SciencesPo
CITIES AND DIGITAL TECHNOLOGY CHAIR

Working Paper

> N°01/2019

Beneath the surface of the Safe City: surveillance in the times of Chinese supremacy?

Alvaro Artigas

SciencesPo
CITIES AND DIGITAL TECHNOLOGY CHAIR

The “Cities and Digital Technology” Chair of Sciences Po’s Urban School has been launched in March 2017 to better grasp the impact of digital technologies on urban governance. Funded by four sponsoring firms (Cisco, La Poste, RTE, Caisse des Dépôts), the Chair aims to create new research fields exploring the interaction between digital technology and cities in an empirical and comparative perspective.

Beneath the surface of the Safe City: surveillance in the times of Chinese supremacy?

Dr. Alvaro Artigas, chercheur associé, Sciences Po, Centre d'études européennes et de politique comparée (CEE), CNRS, Paris, France

alvaro.artigaspereira@sciencespo.fr

Abstract

The global deployment of Information and Communication Technology (ICT) firms has been facilitated in recent years by a vast array of new technologies, ranging from communication networks, lighter and faster infrastructure as well as a new sense of available capabilities by real-time communication systems. Drawing on the possibilities allowed by new technological advancements, such as real-time communication feeds, data collection and aggregation, these companies have irrupted and increasingly disrupted the global scene and engaged in previously neglected areas of activity. As a result of this tropism, the provision of security in major world cities has been transformed and traditional CCTV circuits are being displaced and new *safe city systems*, that bear the promise of omniscience in urban territories through enhanced analytics and continuous innovation. Chinese companies, such as ZTE and Huawei have spearheaded this transformation, as a result of unprecedented financial and organizational means, that combine State support, long-time sectoral trajectories and the capacity to test at the global level all-inclusive platforms that seek to promote both security and safety in cities. Far from being gradual, this change spans today across continents and regions, and aggregates previously disconnected datasets that pertain to human security, often beyond socially accepted boundaries. This report seeks to explain the dynamics as well as the limits of this transformation, resorting to these corporations' strategies as to explain how surveillance regulatory frameworks could rapidly evolve in a not so distant future.

Keywords: safe city, China, surveillance, ZTE, Huawei

"We don't have the reputation and networks that our international rivals do. Thus we have no choice but to make strenuous efforts. We can make good use of our rivals' coffee time"
Ren Ginfeng, Huawei founder (Luo et al. 2011).

Introduction

The rise of Chinese ICT firms has grown to be one of the most interesting developments of the recent years in the realm of communications technologies and their territorial applied solutions. Supported by unprecedented national demand dynamics in China and proactive industrial policies, these companies experienced a swift expansion with a controlled exposition to international demand and competition with other state sponsored ICT firms. Tapping into the considerable scale-and at times unregulated- conditions of the Chinese market, these firms have been operating in an environment that enhanced their technical competence moving from the provision of switches to high-end handsets, covering the full spectrum of communication networks and beyond. This national expansion has been replicated internationally, by the active involvement of Chinese authorities into building a rich and diverse network of trade agreements and partnerships. While emerging markets have remained a privileged target, the relevance of Chinese investments in infrastructure for major urban centers has grown to be a global phenomenon, never better exemplified than by the Belt and Road Initiative (BRI) spanning across several continents.

This unique set of conditions for a continuous expansion of Chinese firms across markets and sectors has contributed to a rapid involvement in the provision of ICT related platforms and services such as Big Data and IoT (Internet of Things). This has allowed firms like ZTE and Huawei to rival major global players by providing innovations of their own, and channeling in many respects, the stream of development of related ICT services. Participating to this development, the move towards the provision of integrated city solutions, has made Chinese ICT companies serious competitors of rival well-established western corporations such as IBM or CISCO and foretelling what smart city systems and *solutions* could potentially become a few decades from now. The development of Safe City solutions has become a strategic bet of Chinese ICT firms to long standing problems of cities in sensible hotspots of the planet (Lagos, Marseille, Lima, Shenzhen). These solutions integrate network industries core technological capabilities with ever expanding analytical real-time possibilities, in order to provide an integrated response by city governments willing -and able- to subscribe to these solutions. Safe City platforms mobilize an array of elements such as enhanced CCTV systems, command and processing data centers and new surveillance possibilities such as drones and aerostatic balloons. This move has not however been left unchallenged by national or local actors, and important questions arise in terms of the aggregated efficiency of these systems, the possible threats to privacy and individual freedoms. The pertinence of these interrogations is even more relevant in the least refined regulatory frameworks in the Global South, as they open unforeseen consequences for cities in the absence of proper enforcement of these concerns. The specific connection of these corporations to the Chinese government, whether present or tenuous is another relevant factor nourishing lukewarm reactions by more developed markets, that have a potential for dissemination into emerging ones[1]: in the light of several enquiries driven by countries like the United States, is there too much of a risk to letting a Chinese-driven model of urban surveillance become the new global standard?

This report will explore Huawei's and ZTE's increasingly salient role of Chinese ICT corporations in the sphere of safe city systems by resorting first to a set of conceptual questions raised by the disruption brought by such systems in the current state of development of urban surveillance. By looking into the impact of data aggregation possibilities and its qualitative as well as quantitative evolution in recent years, we will address the tropism of narrow-ended security approaches to all-encompassing ones. In a second part, we will look into the corporations' pathway of development under variable State patronage. Here inter-bureaucratic competition limited and scheduled exposition to competition and internationalization under an increasingly vocal Chinese diplomacy will constitute key explanatory variables of its development. We will ultimately resort to explain the development of Safe City solutions by Chinese corporations as an important part of these corporations Smart City development plans. Research and Development and innovation strategies will be closely examined in order to better explore relevant Safe City developments (Cochabamba, Santiago, Marseille and Montevideo). Pointing to controversial aspects of Safe City implementation in relation to variable regulatory frameworks in the Global South we will interrogate the challenge brought by global strategic ICT players to local governments. Can actors at the metropolis, cities and district level effectively mediate between the appeal of already-set responses, the contradictory provisions of national regulatory provisions and unpredictable citizen reactions to an unprecedented[2] -and increasingly permeating -deployment of technical systems?

1 Cities under control: ICT society interactions and the challenge of safe cities

The issue of security and public safety, understood as functional prerequisite for a thriving, harmonious and peaceful social development, has become in recent years a priority for local as well as national governments, in spite of it being long established as a key dimension of government. Public safety in particular, has been understood as the mitigation and prevention of incidents threatening the safety of the public but also the protection of the public in the face of such incidents. Whereas related to criminal behaviors, natural or man-made disasters, such as crimes, floods, storms, traffic accidents, fire accidents, mass violence, terrorist attacks, water safety, network security, to name but a few, city governments have made public safety and several of its components a priority on their political agendas. As stated by Foucault and more recent authors, surveillance is a power technique that has ultimately become a key governing technique

[1] « EUA advertem Brasil sobre Huawei e 5G em conversas, diz autoridade norte-americana »[US warns Brazil about Huawei and 5G in talks, says US official] Reuters 18/03/2019

[2] It comes from the French verb "*surveiller*" 'oversee, watch' (sixteenth century), from sur- 'over' and veiller 'to watch', from Latin vigilare, from vigil 'watchful'. Interestingly, 'surveiller' carried with it from the start a tension between the meanings of watching over, of taking care of, and of suspicion and control. It also comprised from the start the complementary notion of watching over oneself and one's own behaviour.'Surveillance' is first attested in 1768, in an article (in the economic journal Ephémérides du citoyen) pertaining to the role of the police in marketplaces, drawing together individuals and the state, public and private interests, law and law enforcement.

of state authorities, corporations and individuals: ‘the focused, systematic and routine attention to personal details for purposes of management, protection or direction’ (Lyon 2007, Foucault, 2004). Surveillance refers thus to “any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered” (Lyon 2001). Surveillance can be thus understood a consequence of processes of modernity (Giddens 1985) and has become an inherent part of our network societies (Castells 2001). While much debate has erupted in Western societies about the risks pertaining to the development of increasingly intrusive surveillance systems[1]- the political will to implement digital surveillance technologies through a massive accumulation and processing of digital data has been an unbroken trend.

The deployment of surveillance technologies stem from the authorities’ will to exert increasing levels of control and oversight of public spaces, as to curb security related issues, ranging from common theft to terrorism. This evolution has an implicit contradictory relation, as the many dimensions entailed in concepts of human or societal security (Kaufmann, 1973), comprising economic and social, health, political or environmental conditions, among many others, seem largely side-lined. Policy debates have been strongly influenced by the media and its territorial coverage, narrowing down the discourse pertaining to organized crime, terrorism and border security issues: by this doing, they participate of a specific process of politicization, where a new interpretation of governmental intervention is legitimated within the social sphere (d’Arcimoles & Borraz 2003). While in previous decades, civil society and local governments spearheaded the demand of security, this has radically changed in recent years due to the greater complexity of its meaning at a city level, encompassing several dimensions and spanning across several levels. Collective action dynamics have been dented in the process as a result of the lesser readability of this issue, and other non-state actors, from the network industries have increasingly occupied the public space. Building on new technologies, the revolution of ICTs in the 1990s and 2000s and the subsequent push of big data analytics (Ejaz 2019), the playing field has been irrevocably altered to the benefit of firms’ driven *city solutions*.

The demand for security *and* surveillance has been pervasive within capital cities, leading to an exponential increase in funding in recent years, as to transform, innovate and enhance the available means of control. In a global economy, metropolitan areas have become key territories where the consequences of disruptive events are exacerbated, and complex social interactions depend on security becoming -if it is not yet the case- a priority in the political agenda. Because crises put critical infrastructures under stress (Quarantelli 1998; Gomez-Ibanez 2003) political control over finite urban territories has become the most tangible dimension of it. It has also become a relevant testing ground for innovations that might -or might not- define the scope of governmental interventions to come, as well as the sphere of individual liberties. It is thus in cities that an increasing scrutiny of every-day life is justified today by the necessity of collecting personal data and meta-data that would allow the authorities to intervene in a targeted manner (Amoore and De Goede, 2005), allocating resources efficiently and anticipating even possible existing

[1] The ‘Snowden revelations’ of mass-surveillance programs brought into the light of day the ever-increasing and far-reaching capabilities of digital surveillance technologies (Greenwald, 2014).

threats. Referred as the “dream of targeted governance” (Valverde and Mopas, 2004), local administrations, firms and governments would, within such as framework, increase their capacity to collect and process large population data-sets; thus exploiting the full range of security related possibilities of big data (Andrejevic and Gates, 2014)[1]. Another trend closely related to this one pertains to the use of commercial related information that would increasingly be used beyond the scope of its initial purpose, for the purpose of security goals (Bellanova and Duez 2012). Often related to geo-localized mobility and transportation flows (air/train/automobile) these enhanced profiling capabilities underwent political controversy over the last decades in liberal industrialized societies (Huijboom and Bodea 2015).

By and large the development of surveillance technologies has espoused urban development at the global scale, expanding its reach by an ever-increasing set of firms that have made security accessible and affordable by cities around the world. The impressive development of ICTs and the possibilities of on-line real-time transmission capabilities by individual electronic devices has substantially increased the appeal of surveillance and its scope, facilitated in major capital cities by the early adoption of CCTV systems. The array of “solutions[2]” available for city governments today reveal the potential of cognition and control of populations in public spaces and has built on a diversified set of established network firms. Both having originated in consolidated markets (IBM, CISCO, NEC) and recent -but rapidly growing ones- (Huawei, ZTE), these firms have conquered significant shares of the world markets and challenged in the process privacy provisions enshrined in constitutional charters. This evolution, raise uneasy questions: are the potential infringements to privacy a necessity -if not an imperative- for security in cities today? Are the present investments consented by local authorities justified in the face of the still blurry results that these platforms could bring?

The uptake by State authorities of mass-surveillance technologies goes hand-in-hand with a more or less explicit reformulation of national security, a classic definition that has morphed into increasingly profiling within territories as a form of preemptive protection of the State and citizens (Bigo, 2006). The everyday practice of digital mass-surveillance relies however on a de facto transnational cooperation among security networks (both private and public) which shows the limits of the controlling ambition of the local, let alone national governments, and the imperatives of interdependence in the digital age (Bauman et al., 2014).

1.1 Data aggregation surveillance systems: a narrow security approach to a multi-faceted risk?

Surveillance has moved from ad hoc responses (Boesma & Fornio 2018) towards crisis management systems, where polymorph crises (Comfort et al. 2010) and ways of managing them

[1] In the case of the EU, for example, communitarian institutions have adopted the ‘EU PNR scheme’: a pan-European program to collect, store, exchange and process passenger information (Directive (EU) 2016/681).

[2] This term is used as such given that it has become a commonplace concept within the ICT sector for the definition of information-related platforms drawing their analytics from large data-sets facilitated by internet technologies.

through ‘big data’ is becoming increasingly the shared resort of local and national governments. Datafication as a new paradigm in science and society refers to the transformation of social action into online quantified data, thus allowing for real- time tracking and predictive analysis for surveillance and crisis prevention purposes (Van Dijck 2014). Given this multiple causal origin of crisis, combining unclear effects and resolution (Van der Vegt et al. 2015) access to information becomes a crucial element of *resilience, response* and *relief* in spite of the potential to easily leading to an extensive monitoring of large pans of cities’ populations. City systems that look to be reactive to risks need therefore an integrated management of information flows and operational networks to build an effective crisis response organization (Pan et al. 2012)[1]. Therefore, processes aimed at collecting, analyzing and sharing information have become mandatory steps of standardizing information products at the local scale to support coordinated responses (Oh et al. 2013).At the same time several major cities in the world have resorted to crises, disasters and social disruptions as a window of opportunity to consistently and legitimately collect and analyze citizens’ data on a large scale (Fonio et al. 2007). The use of crisis information systems, like networks of hardware and software in order to collect, sort and process data is not however neutral, but related to the way crisis information management is organized and legitimized. Information management of increasingly complex surveillance systems at the city level imply however that data has to be translated into “actionable” information that can be used by local governments (Wolbers and Boersma 2013).

Bottom up information systems are probably the most relevant innovation of surveillance platforms that cater for these risks and stem from present technological developments, in particular pertaining to social media platforms. Citizens have thus the ability to generate bottom up information networks (Yates and Paquette 2011), providing a qualitative shift of responses provided by these systems. The availability of new data for effective crisis response is not devoid of pitfalls of its own, as serious concerns exist to this day in relation to the information standards and accountability mechanisms this new data generates, thus adding to the burden of crisis management (Turoff 2002), or even information overload (Hiltz and Plotnick 2013). Scaling information flows is no less a quintessential part of these new aggregated/encompassing *solutions* that seek the ever-continuous expansion of data production sources, exploiting the aggregation possibilities coming from individuals and IoT connected devices. While metropolitan, city or district levels may want to stay in control of this process, by harvesting and integrating the various and heterogeneous data sources in their information management systems, their capacity to ensure harmonized responses is still very much a work in progress and grows increasingly disconnected from the existing corporate responses.

Thus, with the increased availability of data, new challenges are added to crisis responses at the city level. Important concerns arise pertaining to the nature of information standards and accountability mechanisms, information overload (Hiltz and Plotnick 2013), but also the lack of inter-operability between the ICTs used by these systems and the communication sources used by citizens (Truptil et al. 2008). Not least relevant, the issue of limited human processing

[1] Referred by some works as crisis information ecology of dynamic information streams (Turoff et al. 2004; Van de Walle et al. 2009). Information ecology thus refers to the total information environment of organizations (Davenport and Prusak 1997)

capacities, or human bandwidth point to a still unresolved dimension of the interactions between individuals and these systems (Patrignani & Whitehouse 2018)[1]. The use of big data requires adequate data and information management (Pries and Dunnigan 2015): the fact that most cities in the Global South suffer from underdeveloped data analytical skills by the administrations in charge of handling information flows (Boersma & Fonio 2018) is a major concern. Both the great majority of city residents remain oblivious of the nature of their data interactions and data officers are still a rare currency at the local level for most of South East Asia, Africa and Latin America, which can be explained by the priorities allocated to heavy infrastructure promotion (Artigas 2017). Databases can moreover generate patterns that have predictive power for crisis operations -but not necessarily- an automatically explanatory power, thus requiring further processing (Andrejevic 2014). It is the extraction of structured data from unstructured inputs that is the main hurdle for those who want to use big data in the context of crisis response (Castillo 2016).

