche Sicherheit in der AG Interdisziplinäre Sicherheitsforschung möchte hierdurch auch einen Beitrag zur Ausgestaltung der „Wissensallianz Un-Sicherheit“ des wissenschaftlichen Profils der Freien Universität Berlin leisten.

Im Folgenden finden Sie eine kurze Zusammenfassung der Impulsvorträge und der anschließenden Diskussion. Nach einer Begrüßung durch Prof. Dr. Lars Gerhold (AG Interdisziplinäre Sicherheitsforschung, FU Berlin), stellte Prof. Dr.-Ing. Jochen Schiller (AG Computer Systems & Telematics, FU Berlin) die technologischen Herausforderungen der Zukunft dar. Anschließend warf Prof. Dr. Klaus Thoma (ehem. Leiter des Fraunhofer-Instituts für Kurzzeitdynamik, Ernst-Mach-Institut) einen Blick auf die technischen Möglichkeiten die Zukunft sicherer zu machen. Prof. Dr. Wolfgang Bonß (Universität der Bundeswehr München) widmete sich der sozialwissenschaftlichen Perspektive und den möglichen sozialen Verwerfungen, die aus einer sicherheitstechnologischen Zukunft entstehen könnten. Die abschließende Diskussion wurde von Roman Peperhove (Forschungsforum Öffentliche Sicherheit, FU Berlin) unter der Fragestellung moderiert, welche Forschungsfragen sich in der Zukunft am dringendsten stellen werden und welche Themenfelder die Teilnehmenden als die Herausforderungen der Zukunft identifizieren.

Technisierung unserer Welt. Sicherheit im Zeitalter 4.0.

Prof. Dr.-Ing. Jochen Schiller, Arbeitsgruppe Computer Systems & Telematics, Freie Universität Berlin

Die Digitalisierung greift überall um sich, allerdings kommt der Wandel schleichend, entwickelt sich evolutionär und nicht disruptiv. Überall spricht man von Komplexität, die wir nur teilweise oder gar nicht mehr beherrschen können. Von welcher Komplexität sprechen wir? Die Anzahl von Komponenten in Geräten steigt kontinuierlich, das Gleiche gilt für den Vernetzungsgrad, Datenstrommuster, Fluktuationen und die Anzahl von involvierten Akteuren. Vielfältige Systeme werden miteinander verbunden und dies geschieht alles auf Basis des Internets. In der Zwischenzeit werden quasi unbemerkt klassische Dienste über neue, einheitliche Technologien angeboten. Ein Beispiel wäre das Telefon. Das analoge Telefonnetz wurde abgeschafft und damit auch die Notruffähigkeit. Es wird auch nicht gefragt, ob das gemacht werden soll, weil es kaum jemand versteht. Auch KRITIS-Komponenten werden über das Internet vernetzt; hier sind zumindest die Abhängigkeiten unklar, wenn nicht gar unbekannt. Das Thema, das momentan in aller Munde ist: Internet of Things. Hier ist die Kommunikationsfähigkeit in alle Komponenten integriert, d. h. alles ist mit allem vernetzt. Bisher haben wir eine Milliarde klassische Internetnutzer, acht Milliarden Mobilkomm-Nutzer und nun kommen noch 20-30 Milliarden kommunizierende „Dinge“ hinzu. Dies bietet neue Schlupflöcher beispielsweise für Botnetze, die sich in Überwachungskameras einhacken, weil diese eben nicht dagegen geschützt sind. Es wird Legacy Software benutzt, die ungeprüft ist. Oder man bedenke die Lebensdauer von Geräten im Vergleich zu Aktualisierungen von klassischer Computersoftware, die durchschnittlich alle 3 Monate erfolgen.

