Building a safer future in Government

kaspersky BRING ON THE FUTURE

go.kaspersky.com/government

2021

Introduction

When it comes to technology, the government sector wears two distinct – and often competing – hats: that of customer and of regulator. In beginning our investigation into the opportunities and risks that governments face in building an increasingly smart, networked operation, it's useful to look at each of these hats in turn.

Government as customer

Privatization and outsourcing of essential civic services drives competition and can bring cost efficiencies to local government bodies. For example, in London alone, 14 out of 32 boroughs outsource waste collection to French transnational Veolia. However, when it comes to civic services such as waste collection, outsourcing is a **choice** that local governments make, based on their unique needs and budgets.

When it comes to internet and other computer services, outsourcing is **not** a choice: governments do not provide such services in-house. While governments are still able to put out tenders for such contracts, one fact remains constant: they are always reliant on external private operators for the provision of services which are increasingly essential, and increasingly complex. So even though governments can put such contracts out for tender and with rigorous procurement processes, outsourcing of essential technology contracts is not optional, it is **required**.

This dynamic means that governments are always, to some degree, at the mercy of the quality, consistency, security and reliability of external private players for the networked services they can no longer do without.

This chronic dependency is buffered, but also complicated by, government's other hat – that of regulator.

Government as regulator

Governmental power over private technology (and other) providers is immense. Across the world, suppliers must grapple with a huge array of government-enforced standards – a concatenation of ISOs, CISQs, Sops, NERCs, NISTs, RFCs, ANSIs, IECs and more - which, if not met, spell the denial of contracts and eventual dissolution.

Yet the role of government as regulator isn't only restricted to the application of essential standards to service providers. With data now crowned as the 'new oil,' regulations such as the EU's GDPR control how data is used – protecting the rights of citizens.

Compounding this regulatory responsibility is the advent of a new theatre of war – that of international cybercrime. The internet is inherently borderless: even in countries which restrict access to services such as Facebook or WhatsApp, citizens routinely use VPNs to circumvent such bans. International cybercrime is a huge umbrella term, encompassing everything from phishing emails to terror-motivated attacks on essential life-saving services and, of course, espionage. Regulatory motivations are therefore based not only on the need to protect citizens' rights to privacy, but also on safeguarding the integrity of businesses and defending governments themselves.

Dependency on services which they themselves regulate marks the government sector out as unique in its relationship to networked services providers. This brings some interesting factors into play, particularly given the enormous technological developments which are revolutionizing the way governments everywhere operate.

Citizens as customers

Governments come and go, but the structural relationship between government and citizen is always one of monopoly. Each country, each region, can only have one government at a time – citizens don't get to pick and choose from a selection as they do when it comes to market operators.

Even in countries where the ruling government changes every four years, the makeup of the civil service, which executes the will of that government, very rarely changes. Career longevity within civil services departments outpaces that of private companies, becoming one of few sectors in which one can still truly have 'a job for life'.

Despite this monopoly, the citizen's relationship to government is still one of customer to supplier.

Not only do governments have law-bound duties to their citizens to fulfil SLAs which may be implicit or explicit, but – like private entities – their longevity ultimately depends on customer satisfaction.

Governments use technology to satisfy their citizen-customers in two broad ways. The first is through the smooth running of state (or regional) services, such as those implemented in smart cities, or in the UK's Making Tax Digital initiative. The second is by keeping citizen-customers safe from cybercrime.

"A government can't prioritize its citizen 'customers' by using metrics like how valuable they are or how costly to serve — common practices in the private sector under similar circumstances."
McKinsey

"HMRC's ambition is to become one of the most digitally advanced tax administrations in the world… The Personal Tax Account brings together each individual customer's information in one online place. It allows customers to access the service from a digital device of their choice and at a time that suits them. It allows them to register for new services, update their information and see how much tax they need to pay."
Her Majesty's Revenue & Customs, UK

We know where you live

Governments know more about their customers than any market player could ever dream of. They know when we are born, what we earn, how healthy we are, where we live, when we die and even where we're buried – the data accrued is rich and endless. Citizens have to be able to trust governments to keep these comprehensive and sensitive datasets locked away from prying and malicious eyes.

All industries have a responsibility to safeguard the sensitive data repositories they accumulate. It's just that, when it comes to government, the stakes are so much higher.

Lack of technological maturity in governments

"Before the pandemic, agencies were primarily 'doing digital' - that is, leveraging digital technologies to enhance their capabilities but still largely relying on legacy operating models. COVID-19 propelled many governments into the next stage of digital transformation. Seventy-seven percent of government agencies say that digital transformation initiatives pushed during the pandemic are already having a positive impact on their organization."
Deloitte

The image of the weary, paper-pushing bureaucrat is slow to die. Absent the pressures of private market competition, technological adoption in governments can suffer because of inertia on both the individual and the collective (organizational) layer. Governments have been shown to lag behind the private sector when it comes to technological maturity, with the disparity even greater in developing countries. In an environment where many technologies also lack maturity (for example, blockchain), this lag represents an enormous challenge for governments as they innovate.

In this paper we're going to look at eight key technological trends, and the implications of these for governments across the world. For each trend, we'll also draw out some key risks and challenges that governments need to be aware of if they are to safeguard the countries or regions they're responsible for, and achieve maximum citizen-customer satisfaction.

