Smart Cities, Cyber Warfare and Social Disorder

Simona R. Soare
Senior Associate Analyst
European Union Institute for Security Studies (EUISS)

Joe Burton
Marie Curie Fellow, Université libre de Bruxelles (ULB) and Senior Lecturer
New Zealand Institute for Security and Crime Science
University of Waikato

Abstract: Cyber warfare often targets national security apparatus, but local governance vulnerabilities are just as serious and much less studied. In this paper, we examine the potential impact of cyber warfare directed against smart cities and the relationship between cyber attacks and social disorder in urban spaces. The first part of the paper consists of a foresight scenario that serves to identify operational, procedural, governance and capability gaps in responding to and building resilience against fictional, but possible events. In our foresight scenario, Megalopolinn, the capital of a major European NATO ally, comes under a sustained cyber assault from a network of hackers linked to an authoritarian, revisionist state. We map out the multiple surfaces of cyber attack in a smart city grid and how they contribute to a serious breakdown in the city's social, political and technical structures and processes when combined with other hybrid warfare tactics. The second section is a more conventional academic analysis of existing literature on cities as actors in International Relations and the smart city as an emerging unit of analysis in security policy and planning. The third section provides a comprehensive analysis of the rise of smart cities and the vulnerabilities in smart city infrastructure and technologies, including artificial intelligence (AI) and automation, the Internet of Things (IoT), 5G, social media, synthetic media and deepfakes, and the risks posed to governance structures and capabilities that rely on super-connectivity and complex networks. We highlight three vulnerabilities of smart cities – technological, social and governance-related. This section argues that local governance is potentially an easier attack surface than the national level for malign actors who seek mass disruption and that significant changes in local governance structure and practice are needed to close smart city vulnerabilities, including a better understanding of the links between smart city security and national security.

Keywords: *Smart city, cyber warfare, hybrid warfare, local governance, national security, NATO*

1. DARK DAYS IN MEGALOPOLINN

February 2030. The smart city infrastructure of Megalopolinn is under attack. Megalopolinn is Varmatia's largest city, with over 10 million inhabitants. It generates over 30 per cent of Varmatia's GDP and is a major European transport hub and pivotal to NATO logistics, defence planning, military mobility, and reinforcement of Eastern European allies. Varmatia is bordered by Lusia, a hostile foreign power, with which it has a history of confrontation.

At 19:43, on 2 February, massive AI-enabled Distributed Denial of Service (DDoS) attacks, harnessing the city's millions of IoT devices, cripple Megalopolinn's 5G servers and transmission masts. The smart city's master network has been infected by a self-replicating and self-learning worm, which is rapidly propagating through the smart critical infrastructure grid. Within hours, the malware cascades through different sectors of the grid, disabling City Hall servers and cutting GPS services used by the police and emergency services. The coordinated assault shuts down the power and water supply to half the city's population. Citizens do not have access to clean water or electricity, they cannot heat their houses, withdraw money, communicate with loved ones or city authorities.

Megalopolinn is surrounded by navigable water canals, operated by a fully automated water and navigation management system. The worm infects and manipulates the automated industrial control system of the city's canals and dams, leading to the progressive flooding of an area roughly the size of Brussels. The city provides the largest rail transport hub in central Europe and is relied upon by the EU and NATO for military mobility. The flooding occurs just seven days before the DEFENDER 2030 transatlantic military exercise, which depends on the city's infrastructure for the transit of troops and equipment.

Further fuelling popular anger, a video spreads online depicting Megalopolinn's Mayor deriding the desperation of city dwellers. The European Union (EU) East StratCom Task Force (a key EU instrument tasked with countering misinformation campaigns) reports a spike in anti-Varmatian, anti-EU and anti-NATO 'deepfake' videos—synthetic media produced by AI algorithms (Barnes and Barraclough, 2020). National regulation does not allow their rapid removal without due process. In a public address on national television, the City's Mayor, in violation of cyber response protocols, attributes the attack on his smart city to Lusia. National authorities have not been consulted on this attribution, but Lusia is responding aggressively and threatening massive repercussions.

By 3 February, riots, looting, destruction of property and cases of violence are reported throughout the city. Police response is obstructed by the malware, which has disabled smart alarm systems and CCTV cameras and is preventing law enforcement drones from transmitting data necessary for accurate situational awareness. The rioters, armed with Molotov cocktails, baseball

bats and small arms, have placed barricades along all the main roads into the city, and the underground system has ground to halt.

By 5 February, law enforcement is overwhelmed, and rioters are threatening to break into City Hall. The Varmatian government is ready to declare a national emergency. The Varmatian ambassador to NATO hands in an official request for an urgent North Atlantic Council (NAC) meeting to inform allies of potential disruptions to NATO activities and to present allies with intelligence suggesting the Lusian government is orchestrating a sophisticated cyber and hybrid attack against Megalopolinn.

2. THE BRITTLENESS OF SMART CITIES

As the foresight scenario above demonstrates, smart cities are brittle architectures. From technological, social and governance points of view, they have multiple points of failure with cascading, systemic effects. The purpose of the foresight scenario is not to depict the future but to raise awareness of less visible risks and vulnerabilities—in this case, the interdependencies between smart city grids, local governance and social order. The scenario also serves to highlight how smart city security risks might affect broader national and allied security. Our goal in this paper is to analyse the multiple vulnerabilities, risks and threats faced by smart cities and map out much-needed changes in technological, social and governance approaches to help increase local preparedness and enhance resilience in the face of catastrophic cyber and hybrid events.

