

# SMART CITIES ARE SAFE CITIES

5G



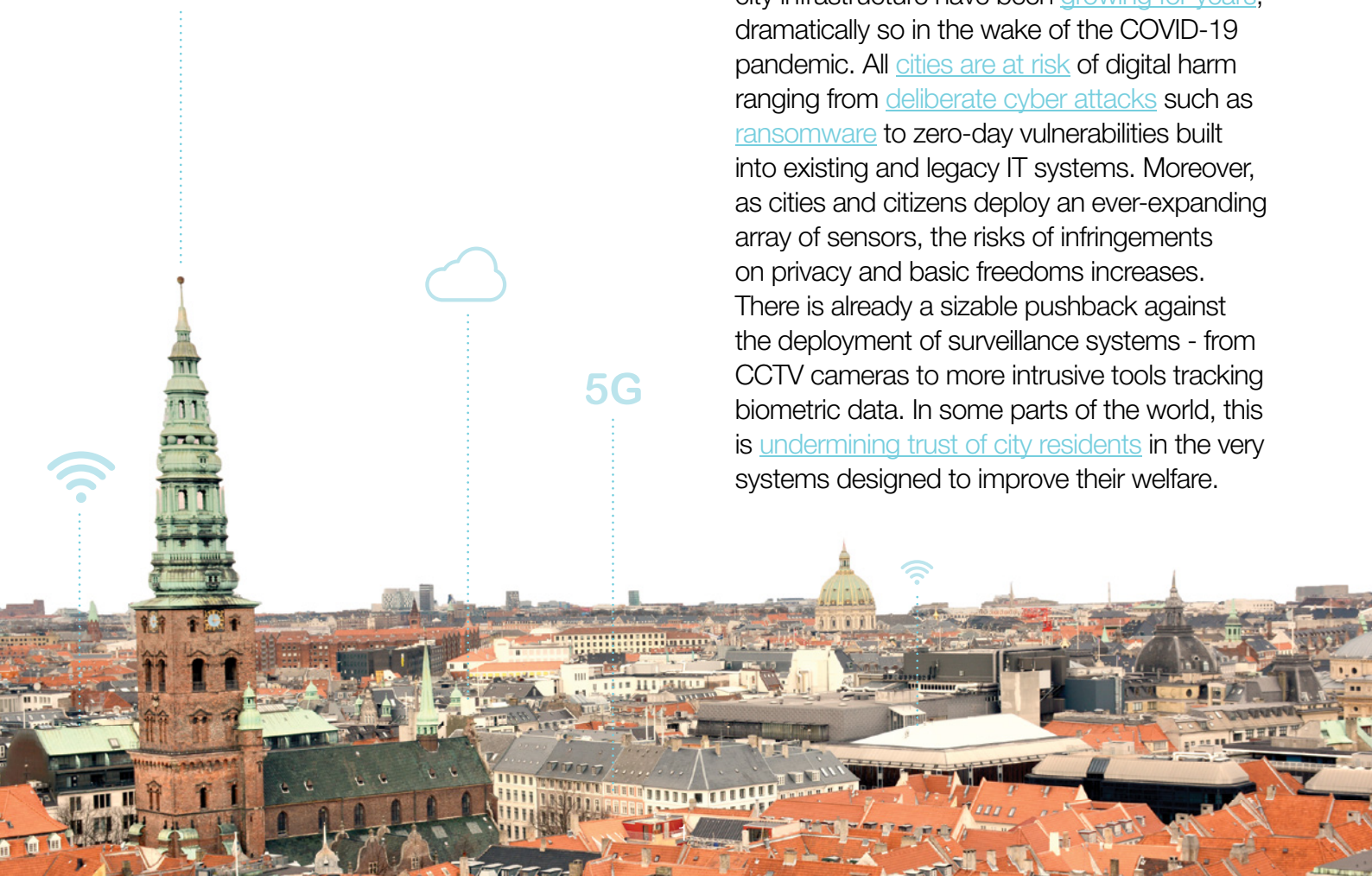
A digital safety, trust and  
inclusion assessment

# SMART CITIES ARE SAFE CITIES

A digital safety, trust and inclusion assessment

**Cities are dramatically scaling-up investment in smart city technologies.** The deployment of digitally connected devices and cloud computing is expected to improve the efficiency and effectiveness of basic services - from energy use and mobility to waste management and crime prevention. There are hundreds of cities describing themselves as “smart”, even if there is still no consensus about what exactly this means. Most major technology companies are investing in digitalization: the smart city market is expected to grow above [\\$820 billion](#) by 2025. There are already at least [1,000 smart city projects](#) underway in 50 countries. The number of smart cities is expected to grow dramatically over the coming decade with the spread of IoT and the adoption of AI and 5G.