Citizen engagement and digital ID

Digital transformation

AR / VR

Blockchain

E-payments & signatures

AI / ML

Smart cities

Regulatory challenges

Trend #1: Digital transformation – public sector innovation

"Almost half of government organizations are actively using cloud services."
Gartner

Digital transformation is an enormous theme, one which might cover every single one of the trends and challenges we're going to look at in this paper. After all, digital transformation is what happens to society – whether citizens like it or not – when governments implement technological solutions to civic problems. However, for our purposes, we're going to be discussing internal digital transformation; that is, the use of technological innovations to transform the operations of government departments themselves.

Given that cloud adoption is the **sine qua non** of digital transformation, it's useful to examine government attitudes to digital transformation through the prism of cloud adoption. Gartner forecasts a 23.1% increase in worldwide end-user spending on public cloud services in 2021, totaling $332.3 billion in investments. The forecast for 2022 is $480 billion.

$41.86 billion

"The (US) Government Cloud Market was valued at $14.93 billion in 2019 and is expected to reach $41.86 billion by 2025, at a CAGR of 18.74% over the forecast period 2020-2025."
GlobeNewsWire

However, these bullish statistics ring slightly differently when we look at the proportion of private vs public cloud adoption among governments.

Needless to say, privacy is a major concern for government, particularly with the citizen-as-customer model propelling digital engagement, with civic services (including local tax payment services) delivered online. The enormous swathes of highly sensitive citizen-customer data that governments now hold and process explain why the majority of cloud adoption in the sector is likely to be private, rather than public.

"The COVID-19 pandemic has accelerated the advent of truly digital government, with agency leaders establishing essential elements of digital infrastructure, the needed workforce, and citizen-facing connectivity."
Deloitte

Data sovereignty is another reason why governments are less likely to adopt (and therefore benefit from) public cloud services. This principle holds that data should only be processed or held in the country or region in which it was collected. The concern that governments frequently grapple with is, how can they guarantee that data held in a public cloud won't be held offshore, perhaps in a region with which it doesn't share a trusted regulatory framework? What would the compliance implications be?

Part of the problem is the lag in technological maturity in some government departments. Still faced with legacy systems and the delayed evolution that results from (sometimes well-placed) caution,

"This acceleration (in digital innovation) presents government leaders with new opportunities to leverage data and technologies that build trust, agility and resilience in public institutions."
Gartner

civil servants often lack the cybersecurity training they need to be able to forge ahead with vital digital transformation strategies without fear of cyberattack. In fact, Gartner cites the 'lack of qualified staff' as one of the challenges governments face when it comes to legacy modernization, and warns that 'emerging technology adoption and the move to digital government is hampered by culture and lack of skills.'

This cautious attitude towards public cloud adoption, while partly understandable, does mean that governments pursuing digital transformation may lose out on some of the agility and efficiency of public cloud use.

Digital transformation – Threat spotlight – Debilitating caution

99%

Estonia has built an efficient, secure and transparent ecosystem where 99% of governmental services are online.

Globally, governments have accelerated the deployment of digital services crisis management systems as a response to the ongoing COVID-19 pandemic. Digital has become the new normal as governments around the world are scrambling to transform services and benefit from productivity and financial gains.

However, unlike commercial industries, which have no choice but to put their trust in the public cloud (or face being eclipsed by more efficient competitors), governments are, to some degree, able to fall back on the monopoly dynamic discussed earlier.

The risk is that, if governments fail to implement similar forms of cloud adoption as those leveraged by banks and industries, a critical misalignment will occur. Governments may struggle to provide the digital services that citizen-customers increasingly expect.

Secondly, governments may find their digital environments diverge considerably from those of businesses within their jurisdictions, causing what might be broadly called 'communication problems.'

Such communication problems range from a failure to understand 'life on the ground' to difficulties in outsourcing because of incompatible systems. Added to this, an unfamiliarity with potentially idiosyncratic digital government systems may cause skills shortages, whereby highly skilled individuals may be unwilling (or unable) to transfer priceless skills acquired in the private sector.

The implications for caution are profound, with cybersecurity and privacy topping the lists of risks. Relying on 'quirky' proprietary solutions instead of the more future-ready cloud solutions used by the open market could expose government data, with a host of unpatched vulnerabilities attracting malicious attacks.

Where cloud adoption is excessively restricted to private cloud, the entire digital estate could be open to attack, while compartmentalization via a properly orchestrated hybrid cloud architecture might have kept critical data secure.

While governments clearly focus enormous efforts on cybersecurity as part of their intelligence and national defense organizations, they will continue to need the cybersecurity solutions of leaders in the private sector to defend their in-house operations, and safeguard their digital transformation strategies. They must make sound, informed decisions, pursuing digital transformation strategies that will best position them to guarantee robust cyber-defense for their operations.

Trend #2: Citizen engagement and digital identity

"Our goal is ultimately to enable residents to conduct all business with the government without ever having to enter a government office."
Ervan Rodgers Ohio (former) CIO

During the COVID-19 pandemic, governments around the world experienced the growing demand from citizens for improved online government services. So an unexpected consequence of the pandemic has been how fast government digital services have expanded. Brand new digital services were developed and rolled out to deal with a world in lockdown where citizens needed to engage seamlessly with government across multiple channels.