What are the main vulnerabilities and threats faced by smart cities? How do we conceptualise them in an allied framework? In an attempt to answer these questions, this paper proceeds as follows. First, we define and analyse the role of cities as actors in international relations and particularly of smart cities as an emerging unit of analysis in security policy planning. Then, we analyse the vulnerabilities, risks and threats faced by smart city infrastructure in cyber and hybrid warfare. We argue that the growing body of literature on the security of smart cities is limited to a primarily technological approach. Smart city vulnerabilities are as much technological as they are human, social and governance driven. For a more comprehensive view, a more encompassing definition of smart cities as synergetic physical, virtual and human systems is required. Furthermore, we argue that a particular focus is needed on clarifying and exercising the connections between smart cities and national security.

A. Cities and International Security

Cities were not the traditional focus of International Relations (IR) or Security Studies literature. During the Cold War, states were the main unit of analysis and were central to realist accounts of international relations. The emergence of the 'national security state' drew particular attention, as the dangers of the Cold War, nuclear arms race and fears of revolutions led to the

creation of powerful security and intelligence apparatus (Raskin, 1976). In the mid-to-late 1980s, however, the focus of IR began to change, and a variety of non-state actors, including terrorist groups and international organisations became the focus of analysis. States were not a 'black box' according to these emerging understandings; what happened inside the state was important in shaping international affairs, and a new range of international theories sought to focus on sub-state actors, identity groups and societal dynamics (Buzan, 1991).

Two emerging trends led scholars to include cities in IR analysis. The first was the trend of globalisation, which increased the political, financial and military relevance of cities and their role as command posts and centres of planning (Alderson et al., 2006). The combination of globalisation's effects and the rapid spread of information and communication technologies (ICTs) made the world 'flat' and global changes had localised effects and vice-versa. The second trend related to urbanisation, a process that has been driven by globalisation, the rise in international markets, industry, the emergence of service-driven economies and job opportunities, and the decline of rural living and economies. Since 2016, over half the world's population has lived in cities, and this is set to rise to two-thirds, an estimated 7 billion people, by 2050 (Ritchie & Roser, 2018).

Cities are not always safe places for people to be. Almost a quarter of people in cities globally live in slum accommodation (United Nations, 2020), and there are grave concerns about how this trend will affect social cohesion and equal access to critical public services, including basic healthcare, transport, water and energy. Recent reports suggest that the growth in urban populations will require a $78 trillion infrastructure investment in the coming years (PWC, 2020). Cities consume 75 per cent of the world's natural resources and are responsible for 80 per cent of global carbon emissions (PWC, 2020). Managing the future of urbanisation, including environmental, economic and social sustainability, will be crucial to urban security as we move further into the 2020s.

Cities serve several important political, economic and security functions. They are major economic hubs. The global stock markets are dominated by New York, Hong Kong, London and Tokyo, and they host the global financial infrastructure and institutions that make the global economy run (Statista, 2020). Cities are also major diplomatic hubs, serving global political relationships, with embassies, consulates and myriad private interests circulating for political influence. They have also become important actors in their own right, with a growing agency in international affairs. The ascension of global cities has allowed a range of internationally influential leaders to emerge, from Boris Johnson to Rudy Giuliani; figures who have transcended city politics and built international reputations. Cities have become strategic resources in wars and civil conflicts, too. The 1993 'Black Hawk Down' incident in Mogadishu and the battle for Fallujah in Iraq had major implications for the outcomes of those conflicts and cities have also been sites of major

political transitions such as the Arab Spring which was centred in Tahrir Square in Cairo. Cities also host iconic landmarks such as the Eiffel Tower, Big Ben, One World Trade Center, Sydney Harbour Bridge and Burj Khalifa which have wider political and security significance.

B. The Rise of the Smart City

Smart cities can be defined as those that effectively integrate physical, digital and human systems in urban environments to deliver sustainable, prosperous and inclusive outcomes for their citizens (British Standards Institute, 2014). At present, technology is certainly present in cities, but fully integrated and automated forms of technological governance that connect different services and the people that use them are still under development. Achieving positive outcomes depends on smart city security, and a growing body of literature has emerged addressing the many technological vulnerabilities that appear to be built into smart city projects. The growing dependency of smart cities on technological interconnectivity and data is also increasing their known and unknown vulnerabilities to cyber attacks and threats from foreign hybrid influence. There is a growing literature on the multiple attack surfaces that a smart city grid presents to adversaries and growing concerns over the threats to civil and political rights that they engender (Sookhak et al., 2019). Other scholars have emphasised the security challenges involved, and particularly attacks that cause disruption to services and steal or manipulate the data collected by sensors (Elmaghraby & Losavio, 2014). Smart city infrastructure consists of smart public transport and traffic control, a smart energy grid, smart water supply, smart waste management, smart building operations, smart healthcare, smart delivery systems, smart local governance services, smart back-office systems and others. These smart services are enabled by a synergetic network of physical and virtual infrastructure that redefines how citizens interact with the city and with local governance. 5G networks, the IoT and autonomous service networks and platforms (electronic services that are automated, with humans in-the-loop) are expected to transform and refine smart city design, operations and efficiency as the 2020s unfold. Each of the smart city infrastructure components presents numerous vulnerabilities, but it is the complex, multi-layered and highly interconnected system-of-systems in a smart city infrastructure that is systemically vulnerable to a growing number of threats from cyber crime to hybrid warfare.

