PUBLIC SAFETY IN SMART CITIES - A (TRANSITIONAL) RESILIENCE PERSPECTIVE

Tor Olav Grøtan and Andrea Vik Bjarkø
SINTEF Digital[1]
tor.o.grotan@sintef.no; andrea.vik.bjarko@sintef.no

Osman Mohammad Ibrahim and Ian Simon Gjetrang
Oslo Kommune[2]
osman.ibrahim@ber.oslo.kommune.no; ian.gjetrang@ber.oslo.kommune.no

Abstract - Academic paper.

The idea of the Smart City gains increasing attraction and is implemented and explored in many ways across the world. A lot of expected benefits and innovations are in focus, but the issues of public safety and security in public spaces have gained comparatively much less attention. Smart City relevant technologies such as Artificial Intelligence (AI) are promising, but also potentially overwhelming from an operational and organizational point of view. This is due to, e.g., information overload, exposure to new threat actors, and new vulnerabilities and security issues related to the digital technologies. Last, but not least, the privacy issues are very challenging. This implies that smart cities must develop new organizational forms and new operational concepts, and organize their attention towards new arenas, including social media, and gather intelligence from a variety of sources. The IMPETUS project addresses this challenge by employing a combined focus on ethics, work processes and technologies in a proper balance that ensures public safety in smart cities, within legal and ethical boundaries. Oslo and Padova are case cities and partners in the project. The complexity of the Smart City implies that it will be impossible to foresee all potential situations that may arise in the operational "theatre" – that is, the public spaces to be protected, the threats and the countermeasures available. The operators at the Security Operations Centers (SOC) must also be prepared to operate at the boundaries of even the best conceivable operational concept. This must be addressed at both a human-centred and an organisational level, with a proactive approach to handling the unexpected.

Resilience Engineering (RE) is an approach that addresses the abilities needed to handle the variations, disturbances and unexpected situations in a complex system. In RE, the scope of resilient performance is not just to be able to recover from threats and stresses, but rather to be able to perform as needed under a variety of conditions – and to respond appropriately to both disturbances - and opportunities. This combined focus is especially relevant for a Smart City. This paper will address how RE is relevant for Smart Cities related to the formulation of an initial operational model, the transition towards the model, and third but not least important, for the continuous evolvement of the operational model. However, as RE is not the only reasonable approach to taking advantage of resilience concepts, the RE contribution will be contextualized through a NEXUS model approach, framing an eclectic set of resilience approaches. Accordingly, "smart city resilience" is seen as a result of different efforts in different contexts. RE is a major foundation, but not the whole story. Nevertheless, a central premise for the discussion will be that the ability to cope with the unexpected requires a different mindset than to anticipate its occurrence. The paper will address how RE and related resilience approaches may

[1] Strindvegen 4, Trondheim, Address: SINTEF, P.O. Box 4760 Torgarden, NO-7465 Trondheim, Norway
[2] Online at: https://www.oslo.kommune.no/english/contact/

This paper is supported by European Union's Horizon 2020 research and innovation programme under grant agreement No. 883286, project IMPETUS (Intelligent Management of Processes, Ethics and Technology for Urban Safety).

inform and inspire the three phases of the operational model and devise how a training-by-gaming approach may be used for addressing situations at the boundaries of what is possible through preparedness efforts.

Keywords: Smart cities, public spaces, safety, security, resilience engineering, training by gaming