In 2021, citizens in developed countries have become accustomed to demanding engagement aligned to their immediate needs as a right. They also now expect to interact with government organizations at the time they want, using their choice of device – just as they interact with the most tech-savvy private sector companies. In short, they want seamless, multichannel capabilities and they want them to be comparable to the best the private sector has to offer.

82%

"82% of government CIOs report an increase in the use of digital channels to reach citizens in 2020 and expect that increase to be sustained in 2021."

73%

"73% of government CIOs report that the role of self-service channels in supporting citizens has increased through 2020."
2021 Gartner CIO Survey

Governments have responded by accelerating the concept of citizen engagement, rolling out a broad package of online services and engagements covering just about all aspects of a citizen's lifespan. They are also putting in place online measures to involve citizens more in shaping government processes. Gartner predicts that over 30% of governments will use engagement metrics to track the quantity and quality of citizen participation in policy and budget decisions by 2024.

At the heart of multichannel citizen engagement is government digital identity. The COVID-19 pandemic and ensuing lockdowns demonstrated just how crucial it has become to validate identity information remotely.

"Gartner predicts that a true global, portable, decentralized identity standard will emerge in the market by 2024, to address business, personal, social and societal, and identity-invisible use cases."
Gartner Top 10 government technology trends

No in-person interaction was possible but users still needed to access the entire range of government services. But tech savvy citizens do not expect to encounter complications accessing straightforward services. Although government services coped admirably well, authentication and identity-proofing has become more cumbersome and difficult to navigate. A single digital identity allowing access to all government online services has therefore became the absolute priority in developed countries.

A unique digital identity, that understands and joins together all government services a citizen uses, offers obvious advantages: streamlining service delivery, accumulating data to make services more intuitive and proactive, prompting customers on next actions, eliminating reset passwords for individual government services, and improving overall customer experience – all conducted without compromising data or exposing systems to new threats. The concept of citizen digital identity is also expanding and adapting to meet increased demands.

Citizen engagement and digital identity– Threat spotlight

Transforming the culture within government agencies, to reach the same standard as the private sector, is a formidable challenge. For effective digital identification and citizen engagement, governments must become skilled at harnessing data and insights to generate solutions which will be part of a seamless multichannel experience.

But the automation of government services and potential for manipulation of data generates unease amongst citizens. Cynics label digital identity and multichannel government engagement as opening the door to mass surveillance, misuse of data and citizen profiling. Governments must build trust ensuring accountability and transparency. Any cybersecurity breach will destroy citizens' trust - making security an imperative at the heart of government engagement strategy. Relying on any non-optimal cybersecurity solution increases the risk of exposing critical government data. More than ever cybersecurity solutions from the best in the private sector are needed to protect governments as they move the vast majority of their operations online.

In conclusion, governments understand just how crucial it has become to provide digital identity and multichannel online services meeting the growing demands of their citizens. Governments that are slow to transform risk alienating citizens, especially the younger generation. But digital identity and citizen engagement come with the enormous additional responsibility of safeguarding all introduced services from any breach or cybersecurity risk.

Trend #3: E-payments and digital signatures– the heart of e-governance

Typically, citizens become accustomed to new technologies long before their governments implement them in the services they provide. We might have Alexa at home, and pay by Apple Pay, but still need to resort to cumbersome and frustrating processes when faced with filing – or paying – our taxes.

E-payment and digital signature innovations have gradually been implemented by governments around the world. We've already mentioned the UK's Making Tax Digital initiative, but the UK is far from being the only country to implement e-payment and digital taxation initiatives. In June 2018, Singapore announced it was committed to offering electronic payment and digital signature options for all government services by 2023. The commitment was spearheaded by the country's Smart Nation and Digital Government Office.

A digital decade in one year

By far the biggest impetus to e-government has been the COVID-19 pandemic. With everyone 'locked down' at home, unable to visit or work in offices, the need for contactless government services facilitated by digital signatures became an imperative. 'A Digital Decade in One Year' was how the May 2021 e-governance conference in Tallinn, Estonia described the dramatic shift to online services.

Voting – the most powerful digital signature a citizen can make

The Canadian government cites the widespread business and pleasure use of internet technologies by its citizens as one of the key drivers for its introduction of electronic voting, in a rather lengthy exposition and defense of its plans to introduce the technology. The Canadian government's own research into citizens' lukewarm attitude towards electronic voting probably explains the time taken to make the case:

"The global digital signature market value stood at $1,858.3 million in 2020, and it is expected to demonstrate a CAGR of 29.2% during the forecast period (2021–2030)."
PSmarketresearch

"just under half of electors (49.1%) agree, somewhat (31.5%) or strongly (17.6%) that 'Canadians should have the option to vote over the Internet in federal elections'. This compares to 39.4% who disagree." And yet, in regions where the technology has been trialed, the reception was anything but lukewarm, and Canadians as a whole (99% in fact) say that they would be likely to use online voting if it were available to them.

E-payments and digital signatures – Threat spotlight – Is it really you?

According to a Forrester white paper, e-signature workflows keep business moving while also driving long-term revenue growth through improved customer and employee experience. People simply aren't willing to waste time waiting in line to sign in person, when they know very well that the technology exists to allow such things to be done almost in an instant online.

