What If Smart Cities Encouraged Stupid Risks?

Weber, Valentin

Veröffentlichungsversion / Published Version
Stellungnahme / comment

#WHATIF

DGAP MEMO

German Council on Foreign Relations

No. 1 | April 2022

What If Smart Cities Encouraged Stupid Risks?

By Valentin Weber

In 2030, the world's major powers increasingly exploit vulnerabilities in so-called smart cities. In particular, spooks target those cities that operate services based on Chinese tech infrastructure, including Shanghai, St. Petersburg, and Buenos Aires. When a wave of hundreds of such disruptions hits, the major powers downplay this huge incident as a "normal accident" inherent in complex systems. Since the usual suspects – Moscow, Beijing, Washington, Iran, and North Korea – are all negatively affected, none of them seem to have a motive. Indeed, the cause of the disruptions turns out to be much deeper, with roots stretching back a decade. Assessing this hypothetical incident offers real insight into the systemic nature of tech risk.

NORMAL ACCIDENTS IN SMART CITIES?

In May 2030, several Chinese-built smart cities start to misbehave. In Tehran, the police's autonomous situational awareness system goes dark, and riots erupt. In St. Petersburg, the smart traffic surveillance system freezes, creating crippling traffic congestion. All over Germany, rail links come to a halt – a safety measure that is automatically triggered in cases of malfunction to prevent casualties.

Even Shanghai and Beijing experience day-long disruptions that cost eye-watering sums in damages; only a fraction of them will be covered by insurance due to the exemption clauses built into contracts related to smart cities. The United States, Czech Republic, and Lithuania, which had banned Chinese equipment from their core infrastructure, still experience major disruptions in privately held infrastructure related to the Internet of Things. Because Mercedes smart cars rely on algorithms produced by Huawei to identify objects on the road, they set off random false alerts, making it difficult to identify true emergencies. Yet Mercedes, like many companies, sees the disruptions as a nuisance offset by the revenues generated by new technologies. They fail to see the larger systemic implication of such disruptions.

Outside of China, official statements from countries hosting smart cities downplay the event as a "normal accident," the type of which simply occurs in complex systems despite efforts to avoid them. The Chernobyl disaster of 1986 reinforced this message, as did an incident in the nuclear power plant in Doel, Belgium, in 2024.

While it takes national governments a few more weeks to report their findings, the Transatlantic Smart City Alliance, a high-level monthly forum for mayors to share best practices, comes to a rapid conclusion: It is unlikely that China was behind the incident since it drew attention to vulnerabilities in the systems of Huawei that could hurt the Chinese tech champion. Huawei issues a statement that the failures were caused by a glitch in the highly complex software used in most of the affected systems and rapidly provides a patch.

And yet, alternative hypotheses for the failures begin to percolate in Venezuela – home to Caracas, one of the world's most cutting-edge smart cities. True, all major global powers were affected by these disruptions, making it highly unlikely that state perpetrators with sufficient capabilities for such coordinated and highly sophisticated attacks were behind them. And because no system operators were extorted for ransom, a criminal operation is ruled out. But Venezuela is uniquely privy to sensitive information from a close partner: Iran.

Iran's information indicates that the disruptions were not a result of simultaneous multiple actions but a cascade that started in a weak spot in Tehran. Iranian intelligence services assess that this spot was targeted in a state-led action by the United States.

IT ALL STARTED IN TEHRAN

After years of negotiations with the United States, Iran agreed in 2022 to not develop its nuclear capabilities. Despite the agreement, Iran continued

to edge steadily closer to building them up. Tensions between the two countries increased in early 2030 when the US published what it claimed was new evidence of Iran's nuclear ambitions. Teheran refuted the evidence, stating that the US sought an excuse to conduct airstrikes against its facilities.

Russia, which has an interest in drawing the US into another long conflict with Iran, scented an opportunity. President Mariya Putinova, the daughter of former President Vladimir Putin, sought to exploit and exacerbate the geopolitical tensions between the pair, intending to provoke Tehran into an escalatory step. Thus, Russian intelligence disrupted the smart city of Tehran in a false flag operation that pointed to the US. Russia had discovered backdoors in Huawei equipment that it used to its advantage.

Even if Russian hackers were oblivious to the fact that exploiting a very specific code in Tehran would cause ripple effects in other smart cities around the world, including in Russia itself, they succeeded in exacerbating tensions. Yet Russian disregard was only the trigger that led to the widespread outages. The cause was systemic weakness that most countries tacitly accepted because they could use it for the "legitimate" practices of spying and inserting damaging malware.

DO NOT BE TEMPTED TO WEAKEN SYSTEMS

For years, countries have endorsed norms of responsible state behavior in cyberspace, claiming they would refrain from conducting cyberattacks on critical national infrastructure and would disclose system vulnerabilities whenever possible. While these norms have been politically agreed upon by all UN member states, they have been widely violated.

States brazenly continue to integrate malware in networks that they can exploit for spying or in future attacks on critical infrastructure. Major powers such as the United States have defended their actions and made internal assessments of each of their vulnerabilities. If it was highly likely that a backdoor used by US personnel could be exploited by another major power – e.g., China – they patched it. But this risk assessment was secretive, and miscalculations were common.

The vulnerability in Tehran's smart city software was exploited by Russian operators. What Russia did not know is that Huawei itself had been aware of this vulnerability and ordered by the Chinese state to create and maintain it. China had been using it to spy on smart cities and silently accepted the costs of vulnerable systems to siphon off intellectual property from innovation hubs such as Berlin and London.

For its part, the US was aware that Huawei sold its smart city infrastructure to places that are hostile to US interests, notably Iran. Although some advantage was to be gained by US disclosure of what it took to be ordinary vulnerabilities, it instead exploited the backdoors and used them to spy on Iran's nuclear program. Tehran's smart city infrastructure provided the US with valuable clues about the movements of scientists and officials involved in this program.

But what of Germany, which has genuinely pushed for stronger cyber norms? In 2030, Germany's Christian Democratic chancellor, Friedrich Merz, announces a €10 billion package for cybersecurity and launches a major pubic-private parternship initiative to improve the security design and recovery plan for smart cities.

VALENTIN WEBER
Research Fellow,
Technology and Global
Affairs Program

In its "What If" series, the German Council on Foreign Relations (DGAP) envisions the state-of-play in different policy fields in around 2030 and highlights the drivers behind them. The series aims to create awareness of opportunities and risks on issues that may not be top of mind for today's decision-makers but could turn out to be highly impactful. The stories are meant to trigger reflection about Germany's and the EU's strengths and weaknesses and to draw attention toward possibilities for desirable change in a forward-looking manner. For more information, please visit: ***www.dgap.org/whatif***

DGAP
Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
info@dgap.org
www.dgap.org
@dgapev

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 749-5542

Editing Helga Beck

Layout Luise Rombach

Design Concept Luise Rombach

Author picture(s) © DGAP