Daraus ergibt sich ein Sicherheitsproblem, für das noch kaum schlüssige Sicherheitskonzepte bestehen. Die Vernetzung geht so schnell vonstatten, dass es nicht möglich ist, im gleichen Tempo alle Schnittstellen zu verstehen und abzusichern. Die Abhängigkeiten einzelner Komponenten sind oft nicht direkt erkennbar und schwer zu durchschauen. Es müssten Lernprozesse angestoßen werden, um den Umgang mit den neuen Gefahren zu üben. Jedem ist klar, dass er einen Stromschlag bekommt, wenn er in die Steckdose fasst. Wenn es um Gefahren durch Vernetzung geht, ist noch viel Aufklärungsarbeit zu leisten. Im Internet ist nicht klar, wo genau die Gefahren lauern, welche „Ecken“ man meiden sollte. Wer denkt denn daran, dass von einer Insulinpumpe eine Gefährdung ausgehen könnte? Die Technologien werden in Umfelder gebracht, für die sie nicht gemacht sind. Die herkömmlichen Testmethoden aus den Ingenieurswissenschaften reichen hier nicht aus: Belastungstests, Stresstests, Entwicklung von Worst-Case-Szenarien. Offensichtlich werden diese Vernetzungen nicht als kritisch erkannt, obwohl es bereits Vorfälle gibt (medjacking, Angriffe auf Energieversorgung).

Private und strukturelle Sicherheit werden immer enger miteinander verwoben. Das private Smartphone ist mit dem Kernkraftwerk verbunden, das digitale Krankenhaus ist von überall her erreichbar. Alle Bereiche des privaten und des öffentlichen Lebens sind durch smart grids, smart meters verknüpft. Genauso wie das Internet von der Technik her keine Ländergrenzen kennt, genauso gibt es von der Technikseite her betrachtet keine automatische Grenze zwischen privat genutzten Systemen und z. B. KRITIS. Es stellt sich die Frage, ob der Staat überhaupt in der Lage ist, in einer „Infrastruktur 4.0“ Sicherheit zu gewährleisten. Es fehlen Eingriffsmöglichkeiten, Fachkräfte, aber auch eine Handlungshoheit.

Wie kann man sich aber schützen und was kann dem Bürger zugemutet werden? Zu denken ist an die Bereiche Identifizierungsverfahren beim Online Banking, Phishing Mails, verseuchte USB Sticks, Kreditkartenbetrug oder Umgang mit Passwörtern. Ist das noch realistisch zu leisten? Die Bevölkerung findet sich wieder zwischen Fatalismus und der Reaktion alles zu verdammen. Ein Gefühl der Hilflosigkeit gepaart mit Resignation macht sich breit, wenn nicht einmal die großen Firmen diese Probleme in den Griff bekommen. In der Tat ist es so, dass der „normale“ Nutzer mit alldem nicht alleine gelassen werden kann, wenn man Sicherheit, die Wahrung von Grundrechten, Freiheiten usw. aufrechterhalten möchte. Benötigt wird ein Mix aus Ausbildung/Bildung (Internetführerschein, Schule), integrierten Schutzsystemen ähnlich einem Airbag und gesetzliche Regelungen.

Die Technik kann wiederum auch bei der zunehmenden Komplexität hilfreich sein und die Nutzer_in unterstützen. Richtig gemachte Biometrie schont die Privatsphäre und ist somit bei weitem besser, bequemer und sicherer, als irgendein Passwort, wenn es richtig gemacht und auch akzeptiert wird. IT-Sicherheit könnte als Grundlagenwissen in die Lehrpläne der Schulen eingehen. Denn nur wer ausreichend gebildet ist, kann frei agieren und richtige Entscheidungen treffen. Es bräuchte also einen Dreiklang von Staat als Verantwortlichem für die Bildung, dem Individuum, das sich bewusst entscheidet, und von Unternehmen, die Mindeststandards einhalten und eine angepasste Produkthaftung anbieten.

Hieraus ergeben sich für die Zukunft drei zentrale Herausforderungen in der Forschung: die technische, die individuelle und die regulatorische Beherrschbarkeit von Komplexität. Im Detail sprechen wir von Verbindung, Abschottung, Funktionalität von Schnittstellen und Kaskadeneffekten. Auf der individuellen Ebene müssen Fragen der Abstraktion, der Vereinfachung, aber auch der Sichtbarkeit von Technik bearbeitet werden. Auf regulatorischer Ebene können Fragen zu Dynamiken von Gesetzgebung und Reaktionszeiten auf den Wandel gestellt werden.