**The drive toward increasing the smartness of cities introduces new risks.** As cities become more digitally connected and dependent, their attack surface also increases. The risks of cyber attacks targeting city infrastructure have been [growing for years](#), dramatically so in the wake of the COVID-19 pandemic. All [cities are at risk](#) of digital harm ranging from [deliberate cyber attacks](#) such as [ransomware](#) to zero-day vulnerabilities built into existing and legacy IT systems. Moreover, as cities and citizens deploy an ever-expanding array of sensors, the risks of infringements on privacy and basic freedoms increases. There is already a sizable pushback against the deployment of surveillance systems - from CCTV cameras to more intrusive tools tracking biometric data. In some parts of the world, this is [undermining trust of city residents](#) in the very systems designed to improve their welfare.



**The pace of urban IoT deployment is outpacing policy at all virtually levels.** There is very little regulation of new smart city technologies, with most urban authorities relying on vendors and third party providers to voluntarily design-in safeguards. This has created huge exposure for cities around the world, especially those in emerging markets. The risk, then, is that the push to accelerate smart cities could exacerbate critical vulnerabilities ranging from exposure to destructive cyber-attacks and ransomware to leakage of private data. Crucial to the success of smart cities, then, is investment in [digital resilience](#): secure infrastructure, measures to strengthen data protection and privacy, and digital literacy among city personnel, private companies and residents.

**Building “safe” smart cities means investing in safety, trust and inclusion.** Heavily surveilled cities not only deter citizen engagement, they can [trigger backlashes](#) around the world. Increasingly, [residents want to know](#) what happens to data that is harvested from them, how it is retained and ultimately how it is used or misused. Rising [mistrust](#) between urban authorities, private vendors and residents can reduce the effectiveness and efficiency of services and undermine overall social cohesion and collective action. To be smart and safe, cities need to establish rules to regulate their digital ecosystems and improve the quality of life of their residents.

**Fostering inclusive smart cities means closing digital divides and improving digital literacy.** The smarter a city gets, the more digitally connected its systems and society becomes. In principle, this can reduce friction and increase efficiency. Yet it can also exacerbate digital divides and unintentionally exclude vulnerable groups from essential services and their full participation in social, economic and political life. Certain forms of surveillance technology can also discriminate against minority groups and protected classes, deepening mistrust. Developing situational awareness about digital divides and access barriers is critical to smartening cities.



**SecDev conducts digital safety, trust and inclusion audits to help cities rapidly get smarter and safer.** Getting “smart” can and should not come at the expense of basic accountability, trust and quality of life. By providing urban executives, private sector representatives and civic leaders a better understanding of the digital risks facing cities, digital safety, trust and inclusion audits help identify concrete solutions to enhance the security and wellbeing of all residents. SecDev digital audits focus on three key areas:

- **Safety - map infrastructure security:** SecDev assesses a city’s attack surface for vulnerabilities that could be exploited by a wide range of digital harms both outside and inside the city. This includes digital penetration tests of public-facing digital systems, legacy software across internal systems, and new IoT deployments. SecDev’s approach to mapping attack surfaces extends beyond basic compliance assessments. Rather, SecDev examines the overall systems architecture including policy, technology and systems dependencies across city services and critical infrastructure.
- **Trust - track surveillance exposure and data governance:** SecDev assesses the entirety of metropolitan IoT with a focus on assessing the extent of accountability and transparency across technology deployments. This means examining the privacy implications of both publicly and privately operated CCTV and RFID contact services. By creating digital maps that quantify surveillance exposure and an index tracking privacy, cities can better assess their risks and determine the extent to which existing policies meet basic desired standards. The assessment also reviews municipal IoT strategies, and the architecture of public and private policies related to data harvesting, retention and sharing across selected sectors, including transportation, utilities and other city services. The assessment identifies ways to help municipalities engineer and design-in trust through better data governance.
- **Inclusion - measure digital engagement and literacy:** SecDev examines how city personnel, companies and residents interact and respond to digital services, the extent to which they have access to decent broadband and the relationships between their digital connectivity and urban quality-of-life. This is achieved through ethical anonymized data collection together with rapid surveys and focus groups that enumerate perceptions and identify possible digital divides. A goal is to assess the extent of awareness, usage and trust in city digital systems and their impact on inclusion, representation, participation and overall well being.