At present, there are hundreds of smart city initiatives across the transatlantic area, including iCity in Spain, Triangulum in the UK, and DIMIS in Germany (Nominet, 2018). In 2019, local governments globally spent $95 billion on smart city technologies and global smart city initiative spending is forecast to reach $189 billion by 2023 and $263 billion by 2028 (International Data Corporation, 2020). A simple inventory of the sheer number of municipalities and local governments across Europe offers an even more sobering overview of the scale of the challenge: there are over 87,800 municipalities and local governments in European NATO members and over 88,200 in the EU (vom Howe et al., 2019). These municipalities are home to 74 per

cent of the population in Europe and 82 per cent in North America (United Nations, 2018). The US Department of Transportation has issued a 'Smart City Challenge' and in 2014 the National Institute for Standards and Technology (NIST) launched its Smart Cities and Communities Framework. The European Commission (EC) launched a European innovation partnership on smart cities and communities and since 2017 has spent over €53,5 million on projects addressing the energy, transportation and environmental aspects of smart city grids (EC, 2020a). Already, Europe and North America are home to 26 of the world's largest smart city infrastructures (Eden Strategy Institute, 2018). Europe has the highest density of smart city initiatives (IESE Business School, 2019). A majority of municipalities in the transatlantic area will implement at least some form of smart city infrastructure in the next decade and many such initiatives will increasingly be interconnected across regions and share the same technology, software and hardware in the process. This opens the very real possibility that a successful hack of one such vulnerable system can be replicated en masse, with the help of automated virtual tools to affect multiple cities simultaneously.

3. BRITTLE-AT-THE-MAKING? MAPPING SMART CITY VULNERABILITIES

There is a growing awareness of the cyber security risks embedded in smart city infrastructure and their potential physical effects (US Department of Energy, 2017). Rather than being risk averse, the response framework has been one of risk management (US Department of Homeland Security, 2015). The costs of cyber security for smart city infrastructure between 2020-2024 are projected to grow to over $135 billion (ABI Research, 2019), meaning cyber security design and maintenance becomes comparable to the very development of smart city initiatives. Governments and international organisations in the transatlantic area have developed risk mitigation measures to build 'security by design' into smart city grids. These include a myriad of standardisation and certification schemes, including ISO standards for smart cities (ISO/IEC, 2020), EU certification for ICT devices and services (EC, 2020), the US NIST IoT security requirements (Fagan & Megas, 2020; Singhal, 2020) and NATO telecommunications requirements (NATO, 2019; 2020). There is also specific regulation for critical infrastructure protection, with which national authorities and operators of smart city services all have to comply. Because implementation of these standards and regulations remains a national prerogative, differences in strategic focus, technological capacity and available budgets explain different levels of performance.

Yet, despite these growing investments in cyber security, the threats and vulnerabilities of smart cities are still expanding. Between 2010-2014, the US Department of Energy reported over 1,130 cyber attacks against the national critical infrastructure grid, including 19 against nuclear weapons stockpile facilities; 14 per cent of these attacks were successful, leading to disruption of energy supply services and loss of integrity of the data and industrial

command systems at several facilities (Reilly, 2015). Between 2018 and 2019, there was a 363% increase in the targeting of organisations (including local government entities) by hackers (Malwarebytes, 2019) in a trend that points to a significant shift in the activity patterns of cyber attacks and cyber conflict more broadly, from a focus on attacking individuals towards ever-larger entities, especially organisations and local government entities. This trend of increasingly sophisticated, targeted and widespread cyber-attacks, including against local governance and private industry, is well documented in Europe, too (ENISA, 2020).

Unlike national authorities and large organisations which possess the necessary funding, the technology and, more often, the skilled workforce needed to defend against cyber attacks or comprehensively tackle hybrid warfare campaigns, local governments are far easier targets for technological, social and governance reasons. The systemic approach to the security of smart cities seems to be technologically brittle-by-default, socially brittle-by-nature and politically brittle-by-design.

A. Brittle-by-default? Technological Vulnerabilities of Smart Cities

Smart energy grids and smart water management systems can create security vulnerabilities because they are deployed as a layer over legacy systems with many cyber vulnerabilities that are aggravated by poor maintenance. Some services, for example, use operating systems that have not been updated or patched since the late 1990s or early 2000s, (such as Windows XP, that was exploited during the WannaCry attack) making them easy access points into the smart city grid where hackers can disrupt and corrupt other components. A recent industry report identified 17 distinct 'zero-day' vulnerabilities across four types of smart city systems, eight of which were classified as being of 'critical severity' (Warwick, 2018). While access to these legacy systems is becoming easier, the detection and repair of compromised devices in the network can be extremely challenging and costly (Cerrudo, 2014). For example, detecting a data breach takes on average six months or longer (ENISA, 2020). The multitude of systems, devices and protocols in smart city infrastructure, ranging from Bluetooth to 5G, both software and hardware components, and those produced and operated by a multitude of stakeholders, makes interoperability, coordination and compliance monitoring of common security standards difficult (US Department of Homeland Security, 2015). It also obscures clear lines of responsibility and accountability for failures in the system.

