AI & Soc
DOI 10.1007/s00146-013-0525-4

OPEN FORUM

The model gap: cognitive systems in security applications and their ethical implications

Tobias Matzner

Received: 2 October 2013 / Accepted: 22 October 2013

Abstract The use of cognitive systems like pattern recognition or video tracking technology in security applications is becoming ever more common. The paper considers cases in which the cognitive systems are meant to assist human tasks by providing information, but the final decision is left to the human. All these systems and their various applications have a common feature: an intrinsic difference in how a situation or an event is assessed by a human being and a cognitive system. This difference, which here is named "the model gap," is analyzed pertaining to its epistemic role and its ethical consequences. The main results are as follows: (1) The model gap is not a problem, which might be solved by future research, but the central feature of cognitive systems. (2) The model gap appears on two levels: the aspects of the world, which are evaluated, and the way they are processed. This leads to changes in central concepts. While differences on the first level often are the very reason for the deployment of cognitive systems, the latter is hard to notice and often goes unreflected. (3) Such a missing reflection is ethically problematic because the human is meant to give the final judgment. It is particularly problematic in security applications where it might lead to a conflation of descriptive and normative concepts. (4) The idea of the human operator having the last word is based on an assumption of independent judgment. This assumption is flawed for two reasons: The cognitive system and the human operators form a "hybrid system" the components of which cannot be assessed independently; and additional modes of judgment might pose new ethical problems.

T. Matzner (✉)
Wilhelmstraße 19, 72070 Tübingen, Germany
e-mail: tobias.matzner@uni-tuebingen.de

Keywords Model gap · Cognitive systems · Security ethics · Smart CCTV · Drone · UAV

1 The model gap

Regarding security, we constantly evaluate our situation according to highly context-dependent concepts. This pertains to two levels: social and personal. On the social level, various contexts, such as airport, train station, market, private accommodations, can be distinguished regarding both the prevalent security expectations themselves, and the value security has been compared to other values such as freedom, privacy, or justice. On the personal level, in each of these contexts, everyone has their own prospect of security. For example, a rather dirty street lined with graffiti makes some people feel insecure; yet, it can be the sought-after neighborhood for others. In a similar manner, everybody places security at a different position regarding competing values. These context-dependent factors contribute to a variety of differing perceptions on what counts as threat to security in a given context.

Of course, the social and the personal levels are related. The exact nature of this relation is debated in various scientific discourses, which I do not want to get into here. My remarks are just intended to highlight that it does not suffice to reflect the prevailing views or social standards or to presuppose a rather homogeneous and settled view in most of the contexts.

Smart[1] security systems introduce one or more additional evaluations of the context. For the purpose of this

[1] I follow the common use of the word "smart" as in "smart security system" or "smart CCTV" both in public and scientific discourse. Yet, it is important to mention that this choice of words can contribute to the very misjudgment of security technology that is discussed in this paper.

Published online: 05 November 2013