However, digital signatures present a clear cybersecurity risk and, if clear steps are not taken by governments adopting the technology, wholesale identity fraud could take flight, with criminals using stolen digital signatures to break down the existing barriers that in-person ID verification presents.

Government regulations around digital signatures vary from region to region. The EU's eIDAS (Electronic ID and Trust Services) insists on 'qualified signatures', with certificates issued by trusted service providers, while in the US, no such requirement exists.

Digital signature fraud entered the scene almost as soon as the technology was launched. In 2011, a Rome businessman discovered that all of the shares in his company had been transferred to a fraudster who used digital signature fraud to make himself the company's sole director.

Trend #4: Digital reality (AR/VR) in government

"I do think that a significant portion of the population of developed countries, and eventually all countries, will have AR experiences every day, almost like eating three meals a day. It will become that much a part of you."
Apple CEO, Tim Cook

Of the two main categories of digital reality, governments are most likely to adopt augmented, rather than virtual, reality. While the latter involves the wholesale creation of virtual 'worlds,' augmented reality (AR) involves the graphical overlay of digital reality onto real-time images of the real world.

One key government application for AR is enabling real-time in-field workers to see exactly how to fix or build a public resource or asset, simply by following visual, audio and haptic AR signals, including from hands-free head-mounted displays (HMDs). This dramatically increases the geographical reach of technical workers, and achieves the twin goals of boosting accuracy and reducing costs.

"[AR] gives workers tools to interact with digital data in the real world."
Deloitte

AR can be applied to countless applications including citizen engagement, military, safety, emergency services, cultural provision, education, health, maintenance and transport. Navigation is another key application – for trains, planes and automobiles alike – graphical overlays guide drivers and pilots towards what we hope will always be a safe landing.

Leveraging the wealth of data that comes courtesy of the IoT and connected cities (of which more later), multiplies the potential applications of AR, particularly when it comes to strategic planning. For example, by using traffic and pedestrian data, governments can see the effect a range of decisions would have on traffic flow, safety and pollution.

State-funded education is another sector adopting AR technology as fast as possible to cope with the distance learning revolution brought on by the COVID-19 pandemic. Optimized distance learning will continue to expand in education systems globally.

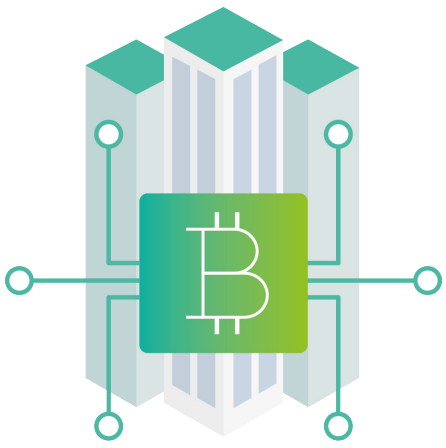
Digital reality – Threat spotlight – Beyond distraction

Aviation has always been a key terrorist target – from the hijackers of the 1970s to the suicide attacks of 9/11. With pilots increasingly relying on AR to aid navigation, avoid risk (such as flying geese), improve fuel efficiency and aid safe landings, aviation terrorists may be able to launch attacks from the safety of their own desktops.

When it comes to the government sector, military aviation has been particularly swift to seize on the opportunities presented by AR. British defense, security and aerospace multinational, BAE, has developed a helmet-mounted full-color AR display that projects augmented and virtual reality interactive cockpit displays and controls directly in front of the pilot's eyes, replacing current physical cockpit layouts. According to the company's Chief Test Pilot, Steve Formoso, the technology "provides a vital edge over whoever you are flying against."

The problem is that AR could allow terrorists to hack vulnerabilities and effectively move the theater of cyberwar from the office (in conventional cyberterrorism) to the military cockpit. AR for military aviation use is still in its infancy, but Carnegie Mellon University's canonical Emerging Technology Domains Risk Survey has already warned that "the criticality of such systems makes any compromise a potentially high-risk event to victims."

Risks extend beyond direct fatal interference with pilots' visual fields, and include real-time espionage and the potential for mission-critical leaks.



Trend #5: Blockchain in the public sector

Uptake of blockchain has, to date, been slow in the government sector. The technology's immaturity, combined with the barrier to entry represented by blockchain's complexity, mystique, and association with cryptocurrencies, are likely to blame.

According to Gartner's survey of CIOs in government, while 66% are interested in blockchain, only 20% have any action planned. Likely applications include citizen identification, voting and conducting transactions, as well as finance.

Certain regions, however, are ahead of the rest when it comes to blockchain implementation, with China perhaps leading the pack. Alibaba and Ant Financial have led the public-private partnership to develop blockchain applications for government, with Shanghai, Shanxi, Henan, Guangzhou, Guiyang and Hangzhou all having issued policies to encourage blockchain development.

Support from central government, in the form of a direct order from President Xi Jinping, highlights the use of blockchain technologies to create a smart city, as part of the master plan for the Xiongan New Area economic zone.

Such bold technological leadership is likely to inspire similar applications across the globe, with government departments positioned to adopt 'tried-and-tested' urban blockchain applications, and anxious not to fall behind.