Sicherheit im 21. Jahrhundert. Kann die Technik halten, was von ihr erwartet wird?

Prof. Dr. Klaus Thoma, ehem. Leiter des Fraunhofer-Instituts für Kurzzeitdynamik , Ernst- Mach-Institut

Um in das Themenfeld einzusteigen führte Prof. Thoma einen kurzen Diskurs zur Sicherheitsforschung und ihren Technologien. Als Ausgangspunkt stellte er die Fragen: Was wird die Zukunft bringen? Welche Themen bewegen die Menschen? Er identifizierte sechs Themenschwerpunkte: Energie, Mobilität, Umwelt, Gesundheit, Kommunikation und Sicherheit. Warum brauchen wir Sicherheitsforschung? Der Mensch war über die Jahrhunderte immer wieder veränderten Gefährdungen ausgesetzt. Grundlegenden Gefahren gehen von Krieg, Naturkatastrophen, Hunger und Epidemien aus. Forschung und Technik haben dazu beigetragen, dass die Menschen sich besser gegen diese Gefahren schützen konnten. Heute schützen uns unsere Infrastrukturen sicher und wir haben jederzeit Zugang zu Energie, Lebensmitteln, Transport und Informationen.

Durch die zunehmende Urbanisierung, die wachsende Vernetzung unterschiedlichster Lebensbereiche und -funktionen und dem damit einhergehenden Übergang zur global vernetzten Informations- und Dienstleistungsgesellschaft ergibt sich eine bisher wenig erkannte und beachtete Verletzlichkeit durch neue Bedrohungen. Neben terroristischen Angriffen müssen wir uns mit Großunfällen in industriellen

Anlagen und mit Kaskadeneffekten als Konsequenz der Vernetzung unserer Infrastrukturen auseinandersetzen. Somit wird Sicherheit zur Basis aller großen Themen der Zukunft. Sicherheitstechnologien oder der Ansatz „Security by Design“ sind Teil dieser Themenschwerpunkte und entwickeln sich immer stärker zum Innovationstreiber.

Die Sicherheitsforschung ist eine noch junge Querschnittsdisziplin mit besonderen Randbedingungen. Neben den technologischen, spielen soziale und rechtliche Aspekte ebenso eine Rolle wie die Bedarfe der Endanwender. Ziel der Sicherheitsforschung ist es daher, die zivile Sicherheit zu gewährleisten unter Wahrung der Menschen- und Freiheitsrechte.

Im Detail bedeutet dies, Sicherheit für den Bürger sowie Sicherheit und Stabilität unserer Infrastrukturen zu gewährleisten, mit dem Ziel eine resiliente Gesellschaft zu erreichen. Wie erreichen wir dieses Ziel? Es muss ein gesellschaftlicher Diskurs über ethische, ökonomische, juristische und politisch-soziologische Gesichtspunkte geführt werden. Außerdem sollten momentan vorhandene und antizipierbare Bedrohungen und Gefährdungen analysiert und aufgearbeitet werden, um daraus mögliche Szenarien für die Zukunft zu entwickeln. Ein zentrales Problem stellen die „Innovationszyklen“ dar, die in der Technologie wesentlich schneller sind als in den Geistes- und Gesellschaftswissenschaften.

Aus technologischer Sicht muss zuerst die notwendige Sicherheit ins Auge gefasst werden, dann wird die Akzeptanz bzw. die Ablehnung der Innovationen mit Hilfe der Gesellschaftswissenschaften eruiert, was dann zu einer Anpassung der Technologie führen sollte. Der Diskurs von Ingenieur-/Naturwissenschaften mit den Geistes- und Sozialwissenschaften ist von grundlegender Bedeutung. Doch wie ist dieser Austausch realisierbar? Die Technik stürmt voran und die Gesellschaftswissenschaften analysieren ex post? Es wird deutlich, dass der Blick in eine erwartbare oder mögliche Zukunft notwendig ist, damit Probleme erkannt werden und Lösungsansätze abgeleitet werden können.