The resort to big data for crisis situations is not devoid of other problems too. Like any ICT trend it has the potential for triggering processes of change but can also easily become an empty promise (Meijer et al. 2009). A real epistemological problem with big data lies in detecting small and meaningful patterns: there is however a potentially more important operational problem that lies in assessing to what extent real-time crisis big data can enhance disaster response instead of turning into a big data crisis due to the challenges of working with new data sources. Hence, the debate on the use of big data is concerned with methods used to make sense of it and decisions made upon the interpretation of patterns.

All in all, surveillance -and by extension crisis related-data harvesting and processing should be assessed in terms of its capacity to produce tangible changes beyond the merit of just being available: while these changes have still to be assessed, real-time analytic have the potential to become a powerful deterrent. They can transform, if they become a recurrent government tool, procedures and interpretation frameworks. Thus, surveillance lens helps us to understand how city management today has the potential to become a cog of what has been called the “surveillance society” (Gandy 1989; Murakami Wood et al. 2009; Ball et al. 2012). Although the State and state agencies have been playing a major role in surveillance societies (Haggerty and Samatas 2010; Boersma et al. 2014), surveillance is about much more than State control. Surveillance practices operating principles and scope are continuously being determined by the development of state-of-the-art electronic means for collecting and treating surveillance data and meta-data, personal data storage capacity, and algorithm-based analytics (Cardon 2015).

1.2 Citizens surveillance purposes: the limits of the all secure utopia?

The outcome of surveillance related systems, like safe-city platforms, is very much dependent on citizen interactions and above all cooperation, bound within territory bound entities. While the speed of data flows has increased, databases have become decentralized at the city level and easily accessible, leading to individuals also being more easily traced. The Edward Snowden case

[1] Some authors point to the necessity of considering other sort of interactions that could enhance the effectiveness of these systems, thus « ...human beings could use technology to improve horizontal communication on a many-to-many basis, and not just be limited to the use of vertical communication as in broadcasting » (Patrignani & Whitehouse 2018, p.51).

has revealed how the world wide web has enabled a global networked form of surveillance and how the analysis of data has potentially undermined privacy and civil liberties by governments, compromising democratic foundations (Greenwald 2014; Fuchs et al. 2011). The use of information for surveillance practices, in this respect, is not just the outcome of the use of technologies, such as the storage capacity, but of specific approaches to risk and security management by concerned industries and of consumer clustering in marketing (Andrejevic 2014; Andrejevic and Gates 2014). Recent revelations about the extent of collection, processing and analysis of data and metadata at times of specific events in the name of security have raised concerns that there is a dangerous trade- off of privacy and liberty against safety and security (Büscher et al. 2015). Data collection has path-dependent dynamic of its own: it is hard to resist the urge to gather more data on crises just because it is possible and potentially useful for improved crisis response[1].

Citizen surveillance platforms are bound however by alternative and often ambiguous interpretation as to the means, the purpose and overarching capacity of citizens to add layers of unpredictability. It is fundamentally the opposition between control vs social empowerment: the opposition or "dialectic of means and ends" (Friedewald et al. 2017) where technologies are either neutral or where their use is shaped by specific interests (governments, corporations) and citizens, which have the capacity to alter the use of technological innovations for unintended purposes. This does inevitably cast uncertainty as to the purpose of surveillance platforms and raises an important question as to who is in charge of innovations within such an environment. Secondly, the opening as to what is 'socially useful' to individual citizens and urban societies can hardly be established a priori and remains an object very much in flux. This further opens to questions about the means to determine – in diverse groups, institutions or societies – the socially binding delineation of what is true and of what is good (Latour 2012).

Whether such systems can usher "activities performed by citizens broadly and primarily to produce socially useful, empowering knowledge" – rather than as a means of control (Cas & al. 2017) will very much depend on the citizen's capacity to funnel knowledge production proactively towards the protection of common goods' (Tallacchini et al. 2018). Can the perspectives and preferences of citizens participate of such processes, given that, theoretically at least, they are the main beneficiaries of security measures but also the probable targets of surveillance programs? The current framing of these programs has led for the most part to citizens being expected to accept a narrow definition framing of security and to support henceforth the implementation of surveillance solutions. Moreover, there is an implicitly visible semantic slide where the territorial dimension dimension of security, referring to abstract entities' priorities (livable cities, safe districts, the territory), to more tangible dimensions pertaining to individuals or the collective (the collective/the individual).

[1] And the same predicament could be extended to the purpose of accumulating personal data for ulterior purposes, as shown in the recent Facebook scandal that erupted in March 2018.

2 ICTs multinationals and the development of Chinese Safe City technologies: *a capite ad calcem*?

The intertwining of personal data, local government as surveillance platforms is of a complex nature, as outlined in the previous section. In order to understand the dynamics behind the adoption of city surveillance platforms worldwide, it is important to address at a preliminary stage the industry dynamics that have favored its development and the interplay between State and ICT companies in the way of legitimizing these solutions. More specifically, looking into how Chinese ICT companies fit into the transformational flow of ICTs expansion at a global scale will provide the necessary perspective to assess their impact in the promotion of these solutions today and the levers to promote it at the international level. As we will see here, Chinese ICTs corporations have played an increasingly active role in the field of Smart City promotion and Safe City solutions, a new area increasingly determined by patterns of evolving data network construction and aggregation capabilities, government policies and regulatory frameworks. They have actively contributed to the emergence of specific arrangements that have favored in turn corporate strategies leading to investments towards innovation processes and related new technologies.

2.1 Chinese ICT firms in a global context of corporate contribution to communications network expansion

In a common pattern both pertinent for developed and developing nations, governments have set the blueprint for the organization of data communication and the necessary infrastructure through a set of regulatory decisions. Having contributed to the emergence of specific preferences and incentives for related economic actors engaged in this transformational process they have opened avenues for policy intervention and new management possibilities for urban innovation systems. Scientific organizations, think tanks and foundations at time supported by public funding, have also participated of this process as important stakeholders of this process in key emerging countries[1]. As economic opportunities and technical possibilities in data transfer became apparent, ICT and network industry firms soon came to foresee the potential economic returns and were an instrumental component of the network's expansion. Over the subsequent decades it has led slowly but surely to the development of specific technologies that have turned cities into their main operational testing ground. The provision of specific incentives by national authorities and regulatory agencies contributed to the deployment of the network's physical infrastructure as well as to the emergence of specific eco-system of telecommunication companies through specific ICT sector unbundling (Jordana et al. 2006).

Such an evolution has triggered an important diversification of ICT companies that partake of a highly, intensely competitive data eco-system where factors such as price, functionality, service quality, and the development of new products and services have become the main drivers of

[1] As showcased by the publication of academic publications linked to urban innovations by strategic research foundations from these countries, as the Skolkovo foundation in Russia. (Winden W. van et al. 2014)

corporate strategies. These firms have proceeded on this account to the development of complex business-models that include the provision of encompassing urban related services, grounded on smart technologies and the ever-growing array of related *smart city* and *solutions*. Chinese ICTs are important stakeholders an increasingly open competition with long-established telecom companies, such as Alcatel-Lucent, Cisco Systems, Datang Telecom Technology, Hewlett-Packard, Juniper Networks, Ericsson, Nokia Networks Solution, Motorola Solutions, NEC, to mention just a few[1]. The intensity of the competition within the ICT industry has been exacerbated by the rapid technological development within this sector and the possibilities opened by consumers' everyday devices[2]. Furthermore, the industry's consolidation, through a process of mergers and acquisitions worldwide, has largely increased the bargaining power of telecommunications carriers, which increasingly determine the survival prospects of these companies[3].

A quick glance at State-firm interdependence in the industrialized world can provide an interesting perspective to the deployment of these systems in China and the constitution of Chinese ICT companies. In this sense, the sequence ushered by the Defense Department's Advanced Research Projects Agency (ARPA) in the United States is extremely relevant. This agency organized the earliest form of a large-scale data network in the 1960s, facilitating the development of specific technologies and encouraging a more intensive use of telephone lines[4]. It took a couple of decades for private companies (such as AT&T) but also specific foundations and educational institutions (the NSF or UCLA) to develop specific commercial and non-commercial usages for data management and to actively participate in the network's expansion. By the late 1980 private companies actively moved to developing network infrastructure as fiber optic cables offered new possibilities to transfer data over telephone lines and increased the commercial viability of a more active private involvement into what remained a system essentially owned and operated by a government agency[5]. Over the following decades the reduction of operating and consumer costs and falling access charges, favored the explosion of new electronic content and services, accelerating innovations processes pertaining to new alternative modes of transmitting data, such as fiber optics. Other operations like Minitel in France in 1982 followed similar paths to expand their data network: being State-funded and relying on the government-owned telephone network for transmission, its expansion and service deployment was in part curtailed by the high tariffs and high rates for connection charged by France Telecom to private ISPs. It was only after pressures

[1] As portrayed in the OECD Digital Economy Outlook 2017

[2] Mobile phones today are released with accelerated technological functionalities to a market whose consumers have heightened expectations for technical advancement. This results in short life industry cycles with lower returns on investment, which leads inversely to the strengthening of the -already-predominant players in the industry.

[3] Which Kim and Mauborgne (2005) label a Red Ocean traps in the Asian context.

[4] The ARPANET project developed equipment to break down and reassemble data packets, and to route the data along the most efficient path. Though the system was funded and managed by the government agency, it depended on leased telephone lines from a private company, AT&T, to transmit data long distances.

[5] But other private companies, such as AT&T, MCI, and Sprint, which had their own data pipelines already in place, began to offer full commercial services on parallel network infrastructure. In 1991, the NSF moved to allow full private ownership and commercial operation of its network, with Internet service providers (ISPs) allowed operate their own backbone networks. The NSFNET was dismantled, and government ownership of the data network ceased.

stemming from the public at the beginning of the 2000s that access charges would undergo a significant reduction. In the case of Japan finally, the private sector competed from the outset with government plans to build a data backbone: here universities, supported by private corporate interests, worked together setting up data networks linking campuses, research centers, and companies at the end of the 1980s.

For developing countries several of these variables contributed, albeit in a different sequence to the consolidation of competitive ICT related firms. For fast-growing economies in Asia though, data networks, like telephone systems, were initially the property of the State and only came to grow because of the intertwine of regulatory, capital and technological possibilities. The Chinese case ushered a model of its own, combining rapid growth under a continued –albeit competitive-State ownership of the network hardware. The Communist Party of China overwhelming capacity to steer this process led to a controlled environment where State institutions set up general development provisions pertaining to the network infrastructure, but quickly expanding to the regulation of Internet services and content provision. The development of Chinese ICT companies was facilitated by a selective State intervention in the territorial deployment of networks -some regions before others for example- inter bureaucratic competition, but above all, by the continuous protection of ICT infant corporations. Chinese telecommunication companies would be consistently shielded in the early stages by more favorable market conditions at home and by the adoption of selective -and de facto protective- forms of internationalization. We will see how this particular set of conditions for each one of these corporations was instrumental in the development of specific safe city systems, platforms and solutions.

2.2 The case of Huawei: a tale of market supremacy and selective State intervention

The story behind Huawei Technologies Co. Ltd. Development is one of a continuous development of capabilities across carrier network, enterprise and consumer segments from the time of its foundation in 1987 by Ren Zhengfei, a former civil engineer in the People's Liberation Army (PLA). The importance of this company lies in its fast-growing trajectory over three decades, its impressive territorial reach and its resolutely global dimension today. It also matters, for the purpose of this study, to understand how the development of safe city solutions has been the predictable outcome for these global telecommunication corporations, given the impressive financial clout, innovation capacity and strategic global positioning.

Being one of the largest ICT solutions and services provider in the world, and a front runner innovator in 5G technologies it has been increasingly under the spotlight of Western authorities and the United States in particular[1]. Its networking equipment serves 45 of the world’s 50 largest communications operators, with BT Group, Vodafone, Orange, and T-Mobile amongst its most relevant customers. In the 1980s, China’s telecommunications industry relied mainly on

[1] This issue has as of today crossed the boundaries of national policy decisions.
See “US threatens to cut intelligence sharing with Berlin over Huawei”, Financial Times, 11/03/2019, https://www.ft.com/content/00dc81a6-4417-11e9-b168-96a37d002cd3

acquisition of technology and equipment through imports[1]: it is at this time period that Huawei reverse-engineered foreign products and use that process as the foundation to develop more complex technologies. At the later stages, Huawei placed strong emphasis on in-house research & development (R&D) which combined with an aggressive pricing policy allowed this company to deploy its products and solutions over 140 countries[2].

Table 1: Overall revenue and total assets of Huawei from 2007 to 2018 (in US$ Billion)

Year	Revenue of Huawei	Total Assets of Huawei
2007	14.75	28.64
2008	19.69	31.02
2009	23.46	35.74
2010	29.21	39.05
2011	32.63	49.56
2012	35.23	28.64
2013	38.24	31.02
2014	46.11	35.74
2016	75,10	63,88
2017	92.50	66,31

Source: Huawei Financial Results (Huawei, 2014, Huawei 2018 Author compilation)

The specificity of Huawei in relation to other ICT companies from China was its early jump , already in the 1990s, into the development of its own in-house technology, in direct opposition to Shanghai Bell, its main competitor at the time which had relied on a more traditional joint venture approach to import and learn from their foreign partners[3]. Huawei started as a private firm, which placed it from the beginning at a disadvantage in relation to state-owned enterprises (SOEs) in terms of financing. from the government-owned banking system. This predicament forced this company to engage into technologies that would fit the Chinese market specific demands -like in-house large-scale telecommunication switches in 1993. By the time, Huawei managed to secure the first telecommunications network contract by the People's Liberation Army. This connection, while being a typical feature of big communication companies in China, would greatly contribute in the 2010s to raise suspicions of State agencies meddling at the time of securing overseas contracts.

[1] At that point in time, the adoption rate for fixed line telephones in China was less than 0.5 per cent. These fixed line telephones were mostly deployed in government agencies, infrastructures, companies and schools. The great potential in the Chinese fixed line telephone industry attracted many internationally renowned players, such as Ericsson, Motorola and Nokia. Huawei started out by reselling imported telecommunications switches from Hong Kong, a type of fixed line telephone system that switched connections between several branches of telephone systems and also linked phone lines. The system was used to connect internal lines to an external line.

[2] By 2014, Huawei recorded profits of USD 5.5 billion (Huawei Financial Results, 2014).

[3] R&D to production staff ratio. During this period, Huawei had only 200 production staff but over 500 R&D staff (Ahrens, 2013).

Another important step was its territorial experimentation, moving its commercial activities to lesser urban centers, in order to supply switches to towns and smaller cities in rural areas[1]. In the frenzy of major urban city center development at the time (Lincoln & Tao 2016) the former were considered uninteresting to international communication firms at the time (Nankervis et al., 2013). By 1995 Huawei established research centers in Shanghai and Beijing to focus on mobile communication technologies from companies such as Motorola, just before Chinese government started to explicitly support domestic telecommunications companies by removing import policies that favored foreign companies and facilitating financing to the domestic market. Thanks to increasingly narrower relations with government officials Huawei won large contracts on domestic telecommunications infrastructure development for the national railway system, becoming over the next decade the market leader of telecommunications switches and optical devices in China. The consistent investments in research and development, enunciated on Table 1 account for this progression, that have led to the crowding out of the local market mobile technology network and positioned this company as one of the three top corporations behind Amazon [US$ 22,6 bn] and Alphabet [US$ 16,6bn] in terms of R&D in 2018.