New components and technologies added into smart city networks—such as sensors and IoT devices—continue to be vulnerable, despite the adoption of cyber security standards, safeguards and authentication protocols across the transatlantic area. The focus on increasing broadband access and reducing network latency has led to an increased density of oversubscribed networks, which is particularly relevant in times of crisis when networks experience rapid spikes in data use (Afflerbach, 2020). These networks cannot accommodate all subscribers—people and IoT devices—making them brittle and

prone to failure. Most water and energy contractors have different cyber security protocols and use supervisory control and data acquisition (SCADA), an automation control system that has been proven to be a significant and multi-faceted single point of failure in smart city grids (Kitchin & Dodge, 2017). In a system as interconnected as a smart city, security is a function of its weakest component. As a result of the smart city's high interconnectivity of the data and the systems that run on it, the corruption or disruption of one part of the puzzle has important cascading effects across the entire grid. Jamming and spoofing GPS signals can disrupt critical services such as police, fire, emergency medical services, power grids and financial markets (Polunsky, 2019). These effects can easily be achieved through the use of small commercially available drones.

The market is saturated with producers offering smart city technologies at increasingly affordable prices, which is attractive to local governments whose procurement budgets are under constant pressure. Nevertheless, many producers of smart city technologies lack the experience or best practices on inbuilt cyber security measures in the products they sell. Encryption is rarely a staple of local data (with important implications for privacy and safety) and software is generally used with default cyber security settings still in place. Even where encryption of data could be considered, the widespread deployment of low-power sensors makes their inclusion on an encrypted network link difficult. Local governments generally lack the funding incentives necessary to recruit, train and retain skilled experts to design, operate and maintain their digital critical infrastructure, which leaves open higher risks for human error. A distracted, undertrained or dissatisfied employee can—willingly or not—invite vulnerabilities into the network. As the number of cyber attacks against local entities increases (even more so since Covid-19), phishing emails remain the most widely used tool to gain access into the system. However, new forms of malware and ransomware are also proliferating alongside the malign exploitation of weak personal authentication (Ferbrache, 2020).

Paradoxically, public procurement is still not focusing enough on security-by-design approaches to the technologies and services acquired. Local procurement of new services and technologies may be prioritised because of public visibility gains, despite the high costs, and to the detriment of servicing older systems already deployed in the critical infrastructure grid. For example, a 2018 UK government report estimated the cost of the upgrade of national and local broadband networks to be £33,4 billion over a decade; however, the amount could be 30 per cent lower if authorities gradually upgraded the infrastructure over a longer period (UK NIC, 2018: p. 21). Extended periods of budgetary austerity in the transatlantic area have made long-term local underinvestment in critical infrastructure even more likely. An expected economic downturn as a result of the COVID-19 crisis will incentivise local governments to implement more smart city initiatives while also making more budget savings.

The private sector has led the notable (but also profit-seeking) effort to address technical and cyber security challenges posed by emerging smart city infrastructure. The array of technical solutions includes prioritisation of data security and integrity (especially in the context of 5G networks); failsafe and overriding mechanisms, especially for large-scale command systems; access controls; data encryption; higher IT and cyber security standards and regularly updated security protocols; software patching; the deployment of network intrusion mechanisms; and staff training (Deloitte, 2019). Despite the technological solutions available, cyber or hybrid disruption by state and non-state actors below the use of force and with both military and civilian socio-technological tools rewards the disruptor. It is relatively cheap (ex. dark web ransomware is available for under $50), it provides perpetrators with revenue from, for example, ransomware premiums, and it has public visibility as a result of the days or months-long disruption to local government and public services caused by the attacks (Fernandez et al., 2019). The consequences of cyber attacks on smart city grids have important financial and public trust costs for local governments. Technological vulnerabilities are an important route through which cyber warfare can be instigated, but they are not the only ones. People are the other big part of the smart city puzzle and we discuss this aspect next.

B. Brittle-by-nature? Social Vulnerabilities of Smart Cities

An internet search of 'smart city vulnerabilities' reveals 7,9 million responses, the vast majority of which focus on technical challenges, technical mitigation and technical solutions. Even military literature reveals a predilection with technological challenges and solutions in smart city and urban environments, albeit one that is balanced by practical operational considerations (NATO STO, 2020). The 2018 NATO Capstone Concept on Urban Warfare, for example, includes considerations of the effect the social structure of a city has on the security and success of military operations. Even data privacy literature focuses on the technical rather than the social aspects. Paradoxically, the literature on smart city infrastructure almost entirely avoids considerations of the city's social structure as part of its critical infrastructure, including human behaviours and psychology, challenges related to social cohesion and group identity and issues around social justice and equality. This is an important gap considering that disinformation and 84 per cent of cyber attacks rely on some form of social engineering (ENISA, 2020).