Durch die zunehmende Vernetzung sind wir mitten in einer Verschiebung von lokalen zu globalen Fragestellungen. Das Internet macht nicht vor Landesgrenzen halt und das gleiche gilt für den Klimawandel, asymmetrische Konflikte, Ressourcenknappheit, Cyber-Kriminalität und auch Terrorismus. Nach einem Zitat von Frank-Walter Steinmeier, ist die Welt aus den Fugen geraten und vor allem ein Land wie Deutschland ist abhängig von einem stabilen politischen Weltordnungs-System.

Das bedeutet auch für die Sicherheitsforschung sich den Themenschwerpunkten global zu nähern.

Sicherheit im 21. Jahrhundert. Wie viel Sicherheitstechnik verträgt eine Gesellschaft?

Prof. Dr. Wolfgang Bonß, Sprecher des Forschungszentrums RISK an der Universität der Bundeswehr München

Sicherheitstechnik alleine kann nicht ohne die Sicherheitswirtschaft betrachtet werden. Sie „steht für alle technischen Vorrichtungen, die der Sicherheit dienen“[1]. Der Studiengang Sicherheitstechnik der Universität Wuppertal beispielsweise reduziert das Forschungsgebiet auf vier Schutz- und Wissensbereiche: Arbeit und Umwelt, Brand- und Explosionsschutz, Bevölkerungsschutz, Qualität und Zuverlässigkeit und Sicherheit im Luftverkehr. Das Rahmenprogramm „Forschung für die zivile Sicherheit“ des Bundesministeriums für Bildung und Forschung definiert die Schutzbereiche Verkehrsinfrastrukturen, Schutz und Rettung von Menschen, Schutz von Versorgungsinfrastrukturen und Sicherung der Warenketten und fügt dem noch vier „Technologieverbünde“ hinzu: Detektion von CBRNE-Gefahrenstoffen, integrierte Schutzsysteme für Rettungs- und Sicherheitskräfte, Mustererkennung und Biometrie.

Die Sicherheitswirtschaft ist in Deutschland, und nicht nur hier, die am stärksten expandierende Branche. Das größte Wachstum kann im Bereich der IT-Sicherheit verzeichnet werden. Zwischen 2012 und 2015 wuchs die gesamte Sicherheitsbranche um 21%. Dies beinhaltet aber nicht nur Produkte der Sicherheitstechnik, sondern auch Dienstleistungen im Sicherheitsbereich.[2]

Doch mit welchen Begriffen befassen wir uns, wenn wir im Deutschen von Sicherheit sprechen? Safety, Security, Certainty? In der deutschen Sprache fällt dies alles unter den Begriff der Sicherheit. Das Englische unterscheidet aber diese drei Bereiche von Sicherheit (Abb. 1).

Das klassische Verständnis von Sicherheit beinhaltet vor allem die Abwehr von Gefahren und damit verbunden die Idee der vollständigen Sicherheit. Erst mit dem Begriff der Risikogesellschaft kehrte die Unsicherheit zurück in den Diskurs. Der Begriff des Restrisikos fand Eingang in die Forschung und führte zu einer Entlastung der Sicherheitstechnik. Heute geht es nicht mehr um die Herstellung vollständiger Sicherheit, sondern um Widerstandsfähigkeit und die Fähigkeit, nach einer Katastrophe wieder Normalität und Handlungsfähigkeit herzustellen. Damit befinden wir uns im Übergang zum Resilienzdiskurs.

[1] Seite „Sicherheitstechnik“. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 11. August 2012, 20:03 UTC. URL: https://de.wikipedia.org/w/index.php?title=Sicherheitstechnik&oldid=106688998 (Abgerufen: 6. Juli 2017, 07:10 UTC)

[2] Quelle: Brandenburgisches Institut für Gesellschaft und Sicherheit.