Table 2: Total R&D spending (million US$) and R&D in percentage of revenue (2006 – 2017)

	Alcatel-Lucent		**Cisco**		**Ericsson**		**Huawei**	
Year	*Spending*	*Per cent*	*Spending*	*Per cent*	*Spending*	*Per cent*	*Spending*	*Per cent*
2006	1929.82	11.9	4067	14.3	4028	15.3	850.39	10
2007	4314	16.5	4598	13.2	4466	15.4	1285.77	10
2008	3837	16	5325	13.5	4263	16.1	1534.48	8.4
2009	3622	15.3	5208	14.4	4621	16	1954.32	8.9
2010	3532	16.7	5273	13.2	4670	15.5	2674.70	9.7
2011	3200.44	16.1	5823	13.5	4853	14.4	3807.69	11.8
2015	N/A*	N/A*	6207	12,6	4131	14.09	8700	15
2016	N/A*	N/A*	6296	12.6	3702	14.22	11000	14.6
2017	N/A*	N/A*	6332	13,1	4043	17,10	13800	15

Source: Ahrens, 2013, and the author's compilation.

* Alcatel Lucent merged with Nokia in 2015/ ** Current projections

While Huawei's technology development has matched other corporations' strategies in East Asia (Deyo 1987) the process of reverse engineering of Cisco Systems and Fujitsu has been tainted by accusations of improper technology acquisition[2]. The outcome of these cases forced Huawei to alter its processes -such as source codes- in order to maintain its operations abroad.

[1] For example, variable power supplies in rural China required significant levels of network customization for the telecommunications switches.

[2] Reverse engineering, or the acquisition of technology by taking apart and studying an existing product in the market, is permitted under Chinese law and not considered intellectual property theft. This didn't prevent Motoral and Cisco systems to file complaints against Huawei over the theft of intellectual property. See Motorola claims espionage in Huawei lawsuit, Financial Times 22/06/10 https://www.ft.com/content/616d2b34-953d-11df-b2e1-00144feab49a

Irrespective of this and building on an increasingly innovating capacity and in-house original products, Huawei managed in time to become the world's first applicant for patents[1]. The span of innovation of this company has in this sense experienced an ever-growing expansion ranging from seamless mobile broadband connections on China's high-speed trains and in-flight Wi-Fi service for airline passengers, to bendable-screen smartphone sets in the most recent version of the Mobile World Congress in Barcelona, in February 2019.

Today, Huawei's research and development caters for three main categories of products and services which are: operator carrier networks, enterprise solutions and consumer products and services. At the beginning, Huawei's fixed phone line switches were the first in-house products to be developed. These telecommunications switches were highly adaptable and became a mainstay in the Chinese market, still accounting in 2018 for much of carrier networks sales. This product segment also includes a wide range of wireless networks, fixed networks, telecom software and core networks as well as services solutions to telecommunications operators. The second segment, which is the enterprise business segment, is engaged in developing and manufacturing ICT products and solutions including enterprise network infrastructure, cloud-based data centers, enterprise information security as well as unified communication and collaboration solutions for government entities. This segment has invested consistently in the public utilities as well as the energy, power, transportation, finance and other industries, looking specifically into related smart solutions. Over recent years, given the impressive progression of R&D in network and enterprise telecommunications solutions (See Table I), Huawei has managed to become a global market operator and developer. Huawei has lastly been raising its investing levels since 2012 in its last sector of activity, that is the consumer market of mobile broadband devices, home devices, tablets, smartphones as well as related applications. The company has been rolling out mobile devices to compete with companies that have aggressively engaged into a process of mergers and acquisitions.

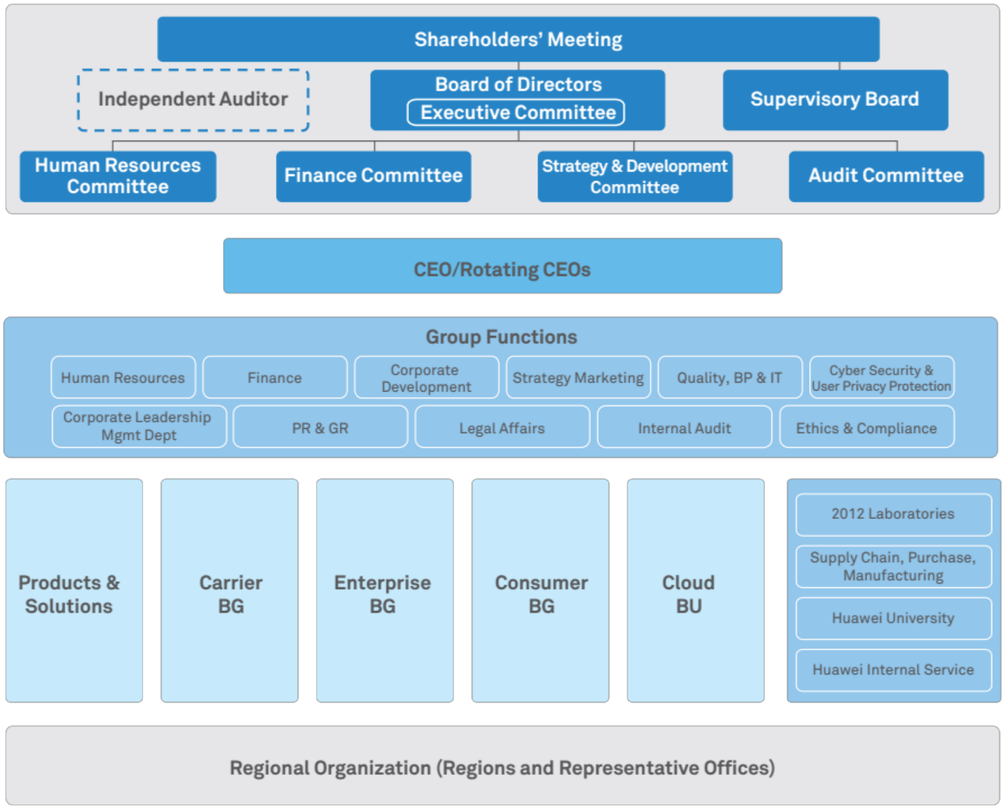
By 2015, Huawei employee count reached 170,000 staff, including more than 40,000 non-Chinese nationals. From 22 regional offices and over 100 subsidiaries around the world, approximately two-thirds of its revenue come from international markets. Huawei has also filed over 49,000 patents, as part of its R&D effort (Ahrens, 2013, Huawei 2013), making this company one of the world's ICT most significant firms in this sector. Despite its growth, Huawei is facing a number of issues regarding the quality of certain components, a criticism that has been however reverted in recent years. More importantly however, Huawei's aggressive low-price approach, has directly resulted in eroding profit margins in some markets, pinpointing a classic pattern of Chinese multinationals seeking a rapid, albeit unstable international expansion. In the face of spiraling R&D expenses, this could compromise the company's future investment capacity, in particular given the current predicament of widespread suspicion of security breaches building on the US fierce opposition to any deployment of the firm's technologies on his national soil[2]. As it turns out, Huawei's controversial technology development, has been increasingly combined with intellectual

[1] In terms of international patents in terms of number of filings, according to WIPO data (Shih, 2015).

[2] Which has led to Beijing's authorities retaliation. https://www.theguardian.com/world/2019/mar/07/huawei-sues-us-over-government-ban-on-its-products Consulted on 3/8/2019

property theft allegations and close links to the People's Liberation Army (PLA) and the Chinese government. This has left certain western countries and its closest allies out of the reach of these spearheading technologies, raising uncomfortable questions for the future regarding technological support for innovations that closely relate to city development[1].

Table 3- Huawei's organizational chart (as of December 31, 2017)



Source: Huawei Investor Report 2017 (published 2019).

2.2.1 The stepping stone of Safe City solutions: R&D and strategic corporate alliances

Huawei has today about half of its staff working on R&D activities with over 16 R&D centers and 28 joint innovation centers around the world. This has allowed this company to move swiftly beyond the scope of traditional network equipment towards wireless technologies, data communications and to consequently develop specific enterprise and govtech solutions. Building on previous successes in 3G network, Huawei is a driving force of 4G LTE (Long Term Evolution) network development[2]. Having started to develop a 5G standard, the company expects this standard to be commercially delivered by 2020 (Forbes, 2013) and significant strides have been made in 2018 and 2019 for its quick deployment. The 5G standard will give mobile broadband speed up to 10 gigabytes – 100 times faster that 4G mobile -opening unprecedented possibilities for government related solutions, in particular in terms of data aggregation, streaming, real-time analysis.

[1] Ericsson chief warns fears will add to Europe's delay, Financial Times, 19/02/2019

[2] See https://www.agenceecofin.com/industrie/2908-13230-huawei-leader-du-marche-mondial-de-l-equipement-lte

Beyond these technological breakthroughs, lasting govtech solutions and all-inclusive kind of platforms have demanded robust firm partnerships, as to control the development of the different components of the innovation chain pertaining to systems that rely both on state-of-the-art hardware, wireless systems, software platforms and analytics capabilities. These partnerships have become a pillar of the overall international venturing strategy: by internalizing the partner's technology, Huawei has managed to develop a more efficient and cost effective method than developing in-house innovation, while at the same time increasing it has been able to enhance the company's reach (Luo et al, 2011). Strategic alliances have been made building on this principle, with universities and companies, including competitors such as Intel, Texas Instruments, Motorola, Oracle, and Sun. For specific processes such as international management operations, Huawei's CEO have thus not hesitated to spend up to 3% of revenues buying advice from Western companies like IBM (The Economist, 2012). The experience of Huawei's Open Labs is in this respect an interesting development, which has allowed the native solutions to be in phase with real business needs of local customers, hence allowing the joint development of industry, government-specific solutions that meet the demands of the concerned entities and have the potential of anticipating them. Currently 13 labs are in operation where Huawei collaborates with more than 400 partners across Europe, Latin America, the Middle East, South East Asia, and China. Most recent developments go in the sense of exploring future use cases for mobile applications, to drive business and technology innovation, and to build application-centric networks[1].

Safe City *solutions* have been the company's response to a demand for public safety and the encroachment of new dimensions of safety and security that have been bolstered as an imperative to be addressed by new forms of city governance. The development of Huawei's Safe City has evolved from early stages, when it was focused on the deployment of video surveillance, to a more complex set of goals and technologies that aim at a complete public security management. Safe City solutions, as implemented in Huawei's recent operations, have enabled contracting local governments to test and ultimately deploy crisis prevention capabilities and emergency management mechanisms through a system that combines a multi-dimensional and intelligent security platform. Here the principles of awareness, visualization and collaboration are key operational elements in the way of the implementation of this platform[2]. At its very core, a unified command and control center supported by a Hexagon Safety & Infrastructure Computer Aided Dispatch (CAD) technology, improves crisis prevention and emergency management. In order to better support the system's reliability, Huawei provides contracting parts with a related state-of-the-art industry platform as well, available in the cloud. This platform improves distributed caching[3] technology, helping the concerned operators discover relevant information in a matter of seconds,

[1] In November 2016, was announced the creation of X Labs, a new research program that looks to bringing together carriers, technology providers, and vertical industry partners to form an open collaborative ecosystem.

[2] Huawei Investor Report 2016.

[3] Cache is a special high-speed storage mechanism that can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: *memory caching* and *disk caching*.

irrespective of the number of simultaneous views - estimated to up 10,000 users simultaneously, according to Huawei's official sources.

IoT (Internet of Things) technologies have become a vital component of smart systems raising the issue of one-way feedback from users/citizens that was addressed in the previous section. Insofar IoT devices allow for communications between different electronic devices in order to achieve increasingly expedite data exchange, they are a fundamental operational component of Safe City tangible deployment. They feature and integrating high-definition streaming video from terrestrial or airborne sources (like drones), personal mobile devices using Huawei's advanced communications infrastructure and intelligent analytics. Comprehensive sensing implementation stemming from multi-dimensional security protection relies on IoT ecosystems which can connect all devices, thus facilitating enhanced analytics and prediction, and faster responses when handling emergencies. One of the reasons behind the expansion of these systems lies in the possibilities of cross-analyzing different sources of information: here new devices interact with more traditional data feeders such as CCTV platforms which have seen their technological capabilities increase substantially in recent years[1].

IoT systems are endowed however with an important component of risk inherent to their technical complexity, which has encouraged Huawei to look for business partnerships with global security solutions providers such as GSIA, SAP, Intergraph, Telmex, THALES, and Netherlands VCS. IoT-connected information management systems build on a number of technologies and applications that need be user-friendly and need to comply as well with national regulatory frameworks pertaining to the handling of meta-data and personal data protection. For Huawei's Safe City solutions these technologies operate as follows:

Table 4: Safe City technological components.

Technology	Main function	Resources	Issues at the City level
Multi-Service Integration	Integration of existing subsystems	Access control capabilities to integrate the data, signaling control, media transmission, and terminal application layers.	Infrastructural network capabilities, brownouts management, bandwidth available by Internet providers
Large Sensor Populations	Streamlining and coversion of different sensors feedback	Parsing, format conversion, and storage configuration for the massive amounts of information collected	Non-cooperative behaviours,
Rule-Based Coordination	Sequencing of IoT (Internet of Things) safety and security system	Preset rules that specify the actions to be taken by associated subsystems	Intersection of subsystems with decisions stemming from police, national guard or emergency teams

[1] These video platforms have evolved from closed, special-purpose workstations to open and shared information systems, often optimized for integrated command and control for emergency response, and proactive detection of incidents.

Visualized Command and Dispatch	Graphic rendering of incidents' location and scope of impact	Geographic Information System (GIS) 2D and 3D graphical information about emergency situations	Processing capabilities by operators,

Author's own elaboration from Huawei's official documents and web resources.

The decision to turn safe city initiatives into a specific domain has been driven by the increasing attention stemming from local governments and the possibilities opened by Smart City innovation capabilities. Building on the previously mentioned partnerships, and ever-expanding expenditures in R&D Huawei has developed systems that claim to address public security concerns within cities as well as supporting early warnings for human-generated disasters like war, terrorism[1] - and environmental pollution. While Safe City as a platform could theoretically provide an effective management of the aftermath of these events, it still has has a limited global deployment, given the constraints we enunciated before. Irrespective, the company has managed to reach out to an increasingly larger number of markets as the initial step before implementing large-scale smart city blueprints[2]. The firm currently provides safe city solutions of more or less complexity for more than 60 cities across 30 countries globally and the firm counts on a rapid expansion of this market niche. An increasing integration of safe city solutions to its smart city portfolio is already in progress including smart e-government, smart grid and smart transportation. Due to the initial implementation of safe city solutions in Chinese cities Huawei has been experimenting smart city initiatives[3] on a very large sample, testing interactions with akin firms integrating issues of public safety, education and health care sectors. However, the group's strategy reckons the necessity of tailor-made solutions for specific regional needs such as Europe's sustainability concerns or Latin America relentless security preoccupations[4].

The integrity of these increasingly complex systems lie ultimately in their social acceptability by city residents outside the controlled environment of Chinese cities: under this Safe City framework, residents become a resource (a commodity even) as data feeders for increasing reliability purposes, and this creates processes of accountability that need be factored into the system. This perception is all the more important considering that Huawei intends to expand Safe City solutions towards increasingly complex Smart City systems. For now, however, the Safe City solutions have been singled out as a preliminary component of the Smart City becoming a convenient gateway towards local and national governments looking to provide narrow-specific tangible answers within a medium-term horizon. Thus adopted, this Smart City component can become a tether to further

[1] While terrorism as such as is never mentioned in official documents, the reference to the term « extremism » is recurrent and might point to other uses of mass control and profiling.

[2] Joe So, head of Huawei's global smart city initiatives, stated "Smart city is important to Huawei's business strategy, but it is still too early to estimate the level of revenue they might generate for the business," in *Industrial IoT 5G Insights*. July 2016.