For city inhabitants, the dense smart city infrastructure reconceptualises the city as a 'platform for services' (Kitchin & Dodge, 2018). Local governments provide apps that GPS-track and estimate the arrival time of public transportation (buses, underground, trains), online tax submission, healthcare apps and others. Recent research at Carnegie Mellon University revealed smart city design and operations require more attention to safety, sustainability, equity and resilience. The United Nations (UN) cautions that technological change and smart urbanisation can serve as critical channels for social inclusion, but they can also worsen social exclusion. A city's pre-existing social structure is influential in shaping the impact on smart city infrastructure. Private tech

companies refuse to sell facial recognition technology for smart policing applications used by local law enforcement agencies across the US because the technology is brittle and prone to social biases (Greene, 2020). Less affluent communities cannot afford the skilled work or the investments in modern and secure technologies to safely deploy smart city initiatives, which also increases rather than reduces social exclusion and equitable access to higher standards of living and better local government and public services.

The proliferation of online media as a source of information for an increasing number of people is facilitating the creation of 'echo chambers' for the proliferation of man-made or automated content that spreads disinformation. Cyber warfare and other malign influence campaigns are increasingly sophisticated and exploit local contexts, crises and social tensions. In the age of big data, foreign malign actors need not rely on more than off-the-shelf algorithms that sift through social media and open-source data to reveal several critical indicators for their targeted disinformation campaigns (Hybrid COE, 2020). In this context, big data analysis of Facebook and Twitter posts by a target city's dwellers can reveal their emotions about politically and socially relevant indicators such as elections, political figures, policy priorities or values that, if activated and amplified by disinformation, can undermine and divert democratic processes and institutions. Similar algorithms enable microtargeting of specific categories of a population with highly tailored content that can shape the democratic environment.

The advent of synthetic media, deepfakes and augmented reality tools that can already realistically portray real political leaders saying or doing things that they have never in reality done adds a layer of complexity to the human, behavioural and social challenge created by emerging technologies. This challenge is all the more concerning in dense urban areas, such as smart cities, where information overload and the inability of local governments to fully shape and control their information environments is a serious vulnerability.

Social disorder can be amplified faster today through malign hybrid influencing. Synthetic media with wide and rapid dissemination across dense information networks of smart cities can lead to significant and rapidly escalating social disorder. Because the nature of online communities is not geographically contiguous and urban populations share frustrations over aspects of local governance, smart city social tensions over real or doctored content and deepfakes have a great potential for contagion. As recent research shows, deepfakes and synthetic media are more likely to be deployed in a targeted manner such as during a crisis to maximise impact while avoiding detection, mitigation and attribution (Hwang, 2020).

The social, physical and virtual infrastructure in a smart city meets in another important domain—namely, the symbolism of specific city locations for political and social movements. Social geography is a well-studied factor that shapes urban environments and smart cities contribute to the creation

of urban social geography at scale. Places like Tahrir Square in Cairo, Tiananmen Square in Beijing, University Square in Bucharest, Maidan Square in Kiev and, more recently, Lafayette Square in Washington DC and the Justice Center area in Portland carry much social symbolism associated with the popular struggle against perceived national or local government abuse of power. The symbolism around city landmarks can also be an important trigger of social disorder, including during the Bronze soldier incident in Estonia in 2007.

Social disorder can also follow urban economic downturns, as seen in the massive protests against austerity across Greece. As in our scenario at the beginning of the article, inequities in cities and disparities in living standards can be extreme and be exploited by malicious actors. Global urban centres generate 80 per cent of global GDP (World Bank, 2020). A recent report showed smart city initiatives increased local economic growth by 21 per cent in 136 cities across the world (ESI ThoughtLab, 2020). The implementation of smart city infrastructure facilitated by technological innovations in 5G, big data, AI, robotics and IoT is also set to change patterns of urban economic activity (ex. automation), which will trigger short and longer-term changes in the city's socio-economic structure. Technological change could increase social exclusion through job polarisation, wage inequality and unequal access to public services particularly in large urban areas (UNDESA, 2020).

Privacy concerns and the integrity of personal data are just part of the debate over smart cities and a key part of the intersection between technological vulnerabilities and human-centred and societal dynamics, including societal security dilemmas where citizens fear other groups or their governments. With over 850 zettabytes of data created by over eight billion IoT devices in 2021 alone, the information contained by this largely unstructured and uncured data could reveal important insights for national governments and adversaries alike. Approximately 40 per cent of cities currently use predictive data, and the number of smart cities, volume and types of data (particularly AI-generated, geospatial and behavioural data use) are expected to grow exponentially over the coming years (ESI ThoughtLab, 2020: p. 23). Smart cities will channel and process huge amounts of private-individual and commercial-industrial data, both of which require increased security. A data breach that leads to widespread loss of private user data or proprietary industrial data can have significant local and national economic security implications by exposing industrial vulnerabilities, secrets or leading to a loss of economic competitiveness. This is a particularly significant security concern in Europe, which owns the world's largest volume of industrial data.

While cyber security threats to smart cities are evolving, the 'attack surface' of information warfare is likely to continue to include humans and machines. Unless a comprehensive systemic approach to smart city security is adopted to include its most valuable component—people—hybrid warfare campaigns will continue to undermine local government and security across the transatlantic space. Societal resilience is not a uniquely national-level construct—in fact, much of it begins from the bottom up and local governments,

particularly in the context of smart cities, as increasingly important actors in this process. Perhaps the way to refocus the narrative about the security of smart cities is to comprehensively redefine smart cities as synergetic and integrated physical, virtual and human components, structures and systems.