Kategorie	SAFETY	SECURITY	CERTAINTY
Bedeutung	*„technische" Sicherheit im Sinne der Zuverlässigkeit technischer Systeme*	*„gesellschaftliche" Sicherheit im Sinne politisch-sozialer Sicherheit*	*„kognitive" Gewissheit und ihre Grenzen*
Beispiele	Safety belt, ABS, ESP; allgemeiner: die technische Zuverlässigkeit von Bauteilen, Einheiten, Subsystemen und Gesamtsystemen *(ohne soziale Einflüsse!)*	a) *die soziale Einbettung/ Kontextualisierung technischer Risiken* b) *Politische Sicherheit: innere und äußere Sicherheit* c) *Soziale Sicherheit: social security, Gesundheitssicherung,* d) *Biographische Sicherheit: Erwartbarkeit und Überschaubarkeit des eigenen Lebenslaufs*	die (vergebliche) Suche nach "abgeschlossenen" Theorien Verwissenschaftlichung und die wachsende Ambivalenz des Wissens *(„Wir wissen, dass wir weniger wissen und mit Nicht-Wissen umgehen müssen")*

Abbildung 1

Das Phänomen der Versicherheitlichung wie beschrieben von Buzan, Wæver, de Wilde[3] behandelt die Kernthese: Immer mehr Probleme werden zu Sicherheitsproblemen erklärt, wobei diese Umdefinition nicht selten zu einer problematischen Außerkraftsetzung gegebener demokratischer Verarbeitungsregeln führt. Daraus ließe sich folgern: Die Ausweitung der Sicherheitsdiskurse im Sinne einer Versicherheitlichung ist eine problematische Angelegenheit, welche die Frage nach einer „Entversicherheitlichung" aufwirft.

Wieviel Sicherheitstechnik verträgt nun die modernisiert-moderne Gesellschaft? Folgende Schlüsse lassen sich ziehen: Sicherheitstechnik entwickelt sich gerade in Risikogesellschaften zu einem unendlichen Feld, das sich nur strukturieren lässt, wenn über die gesellschaftliche Relevanz der Sicherheitstechnik diskutiert wird. Es gibt zwar eine programmatische Akzentverschiebung im technischen Sicherheitsdiskurs, wie bereits beschrieben von der absoluten Sicherheit zum Resilienzdiskurs. Diese ist aber in der Praxis der Wissenschaftstechnik bislang nur begrenzt angekommen. Die stetige Ausweitung der Wissenschaftstechnik muss durch einen Diskurs darüber korrigiert werden, welche Unsicherheiten modernisiert-moderne Gesellschaften aushalten müssen. Es kann nicht um eine Wiederbelebung des klassischen Gefahrenabwehrdiskurses gehen. Stattdessen muss es um zweierlei gehen: Zum einen um den Ausbau

[3] Barry Buzan, Ole Wæver, Jaap de Wilde (1998). Security: A New Framework for Analysis.

und eine bessere Verankerung des Resilienzdiskurses und zum anderen um eine kritische Diskussion (und auch Zurückdrängung) der Versicherheitlichungstendenzen in modernisiert-modernen Gesellschaften.

Diskussion

Die angeregte Diskussion der Teilnehmenden berührte verschiedene Punkte des Diskurses zwischen Technik und Gesellschaftswissenschaften und kann unter einigen Themenbereichen oder Fragestellungen zusammengefasst werden.

Themenbereich: „Komplexität“

Ein Schwerpunkt der Diskussion war der Themenbereich „Komplexität“. Wir leben in einer immer komplexer werdenden Welt, die der Einzelne nicht mehr bis ins letzte Detail verstehen kann. Nichtsdestotrotz müssen wir mit dieser Komplexität leben. Damit einher geht auch der Verlust des Gefühls für Gefahren bspw. aus bzw. über das Internet. Eine Einschätzung wird immer schwieriger, da die Gefahren diffuser werden. Es müssten Wege gefunden werden, um eine Sensibilität für die neuen Gefahrenlagen zu entwickeln.

Der Kontrollverlust im Netz wurde thematisiert. Wenn um einen herum alles „smart“ wird, wie kann man dann überhaupt noch die Kontrolle behalten? Es müsste eine adäquate Governance geschaffen werden, die auf die Komplexität der Systeme abgestimmt ist. Bei zu viel Vernetzung verlören wir ansonsten unsere Entscheidungskompetenz.