[3] "There are currently more than 300 smart city initiatives in China alone, many with different requirements. No company can complete a smart city on its own(...)". Statement by Huawei's CEO

[4] "*Countries and cities face different pains. In Europe, green and renewable energy development are key, while in Latin America, safe city initiatives are key priorities (…) governments in both developed and emerging countries are trying to adapt ICT to resolve their pains and become smarter and better societies and economies.*" In https://enterpriseiotinsights.com/20160715/channels/news/huawei-smart-city-tag23

developments in regions and cities of the world while operational hurdles get removed. The company's representatives have acknowledged moreover that that "the scale of planning, research design and execution" still remains a hurdle for any smart city deployment at the city level[1].

2.3 ZTE : an innovating *state-owned privately-managed* ICT corporation

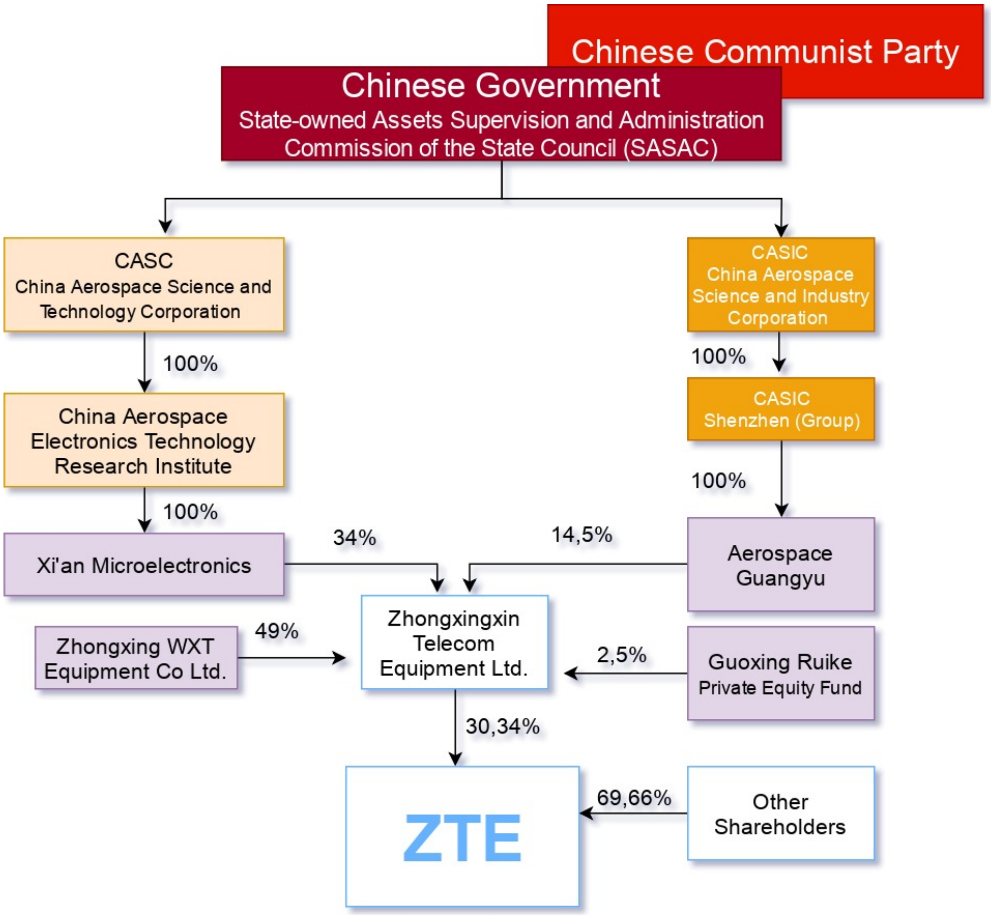
ZTE Corporation or ZTE, is a Chinese multinational telecommunications equipment and systems company headquartered in Shenzhen, Guangdong and one of the top five largest smartphone manufacturers in China in terms of operating revenue. ZTE is a leading integrated telecommunications equipment manufacturer and an important provider of global telecommunications solutions, with shares listed on the main board of the Shenzhen Stock Exchange and the Main Board of the Hong Kong Stock Exchange. Initially founded as Zhongxing Semiconductor Co., Ltd in Shenzhen, Guangdong province, in 1985, was incorporated by a group of investors associated with China's Ministry of Aerospace. In March 1993, Zhongxing Semiconductor changed its name to Zhongxing New Telecommunications Equipment Co., Ltd with capital of RMB 3 million, becoming in time a "state-owned and private-operating" economic entity. The firm evolved into the publicly traded ZTE Corporation in spite of its linkages to the Chinese government, having made an initial public offering (IPO) on the Shenzhen stock exchange in 1997 and another on the Hong Kong stock exchange in December 2004. The corporation is dedicated to the design, development, production, distribution and installation of a broad range of advanced telecommunications systems and equipment, including carriers' networks, handset terminals and telecommunications software systems, services and other products. ZTE has achieved a leading market position for its various telecommunications products in China with longstanding business ties with China's leading telecommunications service providers such as China Mobile, China Telecom and China Unicom. As at 30 June 2016, ZTE Holdings[2] an intermediate holding company, owned 30.57% stake of ZTE and among the rest of the stakeholders two entities were state-owned enterprises[3].

[1] "National and municipal governments are showing interest and the number of smart city opportunities are growing, but we don't expect this will happen overnight because of the scale of planning, research, design and execution before they become reality". Ibid.

[2] In Chinese 深圳市中兴新通讯设备有限公司

[3] The shareholders of ZTE Holdings were Xi'an Microelectronics a subsidiary of China Academy of Aerospace Electronics Technology), Aerospace Guangyu (a subsidiary of CASIC Shenzhen Group) and Zhongxing WXT.

Table 5 - Ownership structure of ZTE 2018


Chinese Communist Party
Chinese Government
State-owned Assets Supervision and Administration Commission of the State Council (SASAC)
CASC
China Aerospace Science and Technology Corporation
100%
China Aerospace Electronics Technology Research Institute
100%
Xi'an Microelectronics
34%
CASIC
China Aerospace Science and Industry Corporation
100%
CASIC
Shenzhen (Group)
100%
Aerospace Guangyu
14,5%
Zhongxing WXT Equipment Co Ltd.
49%
Zhongxingxin Telecom Equipment Ltd.
2,5%
Guoxing Ruike Private Equity Fund
30,34%
ZTE
69,66%
Other Shareholders

Source: ZTE reports, Author's compilation

The company operates today in three sectors: carrier networks (54%), terminals (29%) and telecommunications (17%) and consolidated over the last decade a know-how in wireless, exchange, access, optical transmission, data telecommunications gear and telecommunications software. As in the case of Huawei, ZTE expanded its operations to services such as video on demand and streaming media and sells products under its own name but also as an OEM (Original Equipement Manufacturer[1]). Building on the proceeds of its successful IPOs, the company further expanded its overseas sales to developed nations, and overseas production. Making headway in the international telecom market in 2006, it took 40% of new global orders for CDMA networks[2]. The group's incursion in Western markets began with the Canadian Telus' lead, and in 2007 ZTE sold to UK's Vodafone, Spain's Telefonica, and the Australian Telstra, in addition to garnering the greatest number of CDMA contracts globally. By 2010 ZTE had achieved a global customer base, with sales in 140 countries[3] and a consistent expansion to emerging markets. The corporation had

[1] Which is a company in charge of manufacturing spare parts for another company
[2] CDMA (Code Division Multiple Access) and GSM (Global System for Mobiles) are shorthand for the two major radio systems used in cell phones today.
[3] ZTE Financial Report 2013.

by then become the third-largest vendor of GSM telecom equipment worldwide, and as of 2011 it held around 7% of the key 3GPP Long Term evolution patents.

ZTE's operating revenue aggregated has been progressing steadily as a result of 4G system equipment products appetite in the domestic and international markets. Of around $17 billion, for its last published fiscal year (2017), carriers' networks made US$10,1 billion (40%), consumer accounted for US$ 5,5 billion (15%), and government and corporate brought in US$1,6 billion (29%). The demand for routers and switches in the domestic and international markets, optical communication systems in the domestic market and 4G handsets in China and abroad have been instrumental in the group's rapid progression. In addition, the Group enhanced financial expenses control resulting in the relatively substantial decrease in overall financial expenses[1].

Table 6 ZTE annual revenue progression (2015-2017)

Regions	2015		2016		2017	
	Revenue (US$, in millions)	As % of operating revenue	Revenue (US$, in millions)	As % of operating revenue	Revenue (US$, in millions)	As % of operating revenue
China	8408.16	53.0 %	9269.68	57.9 %	9809.31	56.9 %
Asia (excluding China)	2346.35	14.8 %	2305,87	14.4 %	2499.35	14.5 %
Africa	1104.99	7.0 %	910.53	5.7 %	596.25	3.5 %
Europe, the Americas and Oceania	4002.04	25.2 %	3541.20	22.3 %	4322.76	25.1 %
Total	15861.56	100 %	16027.29	100.0 %	17227.69	100.0 %

Source: ZTE Annual report 2017, 2016, 2015, Author compilation

2.3.1 R&D: aggregating techno-layers, designing eco-systems and integrated solutions

ZTE partakes in the provision of technology and product solutions to the global telecommunications market, targeting service providers to government and corporate customers in more than 160 countries as of 2018. Resolutely belonging to the group of global ICT holdings it has been developing as voice, data, multi-media, wireless broadband and cable broadband communications for users all over the world. Research and development activities have experienced an important growth in recent years, and as of 2014 the company claimed to devote 10% of its annual revenue to this activity, producing patents and utility licenses at a rapid pace. By 2017 this number had reached the US$ 2 billion mark. ZTE has filed 48,000 patents globally, with more than 13,000 granted[2]. The evolution of the group has been instrumental in the rise of China as the most significant innovator in terms of intellectual property registrations and applications. While in 1993, China's applications amounted to 1, by 2017 they overtook Japan's and grew by a further 9.1 per cent to 53,345 in 2018, while the number of US-based filings slipped

[1] As a result of the aforesaid factors, the Group reported net profit attributable to shareholders of the listed company of RMB2.63 billion for 2014, representing a year-on-year growth of 94.0%. Basic earnings per share amounted to RMB0.77.

[2] In two consecutive years (2011 and 2012), ZTE was been granted the largest number of patent applications globally,which is the first for a Chinese company. WIPO Annual report 2017.

0.9 per cent to 56,142[1]. Asia accounted for six of the top eight companies, with China's ZTE Corp and BOE Technology Group spearheading the middle kingdom's innovations.

Currently, the Group has approximately 27,000 R&D employees and 19 R&D centers in China, the United States, Sweden, France and Canada, as well as more than 10 joint innovation centers established in association with leading carriers. Collaboration with academia has been an integral component of ZTE's strategy, as it appears from the "ZTE Forum for Cooperation of Enterprises, Academies and Research Institutes": this entity has been created as a conduit towards domestic colleges and research institutes specializing in telecommunications technologies. Emanating from a Chinese government's priorities regarding technological innovation this forum's ambition is to bring together enterprises, academic and research sectors towards market-oriented initiatives under the leadership of national champions and has so far federated more than 30 institutions.

The Group has also succeeded in gaining access to the international telecommunications market with its ICT-related services. Strategic emerging sectors such as Cloud Computing, Big Data and Smart City, have become an increasingly significant share of its activity, seeking consolidation in the long term. During 2016, the Group reported operating revenue of RMB 46.877 billion from the international market, accounting for 50.2% of the Group's overall operating revenue. Signing comprehensive partnerships with mainstream global carriers, while replicating its original development on the Chinese market, has made carrier's networks activities nearly half ot its operating revenue for carriers' networks, followed next by telecommunications software systems, services and other products (RMB 11.58 billion). In connection with wireless and cloud solutions, ZTE has lunched Cloud Radio, QCell, UBR and maintained relatively strong growth in its home market facilitated by rapid urbanization trends and the deployment of new 4G networks. In anticipation of future developments in wireless communications, ZTE engaged -as did Huawei too- preliminary research on 5G technologies and became the first industry player to introduce the Pre-5G concept and conduct related field tests. The corporation also launched large capacity optical network cross-connection equipment and IDC switches. The research and development of the next-generation high-end packet product platform has provided support for the market development of a variety of products, such as core router, multi-service edge router, packet transport network and service gateways.

Proprietary innovation has been an important component of the company's strategy, following the industry's trends in relation to communications between devices and IoT. In 2014, the Group made focused efforts in the development of the "CGO Laboratory," which was specifically designated as the operating arm for company-level innovative projects established to further enhance the incubation of projects and the development of new businesses and sectors. By then ZTE confirmed its M-ICT strategy[2], with the aim of becoming an enabler in the M-ICT era focused on carriers, government and corporate sectors, striving to add value through information and mobile interconnection for implementation purposes at the city and society level. The ZTE group has been

[1] WIPO https://www.wipo.int/patentscope/en/

[2] ZTE defines the M-ICT strategy as « M denotes as Mobile, Man to Man, Man to Machine, Machine to Machine » stressing the creation of value through information in the process. http://www.zte.com.cn/global/about/magazine/zte-technologies/2015/1/en_700/431209

instrumental, in the same vein as Huawei, in the global adoption trend of ICT technologies towards user-centered applications and technologies that enhance interactions within/between government and corporate networks and services. In connection with Cloud Computing and IT products, ZTE Corp. completed the research and development of cutting-edge Cloud Big Data processing platforms and offered comprehensive, customized solutions for the support of applications in financial, transportation, education, government and public security sectors.

2.3.2 China as a major testing ground for smart and safe city solutions

An increasing attention has been paid to cities in the development of integrated solutions and ICT service provision. Given the enormous market potential they represent at the global level, but most specifically in China, they have become a consistent focus for development of both products and markets. ZTEsoft, the software subsidiary of the group, has been working on the execution of smart cities projects for the last six years related to the implementation of smart metering, smart lighting, and smart parking solutions for municipal and regional governments. With the launching of the Smart City UOC (Urban Operation Center) platforms in Qinhuangdao, Ningbo and Yinchuan, ZTE has operated a learning curve catering to the practical domestic needs regarding Smart Cities development. Developed upon the Group's strengths in Cloud Computing, Internet of Things and Big Data technologies, ZTE smart city solutions aim for a comprehensive approach of cities' problems in the form of "urban management efficiency, facilitating public life and promoting technological innovation". It promotes an alternative model for urban construction, management, and development, resorting to ICTs such as high-speed Internet, big data, Internet of things (IoT), and cloud computing. Over the last three years[1], ZTE's has been able to provide a Smart City model that integrates and shares governmental data through top-level design and overall planning of a whole city. This has been made possible, by the combination of a cloud network-graph architecture, a city operation center based on big data switching and an analysis platform. Based on grand scale experimentations in Yinchuan, Zhuhai, Shenyang, and Shijiazhuang between 2015 and today, ZTE has expanded the reach of the initial model, moving towards data collection from additional sources, expanding governmental and other public service data to city-level data. This has been made by further tapping data value from the Internet of Things (IoT), Internet, and industries to which the corporation was able to gain access over time.

The case of the agreement signed by ZTEsoft with the Yinchuan government in 2014 provides an interesting blueprint to understand these dynamics. Poised to invest $500 million on smart city initiatives ZTEsoft launched its smart city project in September 2015, leading to 13 subsystems having been implemented during the course of three years. Relying on a unified design, scientific architecture, a specific business model, and an operation and maintenance (O&M) platform, it has provided rich application functionality. The subsystems stipulated in the agreement were: smart transportation, smart surveillance, smart community, environmental protection, smart all-in-one card, smart tourism, enterprise cloud, smart government, big data analytics center, one cloud, operation center, GIS & 3D map and elastic network.

[1] At CeBIT 2015, ZTE's EVP, Pang Shengqing, mentioned the concept of Smart City (2.0) to be refined in subsequent years (3.0).