Decentralized, and based on distributed ledger technology, blockchain significantly reduces the need for a central authority – such as (ironically) a government. However, this isn't as frightening as it sounds. The truth is that blockchain is unlikely to destroy central governments but, if used appropriately, it will do away with central points of failure, making key data and transactions more secure than ever, and protecting citizens along the way.

$83.3 billion

"A $4.47 million market worldwide in 2020, it is anticipated to grow rapidly to $83.3 billion in 2027 as central banks figure out how to use blockchain in their digital currency initiatives."
prnewswire

Blockchain – Threat spotlight – Distributed risk and no regulation

Most government departments are likely to use 'permissioned' rather than 'permissionless' (à la Bitcoin) blockchains. The OECD's Office of Public Sector Innovation (OPSI) compares this distinction to that of intranet, rather than internet use.

With permissioned ledger usage, governments must implement rigorous consensus models that restrict usage permissions, without restricting the efficiency of the technology itself.

Various aspects of blockchain technology present significant risks and challenges to governments wishing to implement it. There can be a clash with data privacy regulation, due to the inherent immutability of blockchain (data can be added, but not deleted).

Data storage can also be a challenge – blockchain is designed to work in small pockets, and not in the enormous private data centers that governments are accustomed to. Complexity remains a challenge, and (as we've seen in China), most governments will need to outsource quite a sizeable chunk of build and coding if they are to implement blockchain on any significant scale. Auditing and monitoring such a broad range of suppliers is going to be a key focus.

Interoperability is one of the key problems that could be solved with the implementation of standards. The current lack of interoperability is a double-edged sword, as Deloitte explains: "A lack of standards grants blockchain coders and developers freedom - and can give IT departments headaches as they discover that platforms can't communicate without translation help."

Because blockchain networks each use their own very specific proprietary platforms, coding mechanisms and other peculiarities, it can be hard to safely integrate a blockchain solution into an existing networked data environment. Unless standards are appropriately rigorous, interoperability itself could cause problems that detract from blockchain's famed security, as an analyst from CapGemini explains:

"Considering the interoperability among the networks, security issues of one network can easily be slid into another network with smart contract integrations or calls. This may undermine the security of the complete network."

Trend #6: Smart cities governance and the IoT

Smart cities don't have to be as ambitious and all-encompassing as China's Xiongan New Era economic zone (see above). Initiatives that leverage IoT technology in the creation of smart cities are being implemented all across the globe, piece by piece, as governments become hungry for tried and tested ways to boost efficiency and save costs.

"Smart infrastructure innovations could save cities millions."
Ernst & Young

In smart cities, sensors positioned throughout the infrastructure (public and private) are backed up by cloud-based processing power, in an integrated data system that takes the shape of a constant feedback loop, to titrate decisions and strategies in real time. Common applications include smart water meters, traffic control, public transport, energy efficiency in buildings, and public safety initiatives.

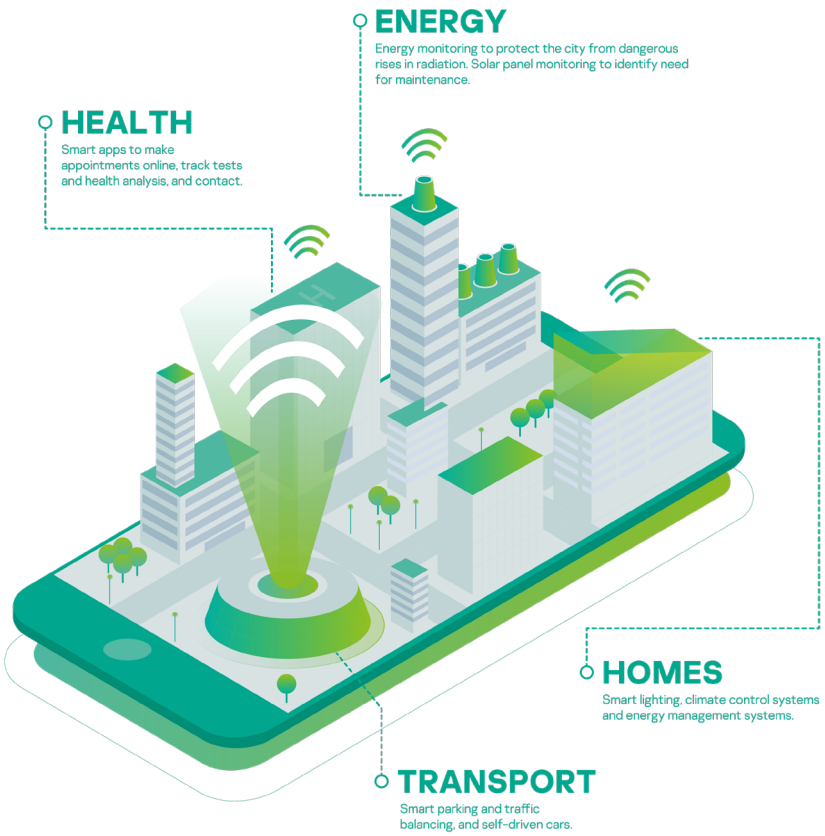
In most if not all cases, governments once again turn to private cellular providers to implement the IoT technology essential for driving the smart city revolution. One great example is the collaboration between Finnish health technology startup Nordkapp, and NYC-based urban systems design practice Urbanscale, to create Urbanflow - a project with a vision to make Helsinki more accessible and enjoyable for both residents and visitors through a situated interactive service.