Einer der Teilnehmenden bemerkte, dass auch die sogenannten „Digital Natives“ längst nicht zwangsläufig ein größeres Verständnis von Rechnersystemen oder Technologie hätten als „Digital Immigrants“. Bisher bietet das deutsche Bildungssystem keine Grundlage für einen tiefer gehenden Diskurs, weil die Möglichkeiten dazu fehlen. Der Kontakt zu Schüler_innen müsste früh aufgenommen werden, um die Zukunft gestalten zu können.

Die Teilnehmenden diskutierten Dienstleistungen, die im Netz angeboten werden, und konstatierten, dass vor allem angebotene „Services“ im Netz Probleme generierten, da Plattformen beispielsweise zum Datenklau missbraucht würden und Schlupflöcher für den Zugriff auf private Daten eröffneten.

Fragestellung: Wie viel Freiheit ist uns die Sicherheit wert?

In diesem Zusammenhang wurde auch diskutiert, dass eine totale Öffnung und Transparenz der Daten als Flucht nach vorne, zukünftig ein Weg sein könnte, um Missbrauch von Daten einzudämmen. Andere Maßnahmen bedeuteten auch eine Verringerung der Freiheit im Netz. Wir müssten die Frage, wie viel Freiheit sind wir bereit im Namen der Sicherheit aufzugeben, kritisch stellen und in einem gesellschaftlichen Aushandlungsprozess diskutieren. Der von Prof. Bonß definierte Begriff der Entversicherheitlichung kam hier wieder ins Gespräch und wurde als interessanter Ansatz aufgenommen.

Beim Thema Datenspeicherung wiederum wurde eingeworfen, dass es doch ein Unterschied sei, ob die Daten von privaten Anbietern oder vom Staat gespeichert würden. Die Teilnehmenden konnten hier

keinen Konsens erreichen. Es wurde unter anderem darauf verwiesen, dass jeder Onlineshop, die Daten seiner Kunden speichere und verkaufe.

Auch hier kamen die Teilnehmenden wieder auf die Bildung zu sprechen. Nur aufgeklärte Nutzer_innen können ein Bewusstsein entwickeln und sich effektiv vor Datenklau schützen.

Fragestellung: Gesellschaft im Zentrum der Forschung

Die Teilnehmenden stellten die Frage, wie wir die Zukunft gestalten können. Es sollten neue Methoden in Zusammenarbeit mit Politik, Behörden und Wissenschaft entwickelt und diskutiert werden. Gleichzeitig sollten auch bereits bestehende Theorieansätze miteinbezogen werden, um „vor die Lage zu kommen".

Man war sich einig, dass die Rolle der Gesellschaft einen zentralen Punkt in allen Diskussionen und Entwicklungen einnehmen muss. Wenn die Ideen und Lösungsansätze nicht in der Gesellschaft ankommen, ist der Mehrwert verloren.

Wir leben in einer Umbruchszeit. Es wird interessant sein, in 20 Jahren auf das Jetzt zurückzublicken. Momentan werden immer und immer wieder die gleichen Diskussionen geführt. Im Rückblick werden wir sehen, welche Ergebnisse erzielt wurden, weil wir dann mit der Digitalisierung leben werden. Im Bereich Datenschutz ist zumindest in den letzten zwölf Jahren nicht viel vorangekommen.

Bewertung der Themenbereiche

Im Anschluss an die Diskussion wurden die Teilnehmenden gebeten, die identifizierten Themenbereiche mit Punkten nach ihrer Bedeutung zu bewerten.

Nach der Auswertung sind die Themen, deren Bearbeitung die anwesenden Wissenschaftler_innen als wichtig einstuften, die folgenden:

- Resilienz von Systemen und von Bevölkerung, um auch im Extremfall handlungsfähig zu bleiben.
- Gesellschaft sollte im Zentrum der Sicherheitsforschung stehen.
- Inter- und Transdiziplinarität, weil Sicherheit nie disziplinär gedacht werden kann und auch die Praktiker mit einbezogen werden müssen.