This corporate strategy faces however many challenges in the company's national market, as bureaucratic red tape and coordination issues have erupted between government departments that operate according to specific vested interests. This situation is moreover exacerbated by the weak technological infrastructure present in many Chinese cities, and concerns about the high cost of upgrading their facilities. Thus, many local governments in China would be "internally isolated" and poorly coordinated, leading to a sub-par -and inefficient- supply of public services according to ZTE management[1]. ZTE's partnership with Tencent[2] on a number of smart city projects has been one of the ways through which the group has been looking into overcoming this hurdle: by focusing on systems and infrastructure, Tencent would be in charge of providing terminal services to existing customers. Tencent role has become increasingly relevant through the WeChat app, originally utilized for basic chatting and file sending but having become in recent years a major payments app that has leapfrogged credit and debit cards in China[3]. In this respect, WeChat can potentially grow to become a much broader platform encompassing several other functions pertaining to ZTE Smart and Safe City solutions. The transition towards Smart Cities in local governments in China has opened in this respect the potential integration in time of all smart city functions into a potential 'smart city super app' given WeChat penetration in Asia and beyond in recent years.

The possibilities of replicating this model abroad have been compromised in recent years however, by the increasingly difficult situation of the group in the United States and Europe. The company has been in recent years exposed to controversy by American authorities, following in the steps of Huawei and its recent ban in the American market. Due to the warnings from US intelligence offices[4] and the United Kingdom National Cyber Security Centre[5] over the use of ZTE equipment, the company has ever since been the object of close scrutiny. ZTE had already been banned from buying US components after it had been found to have breached a US trade embargo with Iran. The ban was finally lifted by the US Department of Commerce after ZTE agreed to pay a tranche of a $1.4 billion penalty[6]. In a context of increasing commercial tensions between China and the United States, the company's position has been increasingly exposed to diplomatic crossfire dynamics between these two major trade superpowers, which could deter the group from entering Western markets to the benefit of other regional implantations.

[1] http://www.scmp.com/tech/social-gadgets/article/1838417/chinas-zte-jumping-us16-billion-smart-city-business-after

[2] Tencent Holdings Limited (腾讯控股有限公司 or Téngxùn Kònggǔ Yǒuxiàn Gōngsī) is a Chinese multinational investment holding conglomerate founded in 1998, whose subsidiaries specialise in various Internet-related services and products, entertainment, artificial intelligence and technology both in China and globally. It is based in Nanshan District, Shenzhen and is one of the world's most prominent technology conglomerates and one of the world's largest venture capital firms and investment corporations.

[3] Is Alibaba Losing To Tencent In China's Trillion-Dollar Payment War? Forbes, 28/03/2018

[4] https://www.zdnet.com/article/us-intelligence-chiefs-advise-americans-to-avoid-using-huawei-and-zte-phones/

[5] https://www.zdnet.com/article/uk-telcos-warned-on-use-of-zte-equipment-report/

[6] « U.S. Lifts Ban That Kept ZTE From Doing Business With American Suppliers » New York Times 13/08/2018

3 The global expansion of Safe City models between Chinese global supremacy and local resistances?

Chinese ICT corporations have partaken in the development and promotion of Safe City solutions at the global level, as a result of unprecedented experimentation capabilities and extremely favorable conditions back at their home markets. The support of key ministerial offices and possibilities of experimentation granted by local government authorities has allowed for the transformation of specific Chinese cities into Smart City and Safe City flagship developments, such as Nanjing or Shenzhen[1]. Surveillance *in the city* is currently replicated abroad, and these two companies have expanded their international reach to an ever-increasing number of cities in the Global South and Europe, becoming the main developers for this specific type of solutions. In this section, we will explore how did this expansion take place, building on these extremely favorable conditions, but also on a tactical international deployment that combined accommodating Chinese diplomatic preexisting ties, relevant credit lines stemming from China Development Bank, but also from the companies 'capacity to deploy a multi-level government strategy.

3.1 Huawei's Safe City international deployment conditioned by inwards experimentation and narrow State relations

As seen in previous sections, Huawei's strategy during this period was to win contracts in the Chinese countryside first and to move then to intermediate and major cities (Business Today, 2009; The Economist, 2012). From 1995, onwards, Huawei started entering regional and overseas markets in Southeast Asia, Russia, Africa, Latin America, and Europe. Over the years, Huawei has tuned and adapted its strategy to "developing countries first, developed countries after" (Frost & Sullivan, 2007). This strategy has allowed Huawei to gain sustainable traction in international markets and has contributed to gear up the company from an organizational point of view towards establishing an international presence. This internationalization for all activity sectors allowed Huawei's overseas sales to surpass already by 2014 those of domestic markets. It now has most of Europe's major telecom companies among its customers and Europe, Middle East and Africa operations contributed US $12.4 billion to its revenue, nearly one third of its global revenue[2]. Currently, Huawei relies on a 170,000 strong staff worldwide (De Cremer & Tao, 2015), with 22 regional offices and over 100 subsidiaries around the world.

The company has set its strategy to push for economic and technological advantages in regions -or countries- with an uncertain political environment, which is consistent with the general internationalization approach of ICT Chinese corporations abroad (Mapunda 2014). The case of India is exemplary of Huawei's global expansion and it was replicated both nationally - or even regionally- in the decades to come moving from software development from 1994 onwards to a major global strategic R&D center deployment in less than a decade. Location too has been a strategy to enter regional markets, as Huawei's European headquarters were originally located in

[1] Nanjing played host for the 2013 Asian Youth Games. For the event, Huawei enabled surveillance and protection of key areas, including all 14 stadiums and nearby roads.

[2] « Huawei's Profit Growth Slows » Wall Street Journal 31/03/2017

the UK as to better access telecom EU telecom markets. Another strategy in this internationalization drive was to engage into aggressive pricing to make entries to countries that were looking for affordable technologies, especially developing countries where telecommunications infrastructure was inadequate, and demand was depressed by chronic financial instability. This was not easy initially, as Huawei had to overcome a widespread perception of qualitative inferiority of its products abroad in spite of proven technological capabilities back home[1]. This aggressive Global South strategy led the company to expand its markets from Russia, Thailand, Brazil to South Africa. Because of this rapid expansion, pricing strategies became more aggressive, often undercutting direct competitors' final price for comparable technology by 30 per cent (Mapunda 2014, Ahrens, 2013). While present in the US through seven R&D centers since 2001[2], its implantation in Europe some years later, demanded the development of advanced technology and customization at minimal price premiums, given the competitive setting. This amounted to the emergence of a value-for-money innovation strategy while removing entirely the financial risk to the interested contracting parts. When Huawei made a sale to Neuf, one of the French operators at the time, it was actually building part of the network free of charge and allowing Neuf's engineers to run it for three months to test it before purchase (Harney, 2005) leading to impressive 3G networks sales afterwards. By the end of 2007, Huawei had partnerships with all of the top European operators and was awarded the Global Supplier Award by Vodafone.

The extensive credit backing from the China Development Bank (CDB) has been another important lever in the promotion of Safe City / Smart City solutions: benefiting from 2004 of an impressive US$ 10 billion credit line combined with a contribution from the Export-Import Bank of China, which provided an additional US$ 600 million, Huawei started to undercut prices well below those of its competitors. The company also started to provide vendor-financed loans to their customers (Ahrens, 2013) skyrocketing sales to 85 per cent year-over-year increase for several years onwards mostly achieved out of China (Huawei 2013). By 2010, Huawei made it to the Fortune 500 list with annual sales of US$ 2.18 billion and over 20,000 patents filed (Ura & de Pablos, 2014) and by 2012, Huawei had overtaken Swedish telecommunications giant Ericsson to become the world's largest telecommunications vendor (overall total revenue) in carrier network, enterprise and consumers (The Economist, 2012).

Resorting to this financial backing and adaptation to unorthodox markets, the deployment of Safe City solutions attained soon enough a global dimension, facilitated in the process by important technological partnerships. As a provider of ICT infrastructures, Huawei partnered with Hexagon, the world leader in Safe City software[3] and system integrators such as Safaricom, Tyco and NCS, and software vendors such as Milestone, SAP, IOmniscient, Promad and AgentVi. In spite of these increasingly narrow relations Huawei has been subject to significant controversy due to its

[1] When Huawei entered the Russian market in 1997, it managed to undercut international prices by around 12 per cent and yet still offer impressive after-sales service. http://www.huawei.com/ru/about-huawei/corporate-information

[2] Prasso S. What makes China telecom Huawei so scary? http://fortune.com/2011/07/28/what-makes-china-telecom-huawei-so-scary

[3] http://www.hexagonsafetyinfrastructure.com/overview

relations with the Chinese government: in the United States and Australia, Huawei was thus not allowed to set up network infrastructure due to concerns about national security[1] or even risks of espionage[2]. It is easy to correlate these concerns pertaining with the features of network development in the process of deploying Safe City solutions, which resort to unprecedented levels of data collection and processing. As network development and unrestricted access is an important part of Safe City solutions, it is uncertain at this point how Huawei's will be able to dissipate these concerns. This controversy has moreover escalated to the bulk and speed capabilities of 5G networks, actively promoted by the company, leading in the case of Europe to a rift between countries banning or accepting to engage with these Chinese-developed technologies as of 2019[3]. In an effort to increase transparency, Huawei has been releasing annual reports since 2005. These have been however criticized for various shortcomings, with little attention to year-to-year changes in reporting details, disparities between Chinese and English versions and incomplete financial statements (Zhao, 2010).

3.1.1 Huawei's Safe Cities in Latin America: operating in the world's most dangerous urban environment

Notwithstanding an active promotion of Safe City solutions at a global level over the present decade, this Chinese company has adopted a compartmentalized regional approach proceeding according to a particular sequence, holding of ad hoc meetings with governmental contacts and an intensive media campaign[4]. A "summit" strategy has become thus a choice strategy and has allowed the company to frame the issue of security" in its own terms, redefining it along the lines of social control and information aggregation. While the company's approach to solving security issues is consistent with the technological layer and analytical capabilities of its Safe City platform, this corporate strategy has the potential to reformulate the problem of criminality, traditionally associated in social science and urban studies research with issues of segregation, declining social-economic status, etc. It can moreover contribute to a substitution in time of social/territorial qualitative research on social processes, embodied by legitimate institutions[5], to the favor of Big Data analytics solutions as the sole instrument of security policies.

In the context of Latin America, a region known for high crime levels and important victimization indexes, Huawei has found a terrain suited for aggressive experimentation, combined with controversial private data protection regulations. Huawei's First 'Latin America Safe City Summit' in Mexico City held in November 2014 was organized to discuss trends in the security industry

[1] Marketline Huawei : A world leader marred by controvery, Report, 2013.

[2] A US House intelligence committee report published in October 2012 advised the US government and companies to avoid doing business with Huawei and ZTE, another leading Chinese technology firm, and claimed the companies raised "significant security concerns". In Australia, as of March 2012, the company was blocked from tendering for contracts in the National Broadband Network (NBN), which plans to connect 93 per cent of Australia's homes and workplaces via optical fiber by 2020.

[3] « Angela Merkel resists US pressure to ban Huawei as Germany launches 5G auction » in South China Morning Post 20/03/2019

[4] Thus in 2017, the Safe City Summit will take place in Dubai, with the participation of representatives from previously implemented Safe City solutions from Cochabamba and Marrakech. In http://e.huawei.com/topic/safe-city-2017-en/About-Summit.html

[5] As certain hemispheric organizations such as the Organization of American States. See OAS, *La Seguridad Pública en las Américas ·Retos y Oportunidades*, Washington, 2008.

and explored different ICT approaches used to support smarter and safer cities. The event gathered security experts from the Global Security Industry Alliance (GSIA) among others[1] as well as Huawei's customers in Latin America. At the summit, Huawei showcased its Safe City Solution and promoted sub-solutions such as network access, video linkage, convergent command, intelligent analysis, and video cloud supported by its Long-Term Evolution (eLTE) broadband trunking. The purpose of this initiative was to address the needs of the security industry in the Latin American context, building on the possibilities of well-succeeded Smart City implementation in cities in Mexico, Bolivia, Trinidad and Tobago and Venezuela. The company has moreover consistently emphasized, in this regional context, the imperative of safety for increased labor efficiency and productivity, presenting future new technologies like High-Efficiency Video Coding (HEVC) or H.265 standards. This would have the advantage of providing a high video quality with a low bit rate in a continent with highly dissimilar broadband infrastructure quality.

Two examples of the company's Latin American strategy are worth mentioning here, the case of Cochabamba in Bolivia, and the one of Santiago in Chile. By looking into the sequencing of this deployment and the specific features under consideration for each one of these cities, we will underline the main issues at hand in the consolidation of these *solutions*.

Cochabamba Segura, Bolivia: The largest Safe City project worldwide

On November 2016 was signed the formal agreement for the installation of a Safe City project and the Strategic Cooperation Agreement for Safe City with the authorities of the city of Cochabamba in Bolivia. It represented Huawei's first project for trunk broadband eLTE and the first Hexagon CAD project for Bolivia, and the largest project of Safe City ever concluded by the company at that time. The Safe City project will cost almost 12 million Euros over its different implementation phases. It includes an eLTE base, portable equipment, vehicle terminals, Internet content providers, Hexagon computer-aided design software, networks, information technology and video surveillance systems.

The mayoral authorities agreed on that occasion to implement the first phase of a comprehensive citizen security plan "Cochabamba, smart city, safe city" consisting of the installation of 420 security cameras and the implementation of telecommunications towers and handies with GPS for the Police. One part of the project is the acquisition of equipment and software for a municipal digital network with an investment of €8,3 million. The local authorities favored a long-term collaboration with Huawei in order to turn Cochabamba a showcase for safest cities in Latin America by the deployment in time of Smart City technologies.

The initial stages decided for the deployment of a Safe City platform by the mayoral office have prioritized the placement of cameras in educational units in order to fight against « human trafficking, insecurity, violence and drug trafficking » through CCTV network capable to make face and plate recognition. A second stage will set the towers, fiber optic links and integration of the digital network that will demand a budget of €4,5 millions. Complaints will then be expected to reach the Automatic Dispatch Center (CAD) which will be linked with ambulances, firefighters,

[1] SAP, Intergraph, Telmex, and Netherlands VCS.

municipal units and the police forces. By setting up a 911 number which will be recorded 24 hours a day, seven days a week, calls will be immediately located by GPS. Then the closest and most suited intervention force will make an immediate response to the designated location. Cochabamba Segura project is thought to be encompassing, going beyond a simple upgrading of CCTV networks and allocates significant resources to prevention mechanisms as well as analytics that should assist the clarification of criminal acts. In time, both Huawei representatives and local government authorities expect these networks and technologies to be extended towards health and education areas for the upgrading of Cochabamba to a Smart City[1].

While the implementation of this agreement remains a flagship initiative in the South American continent, for one of the most dangerous cities in the world, the articulation of this platform's possibilities with longstanding structural constraints of the city still remains a daunting challenge. Opposition political leaders have thus denounced the lack of follow through regarding the city Mayor's electoral promises to provide patrol vehicles to each district of the city. Other issues, pertaining to the effective patrolling and use of police facilities (like street boots) have been regularly addressed in the media and could compromise the system's responsiveness. A last issue remains regarding the effective training of personnel, whose particulars have not been disclosed to this day.

Selling the Safe City: A top to bottom State organizations approach for Chilean Cities

Huawei's aspirations to become the first Safe City and Smart City provider in Chile have been comforted by its international weight -global sales of US$ 60.8 billion in 2015- as well by the fact that this multinational corporation is the largest Chinese company present in this country. Very present in the smartphones business in Chile, the company has been pushing through in recent years ICT products and solutions such as cloud-based services and infrastructure; intelligent infrastructure for the electrical industry and rapidly deployable broadband eLTE mobile networks. Building on this array of products and solutions already present in the Chilean market, Huawei started its participation in 2016 at the seminar "Digital Transformation" organized by the PDI (Policia de Investigaciones)[2], the Chinese multinational showed that Criminal Analysis is the basis of an intelligent criminal prosecution. It stressed however that it needs, as does a Safe City platform, a mandatory corresponding investment in infrastructure that supports high-speed Internet, IoT devices, high-definition sensors and technology that guarantees a secure and stable connectivity. Investing in digital infrastructure and ICTs would, according to the company's representatives, not only reduce crime, but would also allow for a more effective handling of accidents, natural disasters, cyber-attacks and terrorism.