$327 billion

"Smart cities' spending on technology in the next six years is expected to grow at a CAGR of 22.7%, reaching $327 billion by 2025 from $96 billion in 2019."
Frost & Sullivan

Urbanflow situates interactive screens throughout the city, offering multifaceted maps that are enriched by smart city data to offer navigation and transport tips, as well as ambient data on pollution, traffic density and other useful information. According to the founders, thanks to Urbanflow, "the city itself becomes more transparent and reactive to its citizens' needs," and "city officials and municipal governments are provided with a completely new way to connect with citizens and visitors, and a city that is more connected to its people works and feels better."

With the UN predicting that 68% of the world's population will be living in cities by 2050 , the push for smart cities is only going to accelerate, as governments grapple with the challenge of organizing and protecting such huge (and growing) populations.



Smart cities – Threat spotlight – The perennial paradox of new technology

Whenever an exciting new technology bursts on the scene, it's not only benevolent users that are quick to seize on it. This tension is an extension of the Dual-Use Paradox. Dual-use research has traditionally referred to technology that can be applied for both civil and military use. However, the term is now extended to encompass the paradox that any technology that might be good for consumers or businesses can also be used by criminals. The welcoming of all new networked technologies, IoT and smart cities, must always be tempered by the awareness that cybercriminals will be equally keen to make use of such innovations.

The Achilles heel of the IoT is the multiplication of attack interfaces that naturally comes with any hyper-connected networked system. Responding to concerns, in May 2021 the UK's National Cyber Security Centre published a set of principles on how to design and manage smart cities to make them resilient to cyberattacks.

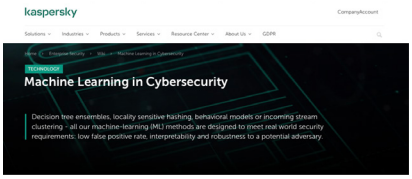
Kitchin and Dodge have identified five key vulnerabilities that cybercriminals seek to leverage in launching attacks against smart cities. These are the issues that governments need to pay particular attention to, if they are to avoid disaster:

1. Weak software security and data encryption.
2. The use of insecure legacy systems and poor ongoing maintenance.
3. Many interdependencies and large and complex attack surfaces.
4. The potential for cascade effects.
5. Human error and deliberate malfeasance of disgruntled (ex-) employees.

Trend #7: Automation & analytics (AI/ML) – benefits for government

Machine learning allows computers to automate inductive reasoning about data, basing inferences on outcomes and events learned from past occurrences. It's not a standalone technology, but a component that can be inserted into an existing system, to boost processing power and efficiency.

We've been using Machine Learning at Kaspersky for many years, implementing decision tree ensembles, locality sensitive hashing, behavioral models and incoming stream clustering to guarantee protection for endpoints and other data assets – read about it here.



"Automation can enable governments to provide outstanding levels of customer experience, driven by innovations that are as sensitive to people as they are to technology."

"We have identified three kinds of benefits. Perhaps the most obvious of these advantages is that of reliability and simplicity... A second way in which automation can boost customer experience in government services is by enabling civil servants to offer more complex and caring service provision... A third enhancement to customer experience that automation of government services can offer is personalized service delivery, including AI-enabled service." McKinsey

Forbes concluded "2021 is the year where AI will get embedded into existing devices and make certain functionality faster and more accurate as standard." It's clear that we're almost at that point, with AI and ML already common in many offices, factories and infrastructure projects.

Gartner has estimated 60% of government AI and data analytics investments will directly affect decision-making processes and results. Automation will reduce processing times and increase productivity by automating manual work. IBM identified that "over 95% of all incidents investigated recognize 'human error' as a contributing factor." It is clear that one of the key benefits of AI and ML is the ability to completely cut human error out of the cyber-risk equation. A properly coded algorithm is not going to let anyone in.

Due to its nature as a component technology, the applications of AI and ML for government are manifold and varied, including citizen-customer interaction (chatbots), HR, taxation, auditing, fraud prevention and safety. Automated analytics can significantly cut risks, whether those risks are financial, medical, security or otherwise. Whatever the implementation, the end goal is increased accuracy, cost-saving and reduced human labor hours.

In 2021 governments globally are beginning to reap the benefits of AI/ML – introducing innovative and improved services, increasing productivity, saving on costs and enhancing data-driven decision-making. Governments' main applications are in education, domestic security, transportation, healthcare and social welfare.

For example, the Australian government has already launched an experimental AI initiative that uses high definition cameras and AI technology to identify drivers who are distracted, particularly by illegally using their cell phones while driving.

AI/ML – Threat spotlight – What happens when human backs are turned?

Any movie fan will be familiar with the fears around machines taking over. When human beings are removed from the equation, how do we ensure that systems remain humane?

The EU has been working to move towards building a sober and considered policy set on cognitive technologies, making sure that investments are made on the one hand, but that public good is always at the forefront of any technologies. In fact, the EU cites the need for trust in ML/AI as one of the reasons behind the introduction of the GDPR.