C. Brittle-by-design? The Missing Link Between Smart City and National Security

One aspect that is virtually absent from the literature on smart cities is their relationship to broader national security considerations and national and international politics, including crisis management. While local government entities are increasingly an appealing, albeit incidental target for cyber criminals driven by vulnerabilities rather than political motivations against specific cities, smart cities could increasingly present more attractive and easier targets for state adversaries or state-supported cyber criminals for disruption and destruction. Large smart city infrastructures like London, Paris and Amsterdam are critical parts of the national security grids and fundamental to economic security. Prolonged mass disruption of their infrastructure—as has been recently seen in the case of month-long disruption in public services as a result of cyber attacks against American municipalities (Robles, 2020)—would be a serious national security threat to allied nations.

This is in part a result of the lesser-known nature of the complex interdependencies and politico-administrative between the levels of local and national governance (Hybrid CoE, 2020). Recent research has revealed the high dependency of critical smart city infrastructure on services generally coordinated at the national level, including satellite-based services, GPS and 5G mobile networks. Despite the dependency of local government daily operations on such technologies, policy-making processes rarely if ever include local government representatives (Polunsky, 2019).

Lessons learned in the field of cyber security are already being broadened and applied in relation to local government and the security of smart city infrastructure, but greater cooperation is needed on lessons learned between local and national government, including relating to information-sharing on evolving cyber threats. The availability of national-level guidance on safety standards and protocols, the presence of local government representatives in national decision-making bodies on vital components of critical infrastructure—including critical infrastructure around democratic processes and institutions such as elections—and the establishment of flexible governance structures will become a prerequisite in ensuring the resilience and security of smart cities across the transatlantic area. In this respect, our argument is not that the national military should be more involved in the governance of cities, but that local government officials and processes should be better integrated into national decision making and security planning.

One urgent area to address is the clarification and exercise of clear roles and responsibilities for the secure operation of smart city infrastructure and for the response to a variety of types of events of varying scopes in relation to smart city infrastructure. There are national and supranational regulations

(EU and NATO) in place for the protection of critical infrastructure which encompasses national, federal and local authorities and private enterprises. Nevertheless, looking towards the future when hybrid and cyber threats will target the seam between the responsibilities of different national, local, governmental and private actors, further clarification and constant updating of these specific roles is required to avoid grey areas of responsibility.

Local threat mapping can be more complex than at the national level and growing cyber attacks against local government entities can make it difficult for local officials to see the bigger picture of hybrid influence campaigns. Local governments face more challenges in linking local effects and events with global competition dynamics, and often do not have the budgets, knowledge, resources or remits to do so. Facilitating deeper vertical (national-to-local) and horizontal (local-to-local) cooperation on best security practices for smart city infrastructure and for the response to events targeting smart city grids, information sharing, audits and the training and exercising of personnel—including contractors and private industry—would be essential steps towards enhancing the preparedness and resilience of smart city environments. This could involve a cyber security committee or advisory group staffed by representatives from the national security services, local government, police and tech sector, tasked with coordinating responses to major cyber incidents, or indeed a multi-stakeholder and municipality information sharing and analysis centre. Recent tensions between the City of London and the Johnson government over COVID-19 responses and the lack of City representation on the government's national emergency management committee are illustrative of the inherent political challenges here (O'Reilly, 2020).

Finally, why should an international alliance like NATO be concerned with smart city security? While sub-national security preparedness is a national responsibility, NATO decisions bear an indirect but critical role in how smart cities conceptualise and design their security architectures. For example, in December 2019 NATO updated its baseline security requirements for telecommunications systems, including 5G networks (NATO, 2019). National governments are principally responsible for the implementation of such requirements, but so are local governments. Yet national policies on telecommunications networks are made with little to no participation or input from local governments and private industry who are subject to said legislation. Smart city infrastructure threats can create important second and third-order effects for the national and alliance levels of governance. For example, cyber attacks on critical infrastructure that lead to man-made disasters such as floods or fires can divert the military capabilities needed for alliance missions over long periods. Alternatively, such events can disrupt military planning, including military mobility, or the operation of militarily relevant infrastructure and logistical hubs. Particularly in areas with greater local autonomy, uncoordinated local government decisions could create vulnerabilities that are less visible because of the lack of clarity over the relationships between security architectures at national and local levels, but that could nevertheless be systematically or opportunistically exploited by adversaries.

NATO Science and Technology Organization's (STO) 2020 Report on Science and Technology trends refers to smart cities as 'synergistic systems' that have critical consequences for the Alliance's ability to defend allied territory or engage in urban warfare beyond the transatlantic area (NATO STO, 2020). Unsurprisingly, the main preoccupation with urban environments in NATO is on the operational side. However, NATO and national military infrastructure largely rely on local public services and grids. Much can be done on improving the preparedness of local governments to withstand severe hybrid and cyber attacks on smart city infrastructure and prevail, whether the use of force is necessary or not. Venues like the NATO Parliamentary Assembly, NATO and EU Centres of Excellence and Atlantic Associations, but also engagement with local governance networks could help assist local and national governments and the Alliance, including by encouraging an acceleration across the transatlantic area of local government-oriented resilience and preparedness-enhancing measures.