The Investigative Police (PDI) and Huawei initiated together a cooperation for the development of a digital agenda on matters of cybersecurity that is inclusive of organized crime and its territorial

[1] Thus Cochabamba's mayor stressed that The Safe City project is only the beginning of the Smart City we want to reach."

[2] The goal of the "Digital Transformation", organized by the PDI (Chilean Investigative Police), was to learn about the most innovative and effective technologies, solutions and trends for research and development. the fight against crime.

expression in Chilean cities. By the establishment of this partnership[1], the Chinese company has agreed to the transfer of technology in the areas that would enhance the institutional mission of police forces, as well as the improvement of its human capital and access to state-of-the-art technologies, in addition to the support of digital issues related to cybersecurity and organized crime as well as immigration related issues. The successful example of Shenzhen and its declining criminality rates over the last 10 years, mobilized by Huawei for the promotion of its Safe City model, has been particularly appealing to Chilean authorities. As for Shenzhen, Santiago's population numbers and the territorial scale remain somehow comparable[2]. Huawei's collaboration is considered a fundamental pillar of the PDI's Strategic Plan, where there is a strong emphasis on technological innovation as a key solution to criminality[3]. This orientation by Chilean police forces has been supported in recent years by the establishment of the National Center for Criminal Investigation Analysis (Cenacrim), which comprises an area of research and technological innovation. The center's main goal is to provide improvements in operational and investigative management. adjusted to the real state of police forces and to participate in time to the development of criminality analytics. Huawei has stressed ever since, that the Safe City ecosystem, combining surveillance, Big Data analytics and related infrastructure, main purpose is to facilitate the collaboration of the institutions as well as responses against crime[4].

Huawei's approach to Chilean cities has been one of a sequence combining expertise dissemination in specific fora, reaching out to governmental authorities when needed and ultimately the conclusion of a memorandum of understanding with national investigation police forces. While no agreement has been so far concluded with the metropolitan authorities of Santiago (Intendencia) or specific districts (comunas), the partnership with the PDI is a powerful lever of credibility and legitimacy in the way of securing specific contracts with local authorities. District mayors have increasingly been facing coordination issues between national police and municipal security forces, as a result of different communication channels, data aggregation and contact platforms. While metropolitan authorities are a low-key player when it comes to decisions pertaining to security in Chile's capital city, the possibilities opened by Huawei's already established presence in the Chilean market and key partnerships with security institutions might allow the company to decisively move forward to a closer partnership with these units.

[1] The Director General of the PDI, Héctor Espinosa Valenzuela, and the CEO of Huawei Chile SA, Qin Hua, signed on Thursday, April 20, a memorandum of technology transfer and consultancy in information technology and communications. See http://www.cooperativa.cl/noticias/pais/organismos-del-estado/pdi/pdi-contara-con-apoyo-de-huawei-para-labores-policiales/2017-04-21/190919.html "Between 2006 and 2015 kidnappings were down 86%; the robberies to people 82%; and car thefts 79%. And all this, without increasing the number of police officers, but after investing in infrastructure and Information and Communication Technologies, " according to Huawei Corporate headquarters statements.

[2] "Between 2006 and 2015 kidnappings were down 86%; the robberies to people 82%; and car thefts 79%. And all this, without increasing the number of police officers, but after investing in infrastructure and Information and Communication Technologies, " according to Huawei Corporate headquarters statements.

[3] Therefore "our criminal experience tells us that technology is fought with technology, and therefore, establish alliances with world-class leaders in the field, allow us to build bridges of rapprochement and cooperation to access refinement of our staff or state-of-the-art technologies. " Ibid.

[4] According to Marcelo Pino, Corporate Affairs Manager of Huawei Chile.

3.1.2 ZTE Smart and U-Safety technology: from pioneering Smart technologies to the development of security-specific solutions

The development of safe city solutions at ZTE has been related in recent years to the general framework of development of smart city solutions, where the latter has become an increasingly relevant component. This has been determined by several factors such as ownership, technological possibilities, and investments strategies and last not least, the capacity to produce innovative solutions specific demands at the city territorial scale. Building on two decades of consolidation and diversification of its corporate activities, ZTEs has increasingly developed its own stream of safe city solutions, in phase with the general stated goals of security, increasingly popular in cities and increasingly tapped by ICT companies. The consolidation of the company's smart city solutions operations spread over 60 cities across 45 countries was facilitated, as for Huawei by the expertise acquired in China: this pathway has played, as seen in the previous section, an important role as catalyzer of the urban possibilities of Chinese telcos.

Building on the complexity of diversified social and environmental problems where information gaps between public safety agencies appear as an increasingly critical problem, ZTE's array of technologies look into the facilitation of these processes within a set integrated environment. Emergency management processes focus more on conducting responsive actions after events rather than taking preventive measures before, in part given the complexity of aggregating across-the-board data with persistent hurdles. A more fundamental reason lies in the technical shortcomings of these cities, where existing bandwidth of current emergency communications systems that does not facilitate face recognition or remains sub-par when assessing specific recognition patterns. While ZTE acknowledges that Safe City solutions will not substitute themselves to public safety systems and their limited operation functions at the city level, they can provide an instrument for integration in the years to come.

U-Safety technology is today present in more than 40 countries, including China, Ghana, Mauritius, Sierra Leone and Senegal. The ZTE U-Safety public safety solution was among the first to be conceived by the ICT industry and was until recently considered to be the most comprehensive integrated public safety solution available in the market[1] Thus the *U-Safety Safe City Solution* model, developed as the corporation's incursion in the realm of surveillance in urban settings combines a whole set of emergency assessment and legal enforcement mechanisms to deal with disasters, social accidents, crimes and other public safety events. Intended to protect life and property during emergency events and enforcing the law to keep social peace, this system is integrated into all the phases of emergency management and institutional responses including emergency forecast, emergency handling, disaster warning, environment monitoring, and crime case detection. As for other integrated surveillance mechanisms this system's purpose is to provide a centralized control of these processes by tapping into administrative and governance processes such as coordination of city services and effective operation within all public safety agencies.

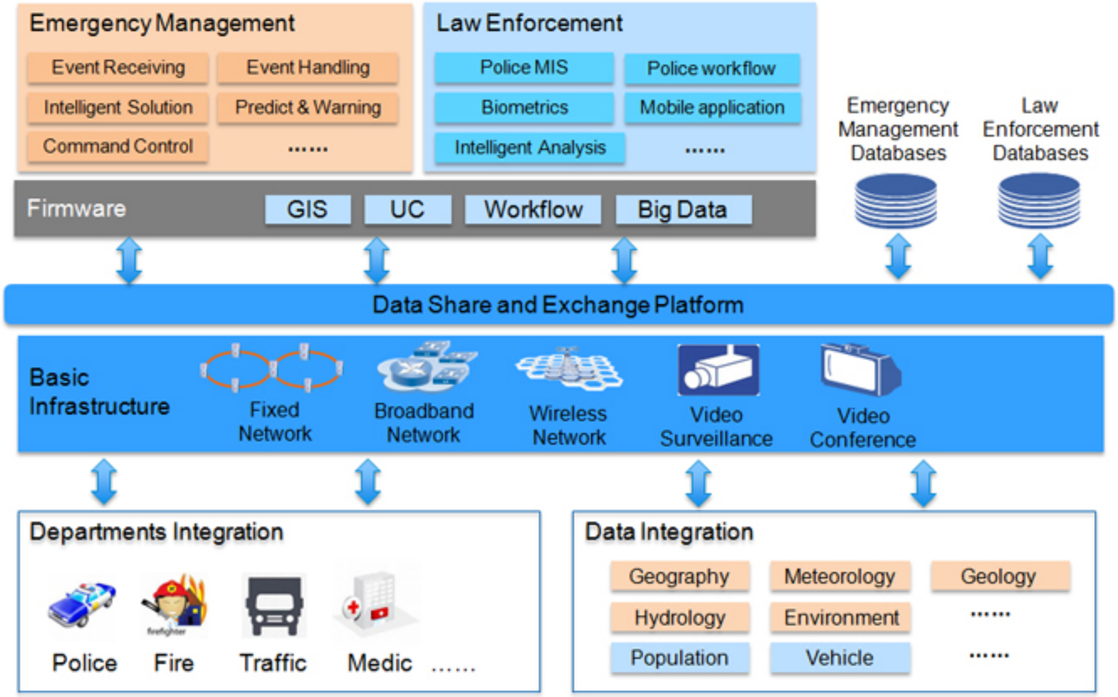
[1] According to the consulting report Integrated Public Safety issued by the analyst firm Frost & Sullivan in October 2012.

ZTE’s U-Safety solutions provides accordingly end-to-end security services for local governments, including trunking calls, video monitoring, video conferencing and other integrated services. The solutions also deliver high-speed data transmission, positioning, command and control, emergency response and intelligent data analysis. The core system is a combination of ZTE’s Coalition Emergency Response System (CERS) and Global open Trunking architecture (GoTa). CERS is an integrated platform of multiple applications and peripheral systems that provides alarm accepting and handling, computer-aided dispatching, information convergence and service and communication application integration. It also can function as a carrier for interaction between subscribers. In addition, CERS integrates a Global Positioning System (GPS) location component, a Geographic Information System (GIS) map, a call center and ZTE’s information management system, Intelligent Transportation.

The architecture of the U-Safety Safe City Solution is composed of 4 layers and 2 applications. The sensors and terminals layer are composed of video monitoring cameras, video conference devices, phones, digital trunking terminals, and different kinds of sensors. This layer provides the foundation for the IoT to assist information and data collection for public safety services. The communication layer is composed of the wireline network, the wireless network and other professional networks such as the digital trunking while the system platform layer is composed of several supporting platforms for public safety applications. The system is connected to different public safety departments and databases through data sharing and an exchanging platform integrated into the emergency database and the law enforcement database. In the applications and services layer, the emergency management includes event receiving and handling, comprehensive event management, forecasting and warning, computer-aided command and control etc. The unified law enforcement platform, as designed by ZTE, has the potential to provide multiple applications such as police information management, workflow automation, mobile law enforcement and biometric identification for the creation of an intelligent system for law enforcement departments.

Finally, the big data platform provides the capability of big data processing & analysis based on the integrated emergency and law enforcement databases. The *intelligent* analysis provides important functionalities such as video analysis and social relationship analysis to assist local police forces in criminal tracking. The law enforcement includes police MIS (Management Information System), workflow, mobile applications, intelligent analysis, etc. The handling of information is thought as to allow for a unified data exchange platform that integrates service data to improve the coordination capabilities of these departments. The public safety monitoring platform uses data mining and mathematical modeling technologies to analyze data coming from multiple sources. This ensures emergency services can automatically react to specific conditions and avert crises.

Table 7: ZTE U-Safety Public Safety Solution hierarchy



The quest for flagship projects in Western Europe and South America….

ZTE U-Safety technologies have experienced a rapid growth and geographical spread as a result of successful partnerships for Smart City developments across the globe. The company has been involved in smart city-type projects in Laos, Sri Lanka, France, Romania, Turkey, Nigeria, Ethiopia, Sudan, Chile, Venezuela and Uruguay, among other countries. ZTE smart city solutions are based on a city operation center and among other things, 14 categories of industrial solutions that include: emergency management, safe city, digital city management, smart government administration, smart tourism, smart campus, smart environmental protection, smart logistics, enterprise connectivity, smart education, smart healthcare, smart transportation, smart community, and citizen card. The subsidiary in charge of the development of cloud solutions, ZTEsoft, has been working on the execution of smart cities projects for the last six years. The company previously stated that most of the work is related to the implementation of smart metering, smart lighting, and smart parking solutions for municipal and regional governments. While not all of these pertain to the Safe City, they are potential components for the development of related platforms that will deal specifically with the issue of security. Regional deployments of U-Safety technologies remain however limited by the presence of the company, the regulatory framework and the array of liberties available for city residents[1].

The strategy pursued by the ZTE group has been thus one of selective engagement in the promotion of Safe City platforms around the world. The decision to pursue these solutions in regions such as Europe or the South Cone of the Americas, where transparency rules and clearly

[1] ZTE looks for increasing business opportunities in smart city projects in certain Asian markets such as India, where the local government is seeking to develop a nationwide smart city program.

established sets of competences coexist with democratic local governments, has limited the appeal of a one size fit them all approach. In this sense ZTE has had to engage in ways that had to take into consideration the legal and political limits to a mass deployment of technological systems -in contrast with earlier Chinese cities' experiences. The adaptation to national private data and privacy regulations has been here a deterrent to the expansion of predetermined operations to these "mature" sub-regional markets albeit it contributed to a learning and respectability curve by the firm.

Looking into the different partnerships and configurations available for Smart City and the extension of U-Safety technology systems by ZTE accounts for the very open playing field available for these platforms today. Whereas with major cities or towns, ZTE has been versatile enough in the promotion of these technologies all over the world. The example of Rüsselsheim am Main, Kelsterbach and Raunheim municipalities in Hessen, Germany, showcase the possible comprehensive cooperation available possibilities for smart city development[1]. Here the provision of smart infrastructure for businesses and authorities becoming a European model region for smart city[2] has allowed for 15 projects to be implemented at a separate municipality or at a cross-municipal level, among which the one of Smart Safety. This is but one example, that showcases the flexibility of the company when looking for partnerships worldwide and the possibilities available given the current necessities of cities to articulate responses for security needs. We will explore this dynamic in the case of Marseille in France, and in Montevideo, Uruguay.

The Example of Marseille: local government and the "big data of public tranquility[3] »

Marseille has been struggling with security issues for several decades in part due to the difficult coordination of the territory of the city at the metropolitan area, combining a major port hub, a complex topography of the city and the long-standing presence of organized crime. All these factors combined have contributed to high victimization levels and raised the authorities' concerns, favoring a quiet revolution since 2007 away from the infamous title of one of the most dangerous cities of Western Europe. These changes were brought by a reorganization of police forces and a visible increase in the ranks of detectives in charge of department security and judiciary police[4]. Since March 2007, the City of Marseille and its Deputy Delegate for Security and Prevention of Delinquency, have been engaged in a process of securing urban public spaces, particularly through an increasingly important video surveillance network. These initiatives continued throughout the last 10 years culminating with the 2016 project "Big Data of Public Tranquility"[5].

[1] ZTE und „Drei Gewinnt": Smart-City-Technologien werden zum Standortfaktor. In http://www.zte-deutschland.de/presse/press_releases/201703/t20170321_15497.html

[2] With the completion of the planning phase, the construction of concrete smart city solutions will now begin, ZTE said.

[3] Marseille se rêve en "safe city" La Provence, 03/08/2016

[4]According to Caroline Pozmentier the Maire of Marseille adjunct delegate to Public Security and Crime prevention: *« It is assumed that without security, there is no economic development and tourism possible (...) and I believe that this security, nowadays and with the current risks, cannot be provided without a total decompartmentalization . Today, we have an incredible amount of digital data, and the goal is to funnel it towards a single system that will help elected officials making decisions about, for example, road improvements, of public space, mobility etc. " ».* Marseille se rêve en "safe city" La Provence, 03/08/2016

[5] This project has benefited from € 600,000 from the European Union's European Economic and Regional Development Fund (ERDF) funding from the partnership between the City of Marseille and the Department of Bouches-du-Rhône.

ZTE was granted a public contract by the Marseille Municipal Government to develop a National Public Security System of the city, under the name “Marseille City Surveillance”. The contracting period began in 2011 and was to be implemented over a period of 18 months. The most salient innovation brought by ZTE is to be found in a platform combining the creation of a control operation center (*Centre de Supervision Urbain* or CSU in French[1]) backed by the installation of nearly a thousand CCTV cameras by the end 2016, to be expanded to 2000 by 2020 throughout the different city districts[2]. Such a transformation has been made possible by the adoption of intelligent image recognition software in 2017, intended to facilitate data processing routines of the existing CCTV network and expedite sound and visual pattern recognition[3]. ZTE had to overcome at first existing compatibility issues with Marseille’s Western surveillance platform type and had further to deploy unprecedented large capacity hardware on network and storage[4]. This was the result of 1080p video quality rendering demands by the authorities, with two distributed storage centers, a central storage and monitoring center and a multicast to local police authorities for purposes of coordination.

