Abstract für CfP „Aktuelle Kriminalogische Forschung“

Soziologische Einblicke in den gesellschaftlichen Kampf um Sicherheit im digitalen Zeitalter

Martin Griesbacher, MA[1]

Ziel des vorliegenden Beitrages ist es, Einblicke in die gesellschaftlichen Dynamiken hinsichtlich öffentlicher Meinung und öffentlichem Diskurs zum Thema „Cybersecurity“ zu geben. Der Beitrag beruht auf zwei ausführlichen soziologischen Studien[2], die im Rahmen eines EU Projektes zur Vertrauenswürdigkeit von IKT Produkten und Dienstleistungen durchgeführt wurden (TRUESSEC.eu – Trust-Enhancing certified Soluctions for Security and protection of Citizens’ rights in digital Europe).

Cybersecurity, also die Sicherheit von IKT-NutzerInnen, legt im Regelfall zunächst den Blick auf „Cybercrime“ nahe. Cybercrime bezeichnet nach der Budapester Konvention jede kriminelle Handlung, die über Informationsnetzwerke und -infrastruktur abgewickelt wird und sowohl virtuelle als auch reale Räume zum Ziel hat.[3] Bei der Benennung cyberkrimineller Handlungsfelder werden exemplarisch nach Wall etwa Cyber-trespassing, Cyber-Theft, Cyber-Pornographie, Cybergrooming und Cyber-Violence angeführt.[4] Neue Informations- und Kommunikationstechnologien potenzieren im digitalen Zeitalter „die Vernetzungsmöglichkeiten bereits bestehender krimineller Strukturen und schaff[en] neue Wirkungsbereiche und Innovationspotentiale krimineller Aktivitäten“.[5]

Unabhängig davon, inwieweit man heute im digitalen Zeitalter von *neuen* Formen der Kriminalität oder nicht sprechen sollte, zeigt sich eine vielseitige Bedrohungslage für NutzerInnen von IKT. Wenn man von einem breiten Sicherheitsbegriff ausgeht, kann Cybersecurity nicht mehr nur auf kriminelles Verhalten im engeren Sinne bezogen werden. Definiert man Sicherheit als situatives Merkmal, bei dem die Wahrscheinlichkeit des Eintretens eines Schadens an der physischen, psychischen, sozialen, ethischen und finanziellen Integrität möglichst gering ist, so kommen auch andere Bedrohungsquellen in den Blick. Cybersecurity kann nicht nur ex negativo als Abwesenheit von Cyberkriminalität verstanden werden, sondern schließt die Wahrnehmung von Risiken und Vertrauensdynamiken ein, die mit unterschiedlichen Akteursgruppen assoziiert werden. Dabei sind nicht nur gesellschaftlich als kriminell etikettierte Akteure zu nennen, sondern auch staatliche, wirtschaftliche oder politische Akteure, deren Handeln sich v.a. auf sensible Bereiche wie den Umgang mit personenbezogenen Daten im Allgemeinen oder Überwachung im Speziellen bezieht (so kann das Eindringen in die Privatsphäre von Individuen über IKT durch die mögliche Missachtung von Bürgerrechen Schaden an der ethischen Integrität verursachen).

Es können drei „Areas of Concern in the Digital Realm“ identifiziert werden: Cyberkriminalität, die Bearbeitung von personenbezogenen Daten durch unternehmerische Entitäten und die Bearbeitung von personenbezogenen Daten durch staatliche Institutionen. Der Beitrag wird auf Basis internationaler Befragungsdaten und exemplarischer Diskursanalysen (siehe Fußnote 2) diese *Areas of Concern* behandeln und Ambivalenzen im Kampf um Sicherheit im digitalen Zeitalter aufzeigen (z.B. Gefährdung von Sicherheit durch staatliche Sicherheitsmaßnahmen oder der Beitrag aggregierter bzw. emergenter Effekte zur Sicherheitswahrnehmung).

---

[1] Projektassistent am Forschungsnetzwerk “Human Factor in Digital Transformation“ an der Universität Graz.

[2] Reichmann, S./Griesbacher, M. (2017), Public Perceptions of Cybercrime and Cyber Security in the EU, Deliverable D3.1, TRUESSEC.eu; Dies. (2018), Current exemplary discourse dynamics in the field of cybersecurity, Deliverable 3.2, TRUESSEC.eu.

[3] Council of Europe (2001), Convention on Cybercrime, European Treaty Series – No. 185.

[4] Wall, D. (2002): Cybercrimes and the internet, in: Ders. (Hrsg.): Crime and the Internet, Routledge, 1-17.

[5] Merkel, M., Dittmann J., Reichmann S., Griesbacher M. (2017), „Sozio-technische Aspekte von Finanz- und Cyberkriminalität“, in: Schartner, P. / Baumann, A. (Hrsg.): DACH Security 2017, S. 24-37.