4. CONCLUSION

The paper has argued that smart cities present a very real local challenge to national and international security policy at the technological, social and political governance levels. Cyber warfare, internet-enabled attacks by states against critical infrastructure and the malicious exploitation of information networks will target cities and their increasing connectivity. Such campaigns will have both political and social effects, including exacerbating identity divides, sowing division and eroding trust in governance systems and elected officials. The focus on technological solutions for smart city security obscures the adaptations needed in the broader local and national security ecosystem. The NATO 2030 reflection process presents a clear opportunity to think more deeply about the implications of local governance on the Alliance's ability to operate smoothly and efficiently in the coming decade. Continuing to build vertical and horizontal cooperation between local, national and allied security planning should be foregrounded in this process as a way of avoiding building brittle security structures.

5. REFERENCES

ABI Research. (2019) Lack of Critical Infrastructure Cybersecurity Investments in Smart Cities will Seed the Future IoT Vulnerabilities. Available from: https://www.abiresearch.com/press/lack-critical-infrastructure-cybersecurity-investments-smart-cities-will-seed-future-iot-vulnerabilities/ [Accessed 4th August 2020].

Afflerbach, A. (2019) Broadband Performance is About More than Speed, *CTC Technology*, available from: https://www.ctcnet.us/blog/broadband-performance-is-about-more-than-speed/ [Accessed 30th October 2020].

Alderson, A.S., et al. (2006) Globalization and the world city system: Preliminary results from a longitudinal dataset. In Taylor, P.J. et al. (eds.) *Cities in glo-*

balization: Practices, policies and theories. London, Routledge, pp. 21-36.

Barnes, C. & Barraclough, T. (2020) Deepfakes and synthetic media. In Steff, R., Burton, J. & Soare, S.R., *Emerging technologies and international security: Machines, the state, and war*. London, Routledge, pp. 206-220.

British Standards Institute. (2014) *PAS 181 Smart city framework*. Available from: https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/ [Accessed 28th August 2020].

Buzan, B. (2007) *People, States and Fear* (ECPR classics). Colchester, European Consortium for Political Research.

Cerrudo, C. (2014) Hacking US Traffic Control Systems. *Defcon Conference* presentation. Available from: https://www.defcon.org/images/defcon-22/dc-22-presentations/Cerrudo/DEFCON-22-Cesar-Cerrudo-Hacking-Traffic-Control-Systems-UPDATED.pdf [Accessed 8th August 2020].

Deloitte Center for Government Insights. (2019) Making smart cities cybersecure. Available from: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Report_making_smart_cities_cyber_secure.pdf [Accessed 10th August 2020].

Eden Strategy Institute. (2018) *Top 50 Smart City Governments*. Available from https://static1.squarespace.com/static/5b3c517fec4eb767a04e73ff/t/5b513c57aa4a99f62d168e60/1532050650562/Eden-OXD_Top+50+Smart+City+Governments.pdf [Accessed 8th August 2020].

Elmaghraby, A.S., and Losavio, M. (2014) Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*. 5 (4), 491-497.

ESI ThoughtLab. (2020) Smarter Cities 2025 Building a Sustainable Business and Financing Plan. Available from: https://econsultsolutions.com/wp-content/uploads/2018/11/ESI-ThoughtLab_Smarter-Cities-2025_ebook_FINAL.pdf [Accessed 10th August 2020].

European Commission. (2020a) *EU-funded projects on Smart Cities*. Available from: https://ec.europa.eu/digital-single-market/en/eu-funded-projects-smart-cities [Accessed 28th February 2020].

European Commission. (2020b) The EU cybersecurity certification framework. Available from: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework [Accessed 16th October 2020].

European Commission. (2017) The making of a smart city: best practices across Europe. Available from: https://smartcities-infosystem.eu/sites/default/files/document/the_making_of_a_smart_city_-_best_practices_across_europe.pdf [Accessed 10th August 2020].

European Union Agency for Cybersecurity. (2020) ENISA Threat Landscape 2020. Available from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents [Accessed 29th October 2020].

Hybrid COE (The European Centre of Excellence for Countering Hybrid Threats). (2020) Helsinki in the era of hybrid threats – Hybrid influencing and the city. Available from: https://www.hybridcoe.fi/wp-content/uploads/2018/08/Helsinki-in-the-era-of-hybrid-threats---Hybrid-influencing-and-the-city_ENG.pdf [Accessed 4th August 2020].

Fagan, M.J., Megas, K.N. et al. (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. Available from: https://www.nist.gov/publications/foundational-cybersecurity-activities-iot-device-manufacturers [Accessed 16th October 2020].

Ferbrache, D. (2020) The rise of ransomware during COVID-19, KPMG. Available from: https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html [Accessed 30th October 2020].

Fernandez, M. et al (2019) Ransomware Attack Hits 22 Texas Towns, Authorities Say. *New York Times*, 20 August. Available from: https://www.nytimes.com/2019/08/20/us/texas-ransomware.html [Accessed 8th August 2020].

Greene, J. (2020) Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. *Washington Post*, June 11. Available from: https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ [Accessed 12th June 2020].

Hwang, T. (2020) Deepfakes: A Grounded Threat Assessment. *Centre for Security and Emerging Technologies, Georgetown University*. Available from: https://cset.georgetown.edu/research/deepfakes-a-grounded-threat-assessment/ [Accessed 10th August 2020].

IESE Business School. (2019) These Are the Smartest Cities in The World For 2019. Available from: https://www.forbes.com/sites/iese/2019/05/21/these-are-the-smartest-cities-in-the-world-for-2019/#606301461429 [Accessed 8th August 2020].

