Acceptance of security technologies

Reinhard Kreissl on behalf of ESSRO

Societal acceptance of security technology is based on societal understanding and citizens' awareness of security problems and threats. Knowledge of citizens on security is predominantly shaped by media coverage. This can produce bias with regard to the general public's assessment of seriousness and probabilities of security threats. Also, data collection through standard survey methods like ESS or Eurobarometer only gives a partial picture of security perception. Respondents ranking security threats chosen from a pre-defined list, create a hit list of threats by ranking a selection of security problems. But this methodology leaves no room to elaborate on their daily concerns. The limited focus on dramatized abstract security threats not only ignores an important dimension of citizens' (in-)security but also narrows down the range of acceptable arguments in security policy debates. A comprehensive deliberation of adequate uses of security technology should integrate public concerns beyond an incident-based interpretation of security threats. Popular threat scenarios such as organised crime, terrorism or human trafficking rarely are felt directly at the level of daily lives of citizens. More often, citizens' security concerns are focussing on risks not threats, i.e. insecurity emerges with regard to the future – probably detrimental – effects of present-day decisions and actions.

Replacing a threat-based approach to security with a risk frame societal acceptance of security technology appears in a different light. Citizen will be more willing to accept security technologies they understand and can relate to and use as a practical tool or resource in their everyday life. The prototype of modern security technology is based on panoptic surveillance: it collects data from an environment, screens the data for anomalies and produces an alert if an anomaly is detected in the data. Citizens are either the objects of surveillance (as in CCTV) or are asked to provide person-related data (e.g. at a border checkpoint) to access places, products or services. Panoptic security technologies operate with a threat logic using the default assumption that everyone is a suspect until proven otherwise.

Security technology could take a completely different direction when taking citizens' security concerns as a starting point and involving them as end-users in co-creative processes of technology development to empower them as active and interacting agents of risk governance. Examples for such "horizontal" technologies in DRS could be Apps that help citizens to coordinate with first responders in disaster and crisis situation and to get access to real-time information about adequate responses. Also, technologies that help citizens identify fraudulent and criminal schemes in the cyber sphere (e.g. offers to get involved as money mules for money laundering, or providing personal information for identity theft schemes) would most probably be acceptable security technologies with immediate use-value for lay citizens. More advanced solutions, based on digital ledgers and block chain technology, that allow citizens to manage differential access to personal data while at the same time improving and facilitating security checks by LEA at border crossings could also be seen as a form of acceptable technology. What all these examples have in common is that they give citizens an active role and produce a practical use value. Technological solutions can be designed using a privacy by design approach, making sure data protection and privacy are adequately considered, the process of technology development from the beginning can integrate citizens as end-users in co-creative processes and the results can help to empower citizens and at the same time increase acceptance of security technology and raise the level of societal security.