TATuP Call

ZEITSCHRIFT FÜR TECHNIKFOLGENABSCHÄTZUNG IN THEORIE UND PRAXIS

Call for Abstracts:

„Cybersicherheit“

TATuP-Thema in Heft 1/2020

Informations- und Kommunikationstechnologie (IKT) hat fast alle gesellschaftlichen Praktiken durchdrungen und beeinflusst unsere Denkweise, unsere Interaktionen mit anderen Personen sowie mit Organisationen und Institutionen; sie verändert unsere Rollen als Bürgerinnen und Bürger, Arbeitnehmerinnen und Arbeitnehmer oder auch als Verbraucherinnen und Verbraucher. IKT als komplexe und vernetzte Basistechnologie des 21. Jahrhunderts macht unsere Welt zu einem reicheren, effizienteren und sehr interaktiven Ort – IKT kann die Kommunikation und Interaktion zwischen Menschen über Grenzen zwischen Staaten und Kulturen hinweg erleichtern oder gar erst ermöglichen. Gleichzeitig machen Komplexität und hochgradige Vernetzung IKT jedoch anfällig für technisches Versagen sowie für kriminelle, terroristische oder gar kriegerische Attacken, so dass es mit zunehmender Komplexität und Vernetzung immer schwieriger wird, die Funktionsfähigkeit von Industrien oder Versorgungsinfrastrukturen aufrechtzuerhalten. Moderne Gesellschaften, deren Funktionsfähigkeit auf IKT beruht, sind damit – mit Ulrich Beck (1986) gesprochen – „gefährdete Gesellschaften“. Es gehört zu den großen Herausforderungen unserer Zeit, diese Gesellschaften in „Risikogesellschaften“ zu transformieren, also in Gesellschaften, die sich angemessen gegen entsprechende Risiken organisieren und eine gesellschaftlich akzeptable und akzeptierte Balance zwischen Sicherheit und anderen Werten finden. Diese Transformation ist der Ausgangspunkt des TATuP-Themas „Cybersicherheit“.

Im Jahr 2014 betrugen die jährlich durch Cyberkriminalität verursachten Kosten weltweit mehr als 400 Milliarden Dollar; gleichzeitig wuchs der Markt aller verfügbaren Sicherheitsprodukte zwischen 2011 und 2014 um 14,3% (CSIS 2014). Aus gesellschaftlicher Sicht sind nicht nur die direkten Kosten (z.B. Reparaturkosten, betrugsbedingte Verluste), sondern auch indirekte Kosten (bspw. Kosten von Präventivmaßnahmen) und implizite Kosten (u. a. geringere Produktivitätssteigerungen durch geringeres Vertrauen in digitale Transaktionen) auf Verletzungen der Cybersicherheit zurückzuführen (Bauer und van Eeten 2009). Angesichts solcher Zahlen kann es nicht verwundern, dass aktuelle Cybersicherheitsdebatten geprägt sind durch Betonung immer größerer und vielfältiger werdender Bedrohungsformen, die von Cyberkriminalität und Cyberspionage bis hin zu Cyberterror und Cyberwar (Dunn Cavelty 2014) reichen. Cybersicherheit ist dadurch auch zu einer Angelegenheit staatlicher Akteure geworden; die Ausgaben für verteidigungsbezogene Aspekte von Cybersicherheit steigen (Brito und Watkins 2011; Boulanin 2013).

Schon dieser kurze Überblick weist auf die Gefahr hin, Diskurse über Cybersicherheit thematisch einzuengen: Je mehr Gesellschaften auf funktionierende IKT angewiesen sind, desto eher neigen sie dazu, Sicherheit über alle anderen Werte zu stellen, auf denen unsere Gesellschaften aufbauen. Infolgedessen werden Grenzen, die bisher unsere soziale, institutionelle, rechtliche und moralische Welt konstituiert haben, infrage gestellt, kompromittiert oder relativiert. Traditionelle Differenzierungen und Abgrenzungen getrennter sozialer Bereiche wie Familie und Freundschaft,