SecDev is developing a digital safety, trust and inclusion index for cities that undergo an assessment. This can help urban authorities and residents benchmark their performance in relation to other like-minded cities. SecDev is working with networks of city leaders and city-facing networks such as the World Economic Forum, among others, in order to develop the most appropriate metrics.

## Digital safety, trust and inclusion assessment

Priorities	Approach	Activities
<b>Safety:</b> <b>Map infrastructure security</b>	<p>Attack surface assessment to identify vulnerabilities of a city's public services</p>	<p>An <b>attack surface assessment</b> that identifies exposed vulnerabilities in Internet facing and internal city systems from an adversarial perspective. The vulnerability assessment examines technology (maintenance, patching, architecture), and process (monitoring, incident response and recovery).</p> <p><b>Deliverables:</b> vulnerability assessment report; technical and policy recommendations for ongoing monitoring and response. Index of trackable measures to assess performance</p>
<b>Trust:</b> <b>track surveillance exposure and data governance</b>	<p>Assess the exposure of conn databases and devices that collect urban surveillance data</p> <p>An assessment of Internet connected databases and devices and the data policies that govern privacy at the city and citizen level</p>	<p>This assessment consists of two components: (i) a <b>technical assessment</b> for exposed IOT devices related (IoT, IP cameras or related network devices; ICS) and their related databases (Elasticsearch, MongoDB, Cassandra, SQL, Maria, Redis), assesses the level of exposure and identifies key technical and privacy issues<sup>1</sup> and (ii) a <b>policy assessment</b> that reviews data collection, management, and retention strategies, open data initiatives, as well as procurement policies and third-party use of data created by IOT devices.</p> <p><b>Deliverables:</b> Assessment report summarizing technical aspects of surveillance exposure and recommendations for adjustments to privacy and data governance policies. Index of trackable measures to assess performance</p>
<b>Inclusion:</b> <b>Measure digital quality of life</b>	<p>Assess level of internet and mobile access, especially for protected classes (e.g. vulnerable populations such as disabled, elderly, migrants)</p> <p>An assessment of access, inclusion, and readiness for digital civic participation especially for especially for protected classes (e.g. vulnerable populations such as disabled, elderly, migrants)</p>	<p>This assessment uses passive and active survey methods to gauge civic perceptions of city digital services. Measures include awareness, usage, as well as measures of inclusion (access, education, economic, and other social factors). The assessment presents a measure of digital inclusion, and identifies potential digital divides that impact on participation, representation, and well-being</p> <p><b>Deliverables:</b> Assessment report summarizing key findings, proposed framework recurrent measurement and index to track performance</p>

<sup>1</sup> Score every IP with a framework that the cyber insurance industry in Zurich is increasingly using to [assess risk and calculate premiums](#); (Possibly) report on devices where there are [serious grounds for suspecting that the use of the device endangers national security or national defense](#)"

# About SecDev

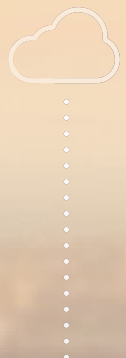
SecDev is an agile research and innovation firm helping clients navigate digital-geopolitical, geospatial and geodigital risk. Our team of experts, forecasters and data scientists support a wide range of clients including public sector, corporations and international organizations in meeting their need for timely, accurate decisions. We transform data into intelligence and identify opportunities to drive digital transformation. SecDev builds value through strategic foresight, data science on demand and intelligence as a service. We are global in scope, fluent in data collection and analytics, experienced in cutting edge technology and singularly results-oriented. We empower clients to make informed choices in a rapidly digitizing era.



To learn more, visit [www.secdev.com](http://www.secdev.com)



5G



Layout

Raphael Durão - [STORMdesign.com.br](http://STORMdesign.com.br)