This contract proved to be an important stepping stone for ZTE as a surveillance products and government security solutions in Europe. While the impact of this new integrated system still has to prove its effectiveness against organized crime, authorities reckon that traditional delinquency and offenses have experienced a significant decrease from 20% to 30%). The local authorities (mayor and local assembly) decided, in the face of this indicators, to step up their commitment to this solution and have made public their ambitions to make Marseille the first “safe city” of France and Europe. The intended transformation of the surveillance system from an experimental to an encompassing one, has forced however the authorities to reconsider the overall implementation of the existing process. Acknowledging that the network’s future depth and width will sensibly expand the reach of surveillance of local authorities and police forces, the city authorities of Marseille have stated their willingness to proceeding towards wider consultation.

The present challenges to such a system in Marseille stem however from the quality of the interactions between local government and neighborhood committees and social housing offices, to make a surveillance system deployed at the full scale of the city acceptable. More specifically, the issue of CCTV presence at the very heart of sensible areas, that might ignite a social backlash or at a more operational level, has the potential to damage the installed surveillance feeders. The other subset of concerns, that are by no means less relevant, pertain to the uses of new fringe surveillance technologies, whose data collection capabilities are still poorly assessed internationally, such as drones. In the wake of these technological dissemination, the collection

[1] http://www.marseille.fr/epresse/documents/thesaurus/documents/29957/2507-fpcsu.pdf

[2] The project budget is € 9 million, of which € 3.7 million is financed by the State and 400,000 euros by the General Council of Bouches-du-Rhône.

[3] Caroline Pozmentier, Deputy Mayor in charge of Security and Crime Prevention. "On average, 24 hours a day, there are around 20 agents in front of the screens of the urban supervision center, which is an immense help, two examples among others: we can program software so that 'they spot any unusual behavior, any gathering at a late hour, but also they will be able to capture and alert about suspicious sounds: too loud music, screams, sounds of gunfire ... ". Ibid

[4] In the first phase of the project, each distributed storage center has a capacity of 150TB and the central storage and monitoring center is 300TB.

and cross-analysis of this data for the purposes of security enforcement by Municipal Police forces appears to be an unavoidable pathway towards a “safe city” operational platform; it is unclear however how the city can actually prevent the collection of citizen’s personal data as of today. The statements by Marseille’s local authorities make no secret of such intent, pointing to the mandatory across-the-board streamlining of data collection from sources as diverse as police, justice, fire-fighter services, transportation and weather. An initial step has been made in this sense by the agreement of prefectural authorities with the Prime Minister office and the Ministry of the Interior for the purposes of sharing data statistics, pertaining to the nature and location of all crime-related events in Marseille. Last not least, data streamlining raises further issues pertaining to institutional hierarchies and possible divestiture of regal powers by central State institutions towards local governments.

Local governments have become the most important partner for ZTE as they are the gatekeepers for contracting opportunities and are perceived of secondary interest when it comes to the possible threat raised by Chinese corporations on surveillance system development in Europe [1]. By actively participating to mayoral fairs (such as the Salon des Maires) or sector-related fora (such as the Federation des Industriels des Réseaux d’Initiative Publique or FIRIP), ZTE has maintained a low profile, insisting on a corporatist identity -a firm belonging to a specific sector of urban infrastructure innovations- and by that token, has managed to successfully integrate the ecosystem of ICT providers in France. While the company seeks to promote intra-FIRIP collaborations for sure, it has also pointed to this organization as a conduit for the promotion of its local communities (collectivités locales) related solutions, previously developed in Chinese cities. Pertaining to Safe City solutions in particular, the successful bid for Marseille’s surveillance platform has led to the reinforcement of the company’s local level solution development and ZTE is currently bidding for a similar platform development in the case of Lyon. The company has referred to this series of contracts as an avenue for the expansion of its operations in Europe, as safe city solutions can pave the way to other biddings in the large array ZTE smart related solutions for the local level[2].

The example of Montevideo and a Public Safety System[3]

The Uruguayan government started looking 10 years ago to incorporating new technologies for the treatment of public safety. The Ministry of the Interior acquired a new technology system in telecommunications applied to public safety where ZTE provided the information and communications infrastructure which was an integrated system composed of emergency communications and command, data transmission, VoIP and video surveillance. The deployment of this infrastructure enabled Uruguay’s government to have fast response and a one-size fit all command capability to deal with different kinds of emergencies, into what was already a favorable

[1] Statement by Antoine Jia, Director of ZTE France in 2017.

[2] As stated by the Commercial Director of ZTE "CCTV is often a point of entry for local authorities, but the development of high-speed broadband will encourage municipalities to invest in new services," says Antoine Jia, ZTE's commercial director for France. Stockage – Les datacenters jouent la proximité Alliancy, 26/11/2013

[3] Ministerio del Interior incorpora alta tecnología al servicio de la seguridad pública El Observador, 9/01/2008

setting, with previously successful digitalization strategies carried out by the government[1]. In January 2008, a contract was signed with the Chinese company ZTE Corporation and the importation of hardware aimed at improving network infrastructure and the general technology available for the police. Simultaneously, it included a metropolitan video surveillance system with 103 cameras located in public organizations, places of high popular concentration and public entertainment centers; cameras in 12 detention centers of the National Prisons Directorate in Canelones and Las Rosas (Maldonado), finally, a system of facial recognition in the different migratory points of the country.

This agreement was concluded after a long negotiation and it led to an investment of around 12 million dollars. The innovations provided by this system looked into an enhanced 911 emergency service with a greater response capacity both in quantitative and qualitative terms. The agreement states that ZTE Corporation is in charge of instructing the employees of the Ministry of the Interior to use these new technologies. This system will contribute in time with the resources available to police officers that will be able to monitor on screen, mobile phones and the place where an incident are taking place. Among the many intended windfalls of the new technology to be implemented, the Ministry of the Interior pinpointed the security offered by the system to the street level following a grid pattern, across the most important places of the city of Montevideo. The main areas to be covered are the Centennial Stadium, the parks, the Montevideo Center and then some other areas will be incorporated, according to the Minister. For his part, the new People's Republic of China Ambassador, Li Zhongliang, present at the signing of the agreement, underlined how this agreement is the expression of current unprecedented levels of bilateral cooperation between both countries. The diplomat put on record the fact that ZTE Corporation, is the largest and most modern ICT company in China and a network solutions provider seeking to expand its service base in the Americas.

While the authorities recognize the potential of such systems, in particular regarding a less physical interaction with the police forces, some agencies such the Junta Nacional de Drogas issued a cautionary note pointing to the limits of these systems and a set of clearly defined objectives. These new platforms have been understood as supporting existing security policies and not necessarily replacing them[2]. The objective of these systems is perceived by the police forces as a powerful tool for graphic support for their interventions as the system can record and provide graphic support in the event that an event occurs where the camera is located.

This 12-million-dollar project participates of a larger framework of agreements sealed with Chinese ICT firms and Uruguay during the State visit to China by president Tabaré Vazquez and the president of the Uruguayan Chamber ICTs Alvaro Lamé. This visit set the blueprint for future agreements with ZTE on the issues of digital city development in areas such as safety and

[1] The Plan Ceibal is a Uruguayan initiative to implement the "One laptop per child" model to introduce Information and Communication Technologies (ICT) in primary public education and is beginning with the expansion into secondary schools.

[2] Thus Milton Romani head of the Narcotics National Board stressed: « this is something magnificent, but be careful because it is a tool that has to be at the service of certain objectives that should be be defined and according to the strategic guidelines drawn up by this administration » El Observador, 01/07/2013.

education, among others. Uruguay authorities have insisted on the know-how in certain areas such as software development and future cooperation formats that could include local sourcing for software development of associated applications. As for the discussions held with ZTE Corporation on this occasion, the authorities reached an agreement for the of drone-based alarm-communications system already in extensive use in several Chinese cities in partnership with the Quanzhou branch of China Telecom. The appeal of these systems for Uruguayan authorities lies in the quality of emergency communications that can be easily deployed and has a competitive cost for a reliable communications system based on macro cell 4G for the telecommunications backhaul[1].

Conclusion

The dissemination pace of a new brand of surveillance systems is challenging traditional views of security in cities, combining technological possibilities, with ICT companies' blueprints for encompassing safe systems today. The announced transformation of surveillance has not, in appearance at least, the potential to completely overhaul the institutional framework devoted to crime and hazard prevention, inasmuch as the government levels concerned, police forces and security agencies' role retain their quality of vital components of these new platforms. Big data analytics and data aggregation capabilities exert however significant changes to the comprehensiveness of these systems, that proceed to increasingly combine security dimensions that were disconnected to one another, like health, natural disasters and crime. By providing a set of standardized responses, real-time analysis and preventive alerts, security and safety as distinct notions are increasingly morphing into an operational one. This creates the risk of potentially escalating information loops, but also of altering the complexity of security perceptions into standardized interpretations, which presents no doubt, a fundamental challenge to security policies in Cities, and challenge existing policy networks of response to related issues in the medium and long term.

While there is an unavoidable learning curve to the integration of these systems to complex urban settings, and the outcomes are far from clear at this point, fundamental questions emerge: who is in charge of developing and promoting these systems? Which specific role do ICT companies play when they reap major contracts with local governments? If corporate actors are key drivers of a new reality by aggregation of individual city contracts at a global scale, it is safe to assume they can alter the variables and even understanding of existing safety and security frameworks within cities. The understanding of these platforms capabilities remains however blurry, namely in the Global South, where Big Data capabilities and analytics remains to this day scarce. In this asymmetrical relationship, the very organization, goals and strategy of the corporation become key analytical variables to study in the way of understanding the possible transformation of city surveillance into a global one.

[1] Backhaul refers to the physical part of a communications network between the central backbone and the individual local networks

References

Ahrens, N. (2013). China's competitiveness: Myth, Reality and Lessons for the United States and Japan, A report of the CSIS Hills Program in Governance.

Amoore L and de Goede M, 2005, Governance, risk and dataveillance in the war on terror. Crime, Law and Social Change 43: 149–173

Andrejevic, M. 2002. The work of watching one another: Lateral surveillance, risk, and governance. Surveillance & Society, 2(4): 479–497.

Andrejevic, M. 2012. Exploitation in the data- mine. In: Internet and Surveillance: The Challenges of Web 2.0 and Social Media, edited by C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval, 71–88. New York: Routledge.

Andrejevic, M. 2014. Surveillance in the big data era. In: Emerging Pervasive Information and Communication Technologies (PICT), 55–69. Dordrecht: Springer.

Andrejevic, M. and Gates, K. 2014. Big data surveillance: Introduction. Surveillance & Society, 12(2): 185–196.

d'Arcimoles M. Borraz O. "Les boues d'épuration municipales et leur utilisation en agriculture".Sociologie du travail 45 (2003) 45-62

Artigas, A. "Infrastructure et nouveaux émergents" in Chevauché, Halpern et Lorrain, Villes Sobres, Presses FNSP, Paris 2017.

Ball, K., Haggerty, K. and Lyon, D. (Eds.). 2012. Routledge Handbook of Surveillance Studies. London: Routledge.

Barbieri, E., Huang, M., Tommaso, M. R. D., & Lan, H. (2013). Made-in-China: High-tech national champions of business excellence. *Measuring Business Excellence, 17*(2), 48-60.

Bauman, Z. and Bordoni C. 2014, State of Crisis. Cambridge Polity Press.

Bellanova, R. & Duez, D. 2012 'A Different View on the 'Making'of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage'. European Foreign Affairs Review 17, Special Issue : 109–124

Bigo D. 2006,« Le visa Schengen et le recours à la biométrie », in Du papier à la biométrie. Identifier les individus, X. CRETTIEZ, P. PIAZZA (dir.), Paris, Presses de Sciences Po, pp.237-267.

Boersma, K. Fonio C. 2018, Big Data, Surveillance and Crisis Management, Oxon, Routledge

Boersma K. and Fonio Culotta, C. A. 2010, July. Towards detecting influenza epidemics by analyzing Twitter messages. Proceedings of the First Workshop on Social Media Analytics, New York, 115–122.Ejaz, W. "Internet of Things for Smart Cities: Technologies, Big Data and Security" Springer London 2019.

Boersma, F.K., 2013. Liminal surveillance: Intensified use of an existing CCTV system during a local event. Surveillance & Society, 11(1/2): 106–120.

Boersma, F.K., van Brakel, R., Fonio, C. and Wagenaar, F.P. (Eds.). 2014. Histories of State Surveillance in Europe and Beyond. London: Routledge.

Boersma, F.K., Diks, D., Ferguson, J. and Wolbers, J.J. 2016. From reactive to proactive use of social media in emergency response: A critical discussion of the Twitcident

Boersma, F.K., Wagenaar, P. and Wolbers, J. 2012. Negotiating the "Trading Zone": Creating a shared information infrastructure in the Dutch public safety sector. Journal of Homeland Security and Emergency Management, 9(2): 6.

Boucher, P. Nascimento, S. and Tallacchini, M. 2018. Emerging ICT for Citizens' Veillance: Theoretical and Practical Insights. Science and Engineering Ethics. 24. 10.

Boyd, D. and Crawford, K. 2012. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society, 15(5): 662–679.

Burns, R. 2014. Moments of closure in the knowledge politics of digital humanitarianism. Geoforum, 53: 51–62.

Burns, R. 2015. Rethinking big data in digital humanitarianism: Practices, epistemologies, and social relations. GeoJournal, 80(4): 477–490.

Büscher, M., Perng, S.-Y. and Liegl, M. 2015. Privacy, security, liberty: ICT in crises. International Journal of Information Systems for Crisis Response and Management, 6(4): 72–92.

Business Today. (2009 June). Huawei Technologies a Chinese Trail Blazer in Africa. *Business Today*. Retrieved from http://www.businesstoday.lk/article.php?article=931

Cardon, D. 2015 À quoi rêvent les algorithmes. Nos vies à l'heure des big data, Paris, Seuil

Cassa, C.A., Chunara, R., Mandl, K. and Brownstein, J.S. 2013. Twitter as a sentinel in emergency situations: Lessons from the Boston marathon explosions. PLoS Currents, 5.

Castells, M. 2001. The Rise of the Network Society: The Information Age: Economy, Society, and Culture, Vol. 1. Oxford: Blackwell.

Castillo, C. 2016. Big Crisis Data. Cambridge: Cambridge University Press.

Chan Kim W. and Mauborgne R.A. Blue Ocean Strategy, Expanded Edition: How to Create Uncontested Market Space and Make the Competition Irrelevant, Harvard Business School Press 2005

Chen, M., Mao, S. and Liu, Y. 2014. Big data: A survey. Mobile Networks and Applications, 19(2): 171–209.

Clover, C. (2015). China’s Huawei reports best revenue growth in 5 years, Financial Times, July 20, 2015, Retrieved from http://www.ft.com/intl/cms/s/0/52ae5b0c-2e8c-11e5-91ac-a5e17d9b4cff.html#axzz3rg2JXplj

Comfort, L.K., Boin, A. and Demchak, C.C. (Eds.). 2010. Designing Resilience: Preparing for Extreme Events. Pittsburgh: University of Pittsburgh Press.

Comfort, L.K., Ko, K. and Zagorecki, A. 2004. Coordination in rapidly evolving disaster response systems the role of information. Amer ican Behavioral Scientist, 48(3): 295–313.

Coombs, W.T. 2015. Ongoing Crisis Communication, 4th edn. Thousand Oaks: Sage.14

Davenport, T.H. and Prusak, L. 1997. Information Ecology: Mastering the Information and Knowledge Environment. Oxford: Oxford University Press.