Arbeit, Politik, Bildung, kommerzielle Aktivität und Produktion, Gesundheitswesen, Forschung usw., die jeweils durch kontextbezogene Normen und Regeln bestimmt sind, werden durch IKT bedroht. Betroffen sind bspw. Konzepte wie informierte Einwilligung, persönliche Daten oder Anonymität sowie die ihnen zugrundeliegenden Werte wie Autonomie, Fairness, Privatsphäre und Verantwortung. Diese Werte können durch den Wert der Sicherheit außer Kraft gesetzt werden, wenn Cyberbedrohungen als grundlegende Störung der gegenwärtigen Lebensweise angesehen werden. Wie viel Absicherung erforderlich ist, ist umstritten. Möglicherweise reicht das Repertoire der vorhandenen Maßnahmen und Mechanismen bereits aus, weil Gesellschaften es gewohnt sind, Risiken einzugehen und im Bedarfsfall zu handeln (Odlytzko 2019). Cybersicherheit herzustellen bedeutet daher nicht nur die Überwindung technischer Hindernisse, sondern auch ein tieferes Verständnis für die Veränderungen, die sich aus der Digitalisierung des modernen Lebens ergeben. Es bedarf einer multiperspektivischen Sichtweise, an der Expertinnen und Experten aus verschiedenen wissenschaftlichen Disziplinen ebenso wie aus unterschiedlichen Professionen beteiligt sein müssen.

Literatur

Bauer, Johannes; van Eeten, Michel (2009): Cybersecurity. Stakeholder incentives, externalities, and policy options. In: Telecommunications Policy 33(10–11), S. 706–719.

Beck, Ulrich (1986): Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt am Main: Suhrkamp.

Boulanin, Vincent (2013): Cybersecurity and the arms industry. In: SIPRI Yearbook 2013: Armaments, disarmament and international security, S. 218–226.

Brito, Jerry; Watkins, Tate (2011): Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. Mercatus Center Georg Mason University, Working Paper No. 11-24. Online verfügbar unter: https://www.mercatus.org/system/files/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy_0a.pdf, zuletzt geprüft am 12.04.2019.

Dunn Caveltry, Miriam (2014): Breaking the cyber-security dilemma. Aligning security needs and removing vulnerabilities. In: Science and Engineering Ethics 20(3), S. 701–715.

Odlyzko, Andrew (2019): Cybersecurity is not very important. Working Paper. Online verfügbar unter: http://www.dtc.umn.edu/~odlyzko/doc/cyberinsecurity.pdf, zuletzt geprüft am 15.04.2019.

Erwünschte Beiträge

Für das TATuP-Thema „Cybersicherheit“ werden Beiträge gesucht, die sich aus Sicht der Technikfolgenabschätzung und Technikbewertung mit den oben skizzierten Themen auseinandersetzen und bspw. technische Entwicklungsstränge im Bereich der Cybersicherheit, den Zusammenhang von Cybersicherheit und kritischen Infrastrukturen, Angriffsszenarien und deren mögliche (gesellschaftlichen) Auswirkungen, gesellschaftliche Veränderungsprozesse, Aspekte des Cybersicherheitsdiskurses auf nationaler, europäischer und/oder globaler Ebene, politische Diskurse und Reaktionen sowie Überlegungen zur Abwägung von Cybersicherheit und anderen Werten

behandeln. Dabei sollte stets versucht werden, unterschiedliche Stakeholder-Perspektiven zu berücksichtigen. Die genannte Themenliste ist nicht erschöpfend; daher ermutigen die Herausgeber des TATuP-Themas potenzielle Autorinnen und Autoren, Abstracts mit verwandten, aber nicht explizit genannten Themen einzureichen. Dies gilt insbesondere für Einreichungen, die sich damit auseinandersetzen, ob durch neue technische, organisatorische und/oder legislative Entwicklungsstränge im Bereich der Cybersicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) mit disruptiven Veränderungen zu rechnen oder eher von kontinuierlichen Entwicklungslinien auszugehen ist.

Herausgeber dieses TATuP-Themas

Karsten Weber (OTH Regensburg), Markus Christen (Universität Zürich) und Dominik Herrmann (Universität Bamberg)

Einreichung

Bitte senden Sie Ihr Abstract bis spätestens **06. Juni 2019** per E-Mail an redaktion@tatup.de und beachten Sie dabei folgende Punkte:

- max. 3000 Zeichen inkl. Leerzeichen;
- die Redaktion führt die Korrespondenz mit der Autorin bzw. dem Autor, die bzw. der das Abstract eingesendet hat;
- nennen Sie alle beteiligten Autorinnen und Autoren mit vollständigem Namen, E-Mail-Adresse und institutioneller Anbindung.

Zeitplan

06. Juni 2019: Deadline für die Einreichung von Abstracts.

Ende Juni 2019: Entscheidung über Einladung zur Einreichung eines Manuskriptes.

23. September 2019: Deadline für die Einreichung des Manuskriptes.

ab **Mitte November 2019**: Rückmeldungen aus dem Begutachtungsprozess, anschließend Überarbeitungen durch die Autorinnen und Autoren.ca.

Ende März 2020: Veröffentlichung.