In theory, cognitive technologies could be vulnerable to a particular form of cyberattack that might be called 'false learning': hackers feed false data into a system in order to make it learn erroneous 'facts' that will skew its mission. There have not been many such attacks to date, partly because the cybersecurity industry itself has been hot to uptake AI, and partly because the technology is still new, giving hackers less time to adapt.

However it is clear that wide-scale AI and machine learning implementation offers cybercriminals new big data attack possibilities. AI is being used in ransomware, malware and phishing attacks. AI algorithms are utilized to create video, audio and image deepfakes creating potential chaos in societies so that the line between reality and deception gets ever more blurred.

Another issue is government introduction of AI technology without sufficient safeguards. In June 2021 the US Government Accountability Office report highlighted that federal agencies using AI facial recognition held almost no accountability for the data collected.

Trend #8: Regulatory challenges

With all of the technologies we've examined in this paper, and with the sheer number of citizen-customers involved, the pressure to implement appropriate regulations is never more acute for governments. Governments must walk a fine line between encouraging businesses to innovate (so that their country doesn't fall behind), and implementing regulations to keep their citizens safe and satisfied.

A further challenge results from the set-in-stone fact of globalization and the sheer scale of the digital revolution. What happens when citizens from one jurisdiction interact with services supplied from another, perhaps less regulated one? How can governments control this?

There are far too many regulations around the world to summarize here. The UN's International Telecommunication Union is striving to encourage suitable regulations for its 193 member states, to establish global standards for a safer, globalized world. Its International Telecommunication Regulatory Database (in its 22nd edition for January 2019) is the canonical reference for the thousands of standards applied variously by countries across the globe.

75 billion

"The number of Internet connected devices is expected to increase from 31 billion in 2020 to 35 billion in 2021 and 75 billion in 2025."
Securitytoday.com

Regulatory challenges – Threat spotlight – The 'pacing problem'

Analysts at Deloitte say that regulators can be slow to keep up with the pace of technological innovation, resulting in what they call the 'pacing problem':

Bakul Patel, the US Food and Drug Administration (FDA)'s associate center director for digital health, says "There's a disconnect between the speed, iterative development and ubiquitous connected nature of digital health technologies and the existing regulatory structures and processes. The current regulatory approach is not well-suited to support that fast pace of development."

Risks for governments are twofold. Failing to keep pace with new technologies could lead to greater security risks, and a critical misalignment between the tech sophistication of government digital services and the ingenuity of hackers and cybercriminals. At the same time, resorting to loose regulation in order to expedite the development and adoption of new technologies could prove fatal.

Summary

Government organizations globally bear a heavy responsibility for meeting critical national security demands, and keeping their operations (and their citizens) safe. Of course all industries must safeguard the sensitive data repositories they accumulate, but for government, the stakes are so much higher. Every technological advance government organizations adopt could result in an increase in unexpected and new cyber threats. Understanding what those threats are likely to be is crucial. With swathes of highly sensitive personal data on citizens, and equally significant masses of political intellectual capital, making the right cybersecurity choice is critical. Without it, governments may find they are not free to leverage the exciting new technologies they need to build smart cities and to explore the many other connected societal innovations that will soon become the norm in countries across the globe.

Having a truly global security partner with relevant experience in all relevant emerging technologies is an essential support, assisting organizations to navigate the future. In spite of today's extremely volatile and challenging environment, Kaspersky has the perfect solutions to protect your data – and that of your citizens. Just use the table below to choose the solution that suits your organization best.

Choose what fits best to protect your organization

Kaspersky helps government bodies globally adopt proven security strategies in today's volatile and challenging environment. Our perfectly engineered, tailored solutions and services – assisted by world-leading security intelligence - protect data and business continuity 24/7 against advanced threats and targeted attacks – mitigating risks, detecting attacks earlier, dealing effectively with live attacks and fortifying future protection.

Step-by-step cybersecurity approach for future-proof protection

Our step-by-step cybersecurity approach is designed to clarify which level of security as well as which specific solutions suit your organization best. The frameworks provide a comprehensive set of threat protection measures coordinating seamlessly with one another to meet the needs of each individual organization, and offer a cybersecurity roadmap assuring smooth transition from one IT security maturity level to another when the time comes.

Kaspersky's step-by-step cybersecurity approach

1

Kaspersky Security Foundations – essential core of cloud-based, automated protection for all devices, VDI and hybrid server infrastructures, before organizations advance seamlessly to ...

2

Kaspersky Optimum Security - for organizations requiring more specialized security against new and evasive threats, before effortlessly implementing our third tier ...

3

Kaspersky Expert Security – for organizations with established mature IT security teams combatting the most complex targeted attacks.

Cybersecurity maturity level	Solution
IT Smaller organizations without a specialized IT security team	**What** Kaspersky Security Foundations **How** Implement fundamental security for organizations of any size and infrastructure complexity, delivering cloud-managed automatic prevention of commodity cyberthreats on any devices, VDI and hybrid server infrastructures. ▸ **Endpoints:** Protect every endpoint in your organization with Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security ▸ **Cloud:** Benefit from borderless security with Kaspersky Hybrid Cloud Security ▸ **Network:** Secure your perimeter with Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway ▸ **Data:** Safeguard valuable and sensitive data with Kaspersky Security for Storage ▸ **Security Management:** Access expertise with Kaspersky Premium Support; Kaspersky Professional Services
IT security Organizations in need of advanced defenses, but with limited specialist IT security resources	**What** Kaspersky Optimum Security **How** Combat evasive threats with effective endpoint detection and response and continuous security monitoring – but without prohibitive costs or complexity ▸ **Advanced detection:** Boost ML behavior analysis, sandboxing, threat intelligence and automated threat hunting* with Kaspersky Sandbox, Kaspersky Threat Intelligence Portal and Kaspersky Managed Detection and Response Optimum ▸ **Analysis and investigation:** Enhance threat visibility and simplified investigation process with Kaspersky Endpoint Detection and Response Optimum ▸ **Rapid response:** Deploy automated in-product response options, as well as guided and managed response scenarios* with Kaspersky Endpoint Detection and Response Optimum and Kaspersky Managed Detection and Response Optimum ▸ **Security awareness:** Equip employees with automated tools at all levels and develop key cybersecurity skills with Kaspersky Security Awareness Training *Supported by Kaspersky experts

Mature and fully formed IT security team and/or dedicated SOC

- Have a complex and distributed IT environment
- Are a highly likely target for complex and APT-like attacks
- Have a low risk appetite due to high costs of security incidents and data breaches
- Are concerned about regulatory compliance

What

Kaspersky Expert Security

How

Complete mastery over the most complex and targeted cyberattacks

- **Equipped:** Equip your in-house experts to address complex cybersecurity incidents. Benefit from a unified cybersecurity solution. **Kaspersky Anti Targeted Attack Platform with Kaspersky EDR** at its core empowers your team with XDR capabilities.

- **Informed:** Enrich your knowledge pool with threat intelligence and upskill your experts to deal with complex incidents:
  - Integrate actionable, immediate threat intelligence into your security program. **Kaspersky Threat Intelligence** gives you instant access to technical, tactical, operational and strategic threat Intelligence.
  - Develop your in-house team's practical skills, including working with digital evidence, analyzing and detecting malicious software, and adopting best practices for incident response, with **Kaspersky Cybersecurity Training.**

- **Reinforced:** Call upon external experts for security assessment, immediate support and back-up:
  - Take advantage of immediate support from the **Kaspersky Incident Response** team of highly experienced analysts and investigators to fully resolve your cyber-incident, fast and effectively.
  - Bring in a second opinion and managed threat hunting expertise from a trusted partner with **Kaspersky Managed Detection and Response**, so your in-house IT security experts have more time to spend reacting to the critical outcomes requiring their attention.
  - Understand just how effective your defenses would really be against potential cyberthreats, and whether you're already the unwitting target of a long-term stealth attack, through **Kaspersky Security Assessment**.

Targeted Solutions

What	How
 **Kaspersky Fraud Prevention**	Advanced Authentication allows for frictionless and continuous authentication, cutting the costs of second factor processes for legitimate users, while keeping fraud detection rates high in real time. Automated Fraud Analytics thoroughly analyzes events that occur during the entire session, transforming them into valuable pieces of data. Protects the external perimeter of any organization, ensuring safety and protection for citizens/customers.
 **Kaspersky DDoS Protection**	Covers a bandwidth of up to 2Gbps, with extensive service coverage, including attack analysis reports and anti-DDoS capability assessments. Optional automatic always-on DDoS mitigation, fortified by Kaspersky engineers running parallel checks to optimize defense according to the nature of each DDoS attack.
 **Kaspersky Threat Attribution Engine**	A malware analysis tool deployed on your network, “on premise”, in your private or public cloud, that incorporates 22 years of Kaspersky’s database of APT malware samples. Delivers automated analysis of the “genetics” and “genotypes” of malware for code similarity with previously investigated APT samples to rapidly link new attacks to known APT malware, actors, campaigns and previous targeted attacks.
 **Kaspersky Research Sandbox**	Emulates company-specific systems in an isolated environment, performing automated, behavioral malware analysis, and enabling safe detonation and detection of advanced and previously unseen threats.

...Or do it yourself!

Build your own National Security Solution.

Take total control over your cyber-defenses by building custom security products based on Kaspersky technologies, via the Kaspersky Technology Alliances program. We provide multiple Software Development Kits (SDKs) and Threat Data Feeds, empowering you to develop your own bespoke solution, 100% tailored to your unique specifications.

Your customized solution yields multiple unique benefits, including:

- Deploy when and where you need it most, fitting your unique requirements to perfection.
- Choose between implementing custom solutions as 'classic' software security suites or on a hardware platform (secure web gateway or UTM device).
- Implement multi-layered protection, for example by deploying Kaspersky-enabled secure web gateways at the points of network entry.
- Eliminate complexity with crystal-clear, plain text Threat Data Feeds.
- Maintain total control and sovereignty over your data, with a custom solution developed by experts with all necessary security clearances in your own country.
- Configure custom cloud protection solutions, to bypass the risks inherent in deploying third party solutions.

Cyberthreats News: www.securelist.com

IT Security News: www.kaspersky.com/blog

Threat Intelligence Portal: opentip.kaspersky.com

Technologies at a glance: www.kaspersky.com/TechnoWiki

Awards and recognitions: media.kaspersky.com/en/awards

Interactive Portfolio Tool: kaspersky.com/int_portfolio

kaspersky BRING ON THE FUTURE