Dasho, K. U. & de Pablos, P. O. (2014). Asian Business and Management Practices: Trends and Global Considerations: Trends and Global Considerations, IGI Global

De Cremer, D. (2015). Huawei: A Case Study of When Profit Sharing Works, Harvard Business Review. Retrieved from https://hbr.org/2015/09/huawei-a-case-study-of-when-profit-sharing-works

Deyo. F.C. 1987. The Political Economy Of The New Asian Industrialism, New York, Cornell University Press,

Ejaz W. Anpalagan A. 2009 Internet of Things for Smart Cities: Technologies, Big Data and Security, NY, Springer

Elwood, S. and Leszczynski, A. 2013. New spatial media, new knowledge politics. Transactions of the Institute of British Geographers, 38(4): 544–559.

Fingas, J. (2013, October 28). Huawei overtakes LG in smartphone market share during Q3. *Engadgt*. Retrieved from: http://www.engadget.com/2013/10/28/huawei-overtakes-lg-in-smartphone-market-share-during-q3/

Floridi, L. 2012. Big data and their epistemological challenge. Philosophy & Technology, 25: 435–437.

Fonio, C., Giglietto, F., Pruno, R., Rossi, L. and Pedrioli, S. 2007. Eyes on you: Analyzing user generated content for social science. Towards a Social Science of Web, 2: 1–11.

Forbes. (2013, Aug 26). Huawei's CEO: The innovation journey to 5G and beyond. *Forbes*. Retrieved from: http://www.forbes.com/sites/forbesasia/2013/08/26/huaweis-ceo-the-innovation-journey-to-5g-and-beyond

Foucault, M.2004 Sécurité, territoire, population. Cours au Collège de France (1977-78), Paris : Gallimard/Seuil (Collection « Hautes Études »).

Friedewald,M. Burgess, J.P. Čas, J. Bellanova R. and Peissl W. (Eds) Surveillance, Privacy and Security Citizens’ Perspectives OUP, Oxon Routledge 2017

Frost & Sullivan. *(*2007, Oct 3). Stars in the telecom infrastructure market: 3Com acquisition by Bain and Huawei.*Frost & Sullivan Market insight.*Fuchs, C., Boersma, F.K., Albrechtslund, A. and Sandoval, M. (Eds.). 2011. Internet and Surveillance. London: Routledge.

Fuchs, C., Boersma K. Albrechtslund A. and Sandoval M. 2011. Internet and Surveillance: The challenges of web 2.0 and social media. London: Routledge.

Gandy, O.H. 1989. The surveillance society: Information technology and bureaucratic social control. Journal of Communication, 39(3): 61–76.

Giddens, A. 1985. A Contemporary Critique of Historical Materialism: The Nation- State and Violence, Vol. 2. Berkeley: University of California Press.

Gómez-Ibáñez, J. 2003 Regulating Infrastructure: Monopoly, Contracts, and Discretion, Harvard University Press Cambridge MA.

Gorman, S. (2012, Oct 8). China tech giant under fire, Congressional probe says Huawei poses national-security threat to the U.S. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10000872396390443615804578041931689859530

Greenwald, G. 2014. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Picador.

Greenberg, A. (2012, Sep 10). A better approach to Huawei, ZTE and Chinese cyberspying? Distrust and verify. *Forbes*. Retrieved from: http://www.forbes.com/sites/andygreenberg/2012/10/09/a-better-approach-to-huawei- zte-and-china-distrust-and-verify/

Hadfield, A. and Zwitter, A. 2015. Analyzing the EU refugee crisis: Humanity, heritage and responsibility to protect. Politics and Governance, 3(2): 129–134.

Haggerty, K.D. and Samatas, M. (Eds.). 2010. Surveillance and Democracy. New York:

Routledge- Cavendish.

Hiltz, S.R. and Plotnick, L. 2013. Dealing with information overload when using social media for emergency management: Emerging solutions. Proceedings of the 10th International ISCRAM Conference, 823–827.

Hughes, A.L. and Palen, L. 2009. Twitter adoption and use in mass convergence and emergency events. International Journal of Emergency Management, 6(3): 248–260.

Huawei. (2010). *2009 Annual Report.* Huawei Technologies Co. Ltd. Retrieved from http://www.huawei.com/ucmf/groups/public/documents/webasset/hw_092117.pdf

Huawei. (2011). *2010 Corporate Social Responsibility Report.* Huawei Technologies Co. Ltd. Retrieved from www.huawei.com/ilink/au/download/HW_093033

Huawei. (2013). *2012 Annual Report*. Huawei Investment & Holding Co., Ltd. Retrieved from http://www.huawei.com/ucmf/groups/public/documents/annual_report/hw_u_256032.pdf

Huawei. (2016). *2015 Annual Report*. Huawei Investment & Holding Co., Ltd. Retrieved from http://www.huawei.com/ucmf/groups/public/documents/annual_report/hw_u_256038.pdf

Huawei News. (2011, Nov 22).Huawei awarded with Global Growth and Innovation in Telecom Managed Services Award by Frost & Sullivan. *Huawei News*. Retrieved from: http://pr.huawei.com/en/news/hw-104662- globalgrowthinnovationmanaged.htm#.Uq0a5vQW3gs

Huawei News. (2012, Dec 18). Huawei honored with Frost & Sullivan's '2012 Product Innovation Award' in the Middle East. *Huawei News.*

Harney, A. (2005). The challenger from China: why Huawei is making the telecoms world take notice, *Financial Times.* Retrieved from http://www.ft.com/intl/cms/s/0/3696d4cc-6376-11d9-bec2-00000e2511c8.html#axzz3qGSSOlFO

Hiltz, S.R. and Plotnick, L. 2013 Dealing with Information Overload When Using Social Media for

Emergency Management: Emerging Solutions. Proceedings of the 10th International ISCRAM Conference, Baden Baden, Germany.

Huawei. (2014). Huawei Financial Results, Retrieved 28 July 2015. International Data Corporation (IDC). (2015). Worldwide Quarterly Mobile Phone Tracker, Retrieved fromhttp://www.idc.com/prodserv/smartphone-market-share.jsp

Huijboom N. and Bodea G. 2015 Understanding the Political PNR Debate in Europe: A Discourse Analytical Perspective, European Politics and Society, 16:2, 241-255.

International Federation of Red Cross, Red Crescent Societies, & Centre for Research on the Epidemiology of Disasters. 2005. World Disasters Report. Bloomfield: Kumarian Press.

Jenness, V., Smith, D. and Stepan- Norris, J. 2007. Editors' note: Taking a look at surveillance studies. Contemporary Sociology: A Journal of Reviews, 36(2): vii–viii.

Jordana, J. Levi-Faur, D. & Puig, "The Limits of Europeanisation: Regulatory Reforms in the Spanish and Portuguese Telecommunications and Electricity Sectors," *Governance*, 19, 3, (2006): 437-464.

Kaufmann S. and Wichum R. 2016 "Risk as an Analytical category: Selected Studies in the Social History of the Twentieth Century" in Historical Social Research / Historische Sozialforschung Vol. 41, No. 1 (155), (2016), pp. 48-69

Kaufmann,F. 1973. Sicherheit als soziologisches und sozialpolitisches Problem: Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften. Stuttgart: Enke

Kim, B. (2014). Huawei to focus more on smartphone business, *The Korea Times.* Retrieved from https://www.koreatimes.co.kr/www/news/biz/2014/05/335_156166.html

Latour, B. Enquête sur les modes d'existence : Une anthropologie des modernes, La Découverte, 2012

Lincoln T. and Tao X. eds., 2016. The Habitable City in China: Urban History in the Twentieth Century. London Palgrave Macmillan,

Link, D., Meesters, K., Hellingrath, B. and Van de Walle, B. 2014. Reference task- based design of crisis management games. Proceedings of the 11th International Conference on Information Systems for Crisis Response and Management (ISCRAM), University Park, 592–596.

Luo, Y., Cacchione, M., Junkunc, M., & Lu, S. C. (2011). Entrepreneurial pioneer of international venturing: The case of Huawei. Organizational Dynamics, 40(1), 67-74.

Lyon, D. 2001. Surveillance Society: Monitoring Everyday Life. Buckingham: Open University Press.

Lyon, D. 2007. Surveillance Studies: An Overview. Cambridge: Polity Press.

Lyon, D. 2015. The Snowden stakes: Challenges for understanding surveillance today. Surveillance & Society, 13(2): 139–152.

Mapunda, G. An African perspective of the globalization of Chinese business practices in *Julian*, CC, *Ahmed*, ZU & Xu, J (eds) 2014, *Research handbook on the globalization of Chinese firms*, Edward Elgar Publishing, Cheltenham, UK

McAfee, A., Brynjolfsson, E., Davenport, T.H., Patil, D.J. and Barton, D. 2012. Big data: The management revolution. Harvard Bus Review, 90(10): 61–67.

Mayer- Schönberger, V. and Cukier, K. 2013. Big Data: A Revolution That Will Transform How We Live, Work, and Think. London: John Murray Publishers.

Meier, P. 2015. Digital Humanitarians: How Big Data is Changing the Face of Humanitarian Response. London: CRC Press.Big data, surveillance and crisis management 15

Meijer, A., Boersma, F.K. and Wagenaar, P. (Eds.). 2009. ICTs, Citizens and Governance: After the Hype! Amsterdam: IOS Press.

Mulder, F., Ferguson, J., Groenewegen, P., Boersma, F.K. and Wolbers, J. 2016. Questioning Big Data: Crowdsourcing crisis data towards an inclusive humanitarian response. Big Data & Society, 3(2): 1–13.

Murakami Wood, D. and Webster, C.W.R. (2009). 'Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example', Journal of Contemporary European Research. 5 (2), pp. 259-273.

Nankervis, A. R., Lee, F. C., Chatterjee, S. R., Warner, M. (2013). *New Models of Human Resource Management in China and India*, New York, NY: Routledge.

NASDAQ. (2015). Apple Inc. Profitability Analysis. Stock Analysis on Net. Retrieved from https://www.stock-analysis-on.net/NASDAQ/Company/Apple-Inc/Ratios/Profitability

Newsweek. (2006) The Huawei Way, Retrieved from http://www.thedailybeast.com/newsweek/2006/01/15/thehuawei-way.html.

Oh, O., Agrawal, M. and Rao, H.R. 2013. Community intelligence and social media services: A rumor theoretic analysis of tweets during social crises. MIS Quarterly, 37(2): 407–426.

Osawa, J. & Kim, Y. (2014). Huawei Is Shaking Up the Smartphone Market. *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/huawei-is-shaking-up-the-smartphone-market-1408908924

Ovide, S. & Wakabayashi, D. (2015). Apple's Share of Smartphone Industry's Profits Soars to 92%. *The Wall Street Journal.* Retrieved from http://www.wsj.com/articles/apples-share-of-smartphone- industrys-profits-soars-to-92-1436727458

Palen, L. 2008. Online social media in crisis events. Educause Quarterly, 31(3): 12.

Pan, S.L., Pan, G. and Leidner, D.E. 2012. Crisis response information networks. Journal of the Association for Information Systems, 13(1): 31–56.

Patrignani, N., & Whitehouse, D. (2018). Slow tech and ICT: a responsible, sustainable and ethical approach. Chatam: Palgrave Macmillan

Pearson, C.M. and Clair, J.A. 1998. Reframing crisis management. Academy of Management Review, 23: 59–76.

Pries, K.H. and Dunnigan, R. 2015. Big Data Analytics: A Practical Guide for Managers. London: Routledge.

Procter, R., Vis, F. and Voss, A. 2013. Reading the riots on Twitter: Methodological innovation for the analysis of big data. International Journal of Social Research Methodology, 16(3): 197–214.

Quarantelli, E.L. (Ed.). 1998. What is a Disaster? Perspectives on the Question. London: Routledge.Prasso, S. (2011). What makes China telecom Huawei so scary? *Fortune.* Retrieved from http://fortune.com/2011/07/28/what-makes-china-telecom-huawei-so-scary/

Shelton, T., Poorthuis, A., Graham, M. and Zook, M. 2014. Mapping the data shadows of Hurricane Sandy: Uncovering the sociospatial dimensions of "big data." Geoforum, 52: 167–179.

Shih, G. (2014). Huawei's smartphone sales shoot up after copying Xiaomi's online strategy. *Reuters*. Retrieved from http://www.reuters.com/article/2014/12/23/us-huawei-tech-mobilephone-idUSKBN0K11QV20141223#0PtMjtFud8ARYqIB.99

Shih, G. (2015). China's Huawei leads international patent filings: WIPO. *Thomson Reuters*. Retrieved from http://www.reuters.com/article/us-huawei-patent-idUSKBN0MF17820150319

Stout, K. L. (2013). Would you buy a Huawei smartphone? *CNN*. Retrieved from http://edition.cnn.com/2013/05/09/business/china-huawei-smartphones-stout/

Tene, O. and Polonetsky, J. 2012. Big data for all: Privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property, 11: xxvii.

Trottier, D. and Schneider, C. 2012. The 2011 Vancouver riot and the role of Facebook in crowd- sourced policing. BC Studies: The British Columbian Quarterly, 175: 57–72.

Truptil, S., Bénaben, F., Couget, P., Lauras, M., Chapurlat, V. and Pingaud, H. 2008. Interoperability of information systems in crisis management: Crisis modeling and metamodeling. In: Enterprise Interoperability III, 583–594. London: Springer.

Turoff, M. 2002. Past and future emergency response information systems. Communications of the ACM, 45(4): 29–32

Turoff, M., Chumer, M., Van de Walle, B. and Yao, X. 2004. The design of a dynamic emergency response management information system (DERMIS). Journal of Information Technology Theory and Application, 5(4): 1–35.

The Economist. (2012). Who's afraid of Huawei? Retrieved from http://www.economist.com/node/21559922

Ura, D.K. and Ordonez de Pablos, P. (ed), Asian Business and Management Practices: Trends and Global Considerations, IGI Global, Hershey, 2015

Valverde, M. and Mopas M. 2004. 'Insecurity and the Dream of Targeted Governance' in Larner W. and Walters W.(eds) Global Governmentality, London: Routledge

Van de Walle, B., Turoff, M. and Hiltz, S.R. (Eds.). 2009. Information Systems for Emergency Management. New York: ME Sharpe.

Van der Vegt, G.S., Essens, P., Wahlström, M. and George, G. 2015. From the editors: Managing risk and resilience. Academy of Management Journal, 58(4): 971–980.

Van Dijck, J. 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society, 12(2): 197.

Van Winden, W. Braun, E. Otgaar, A. J. Witte. Urban Innovation Systems What makes them tick? New York, Routledge, 2014

Wagenaar, P. and Boersma, F.K. 2008. Soft sister and the rationalization of the world: The driving forces behind increased surveillance. Administrative Theory & Praxis, 30(2): 184–206.

Webster, C.W.R., Balahur, D., Zurawski, N., Boersma, F.K., Ságvári, B. and Backman, C. 2012. Living in surveillance societies: The ghosts of surveillance. Proceedings of LISS Conference, Vol. 2, Stirling.

Wolbers, J. and Boersma, F.K. 2013. The common operational picture as collective sensemaking. Journal of Contingencies and Crisis Management, 21(4): 186–199.

Witzel, M. and Goswami, T. (2012). The case study: Huawei's entry to India. *Financial Times*. Retrieved from http://www.ft.com%2Fcms%2Fs%2F0%2Fa7c4d656-fe89-11e1-8028-00144feabdc0.html&usg=AFQjCNFY4tNu6oYJ2Tm-t1IdnOKyrsKeXQ

Yates, D., & Paquette, S. 2011. "Emergency knowledge management and social media technologies : A case study of the 2010 Haitian earthquake" in International Journal of Information Management, 31(1), 6–13.

Zhao, H. (2010). Why Huawei Doesn't Get Its Way. Caixin. Retrieved from http://english.caixin.com/2010-08-11/100169742.html