IESE Business School. (2019) IESE Cities in Motion Index 2019. Available from: https://media.iese.edu/research/pdfs/ST-0509-E.pdf [Accessed 10th July 2020].

International Data Corporation. (2020) *Smart Cities Initiatives Forecast to Drover $189 Billion in Spending in 2023*. Available from: https://www.idc.com/getdoc.jsp?containerId=prUS45303119 [Accessed 14th August 2020].

International Organization for Standardization. (2020) *ISO/IEC 30145-3:2020 Information technology — Smart City ICT reference framework — Part 3: Smart city engineering framework.* Available from: https://www.iso.org/standard/76373.html [Accessed 16th October 2020].

Kitchin, R. & Dodge, M. (2017) The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*. 26 (2), 47-65, DOI: 10.1080/10630732.2017.1408002.

Malwarebytes. (2019) Malwarebytes Reports 365 Percent Spike in Business Ransomware Detections. Available from: https://press.malwarebytes.com/2019/08/08/malwarebytes-reports-365-percent-spike-in-business-ransomware-detections/#:~:text=Overall%20ransomware%20detections%20against%20businesses,ransomware%20as%20a%20major%20contributor [Accessed 8th August 2020].

OECD. (2018) Smart Cities and Inclusive Growth. Available from: https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf [Accessed 12th August 2020].

O'Reilly, L. (2020). Sadiq Khan says Cobra hasn't met since May 10 and he hasn't spoken to Boris Johnson in four months. *Evening Standard*. Available from: https://www.standard.co.uk/news/politics/sadiq-khan-cobra-boris-johnson-may-10-a4550651.html [Accessed 30th October 2020].

NATO. (2020) *Resilience and Article 3*. Available from: https://www.nato.int/cps/en/natohq/topics_132722.htm [Accessed 16th October 2020].

NATO. (2019) NATO Defence Ministers to address key issues for the Alliance. *Press Release.* Available from: https://www.nato.int/cps/en/natohq/169941.htm?selectedLocale=en [Accessed 16th October 2020].

NATO Science & Technology Organization. (2020) Science & Technology Trends

2020-2040: Exploring the S&T Edge. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf [Accessed 30th March 2020].

Nominet. (2018). Smart city projects showcase – great uses of IoT in urban contexts, available from: https://www.nominet.uk/smart-city-projects-showcase-great-uses-of-iot-in-urban-contexts/ [Accessed 30th October 2020].

Polunsky, S. (2019) The City-Sized Hole in U.S. GPS Planning. *Belfer Center, Harvard University Kennedy School*, Homeland Security Policy Paper #3. Available from: https://www.belfercenter.org/sites/default/files/files/publication/HSP%20paper%20series%203%20-%20draft%202.pdf [Accessed 10th August 2020].

PWC. (2020) *Rapid Urbanisation*. Available from: https://www.pwc.co.uk/issues/megatrends/rapid-urbanisation.html [Accessed 14th August 2020].

Reilly, S. (2015) Records: Energy Department struck by cyber-attacks *USA Today*. Available from: https://eu.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/ [Accessed 10th August 2020].

Ritchie, H. & Roser, M. (2018) *Urbanisation*. Our World in Data. Available from: https://ourworldindata.org/urbanization [Accessed 8th August 2020].

Robles, F. (2019) A City Paid a Hefty Ransom to Hackers. But Its Pains Are Far From Over. *New York Times*, 7 July. Available from: https://www.nytimes.com/2019/07/07/us/florida-ransom-hack.html?action=click&module=RelatedLinks&pgtype=Article [Accessed 7th August 2020].

Smart Cities World. (2019) *Smart city technology market to grow to $263 billion by 2028.* Available from: https://www.smartcitiesworld.net/news/news/navigant-tracks-smart-city-projects-around-the-world-4296 [Accessed 8th August 2020].

Singhal, A., Ibrahim, K., Majumdar, S., & Bastos, D. (2020) Defining Actionable Rules for Verifying IOT Safety and Security. Available from: https://www.nist.gov/publications/defining-actionable-rules-verifying-iot-safety-and-security [Accessed 16th October 2020].

Sookhak, M., Tang, M., He, Y., & Yu, R.F. (2018) 'Security and privacy of smart cities: a survey, research issues and challenges.' *IEEE Communications Surveys & Tutorials*. 21 (2), 1718-1743 [Accessed 16 October 2020].

Statista. (2020) *Distribution of countries with largest stock markets worldwide as of January 2020*. Available from: https://www.statista.com/statistics/710680/global-stock-markets-by-country/ [Accessed 30th September 2020].

United Kingdom National Infrastructure Commission. (2018) National Infrastructure Assessment Report. Available from: https://www.nic.org.uk/wp-content/uploads/CCS001_CCS0618917350-001_NIC-NIA_Accessible.pdf [Accessed 14th August 2020].

United Nations. (2020) *Sustainable Cities and Communities*. Available from: https://unstats.un.org/sdgs/report/2019/goal-11/ [Accessed 8th August 2020].

United Nations. (2018) *68% of the world population projected to live in urban areas by 2050, says UN*. Available from: https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html [Accessed 8th August 2020].

United States Department of Energy. (2017) Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities. Available from: https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf [Accessed 20th August 2020].

United States Department of Homeland Security. (2015) The Future of Smart